Diszkrét matematika 2

9. előadás
Polinomok

Mérai László
merai@inf.elte.hu
https://sites.google.com/view/laszlomerai

Komputeralgebra Tanszék

2023 ősz

Emlékeztető, motiváció

- Egy $f \in \mathbb{K}[x]$ polinom irreducibilis, ha nem írható $f = gh$ szorzatként, hogy $\deg g, \deg h < \deg f$.
- Például az $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ polinom irreducibilis.
- Speciálisan az f-nek nincs gyöke (v.ö. gyöktényező kiemelhetősége)
- Szeretnénk olyan j formális számot bevezetni, hogy $f(j) = 0$.

Kitérő: test fogalma

A test egy olyan számkör, ahol a szokásos számolási szabályok érvényesek $(+, -, \cdot, /)$.

- példa testekre: $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}_p$
- példa nem testekre: $\mathbb{Z}$, $\mathbb{Z}_8$, $\mathbb{R}^{n\times n}$
  (nem minden nem-nulla elemmel lehet osztani, vagy a $\times$ nem kommutatív)

Konstrukció testekre:

- Komplex számok $\mathbb{C}$: formálisan számolni az i komplex egységgyökkel az $i^2 = -1$ szabály szerint,
  azaz $\mathbb{C} \cong \{f \bmod x^2 + 1 : f \in \mathbb{R}[x]\}$ (a megfeleltetés: $x \longleftrightarrow i$)
- $\mathbb{Z}_p \cong \{n \bmod p : n \in \mathbb{Z}\}$

Kitérő: test fogalma

Konstrukció (NB)

Legyen $\mathbb{K}$ egy test és $f \in \mathbb{K}[x]$ egy irreducibilis polinom. Ekkor $\{h \bmod f : h \in \mathbb{K}[x]\}$ testet alkot. Ennek jelölése $\mathbb{K}[x]/(f)$.

A $\mathbb{K}[x]/(f)$ elemei: $\mathbb{K}$ és x-ből képzett formális kifejezések, hogy x gyöke f-nek.

Példa

- $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$ $(i \longleftrightarrow x)$.
- $\mathbb{Q}[x]/(x^2-2)$: $\mathbb{Q}$ és $\sqrt{2}$ elemekből álló formális kifejezések $(\sqrt{2} \longleftrightarrow x)$.

Kitérő: test fogalma

Konstrukció: Legyen $\mathbb{K}$ egy test és $f \in \mathbb{K}[x]$ egy irreducibilis polinom. Ekkor $\{h \bmod f : h \in \mathbb{K}[x]\}$ testet alkot. Ennek jelölése $\mathbb{K}[x]/(f)$.

Példa

- $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$.

Megjegyzés:

- Az $+, -, \cdot$ a szokásos számolási szabályok szerint.
- Osztás: Legyen $h \not\equiv 0 \mod f$. Ekkor h-val lehet osztani, azaz minden g-hez létezik $q \in \mathbb{K}[x]$: $g \equiv h \cdot q \mod f$.
  Mivel $f \nmid h$ és f irreducibilis, a bővített euklideszi algoritmus szerint
  $$1 = uf + vh.$$
  Beszorozva g-vel:
  $$g = guf + gvh \equiv gvh \mod f,$$
  így $q \equiv gv \bmod f$.

Véges testek

Egy számkör **véges testet** alkot, ha test (szokásos számolási szabályok) és véges sok eleme van.

Példa

- Véges testek: $\mathbb{Z}_2, \mathbb{Z}_3, \ldots, \mathbb{Z}_p$
- Nem véges testek:
  $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ (testek, de nem végesek),
  $\mathbb{Z}_6, \mathbb{Z}_8, \mathbb{Z}_2^{2\times 2}, \ldots$ (végesek, de nem testek)

Tétel (NB)

Minden q prímhatvány esetén létezik q-elemű véges test. Ez lényegében egyértelmű, jelölése $\mathbb{F}_q$ (vagy $GF(q)$).

Példa

- $\mathbb{F}_p = \mathbb{Z}_p$
- $\mathbb{F}_{p^n} = \mathbb{Z}_p[x]/(f)$ ahol $f \in \mathbb{Z}_p[x]$ egy n-ed fokú irreducibilis polinom.

Véges testek – egy példa

$f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ irreducibilis. Ekkor $\mathbb{F}_4 = \mathbb{Z}_2[x]/(x^2 + x + 1)$.

- $\mathbb{F}_4$ elemei: polinomok modulo $x^2 + x + 1$: $0, 1, x, x + 1$.
- összeadás, szorzás:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\times$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

Például:

- $x \cdot x = x^2 \equiv x + 1 \mod x^2 + x + 1$
- $x \cdot (x + 1) = x^2 + x \equiv 1 \mod x^2 + x + 1$
- $(x + 1) \cdot (x + 1) = x^2 + 1 \equiv x \mod x^2 + x + 1$
- $\dfrac{x}{x + 1} \equiv x + 1 \mod x^2 + x + 1$

Testek: összefoglaló

- Testek foglama:
  szokásos számolási szabályok, pl. $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}_p$ vizsgán nem kell
- Konstrukció testekre:
  $\mathbb{K}$ test, $f \in \mathbb{K}[x]$ irreducibilis, ekkor $\mathbb{K}[x]/(f)$ szintén test, vizsgán nem kell
- Véges testek:
  $\mathbb{F}_{p^n} = GF(p^n) = \mathbb{Z}_p[x]/(f) = \{g \mod f : g \in \mathbb{Z}_p[x]\}, f \in \mathbb{Z}_p[x]$ irreducibilis,
  vizsgán kell

Lagrange interpoláció

Probléma: Legyenek $x_0, x_1, \ldots, x_n \in \mathbb{C}$ páronként különböző alappontok és $y_0, y_1, \ldots, y_n \in \mathbb{C}$ tetszőleges értékek. Létezik-e olyan f polinom, hogy $f(x_i) = y_i$.
Interpoláció az
L_i Lagrange alappolinomokkal:

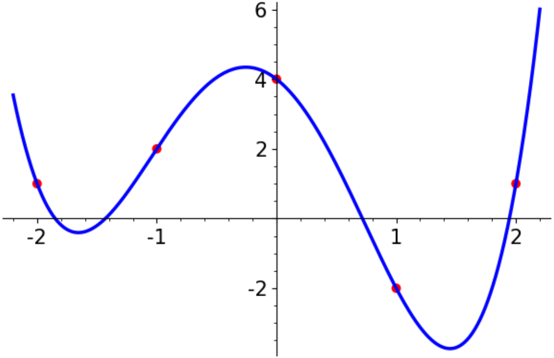
$$L_i = \prod_{\substack{j=0\\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j}.$$

Ekkor

$L_i(x_i) = 1$ és $L_i(x_j) = 0, \quad i \neq j$

Így

$$f = \sum_{i=0}^{n} y_i L_i$$



Lagrange interpoláció

Legyen

$$L_i = \prod_{\substack{j=0 \\ j\neq i}}^{n} \frac{x - x_j}{x_i - x_j} \quad \text{és} \quad f = \sum_{i=0}^{n} y_i L_i$$

Tétel

Legyenek $x_0, x_1, \ldots, x_n \in \mathbb{C}$ páronként különböző alappontok és $y_0, y_1, \ldots, y_n \in \mathbb{C}$ tetszőleges értékek. Ekkor egyértelműen létezik olyan f polinom, hogy $\deg f \leq n$ és $f(x_i) = y_i$.

Bizonyítás.

- Létezés: volt, Lagrange alappolinomokkal.
- $\deg f$: mivel $\deg L_i = n$, így $\deg f = \deg \sum_i y_i L_i \leq n$.
- egyértelműség: ha $f(x_i) = g(x_i) = y_i$, $(i = 0, 1, \ldots, n)$ és $\deg f, \deg g \leq n$, akkor legyen $F = f - g$. Ekkor $\deg F \leq n$.Ekkor $F(x_i) = 0$, így F-nek $n + 1$ gyöke van, ellentmondás.

Lagrange interpoláció

Példa

Legyenek $x_0 = 0, x_1 = 1, x_2 = 2$ és $y_0 = 3, y_1 = 0, y_2 = 1$.
Keresünk $f \in \mathbb{Z}_5[x]$: $f(x_i) = y_i$.

- Alappolinomok:

$$L_0 \equiv \frac{(x-1)(x-2)}{(0-1)(0-2)} \equiv \frac{1}{2}(x-1)(x-2) \equiv 3(x-1)(x-2) \mod 5$$

$$L_1 \equiv \frac{(x-0)(x-2)}{(1-0)(1-2)} \equiv -(x-0)(x-2) \equiv 4(x-0)(x-2) \mod 5$$

$$L_2 \equiv \frac{(x-0)(x-1)}{(2-0)(2-1)} \equiv \frac{1}{2}(x-0)(x-1) \equiv 3(x-0)(x-1) \mod 5$$

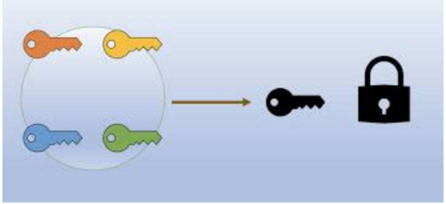
Így

$$\begin{aligned} f = 3 \cdot L_0 + 0 \cdot L_1 + 1 \cdot L_2 &= 3 \cdot 3(x-1)(x-2) + 3(x-0)(x-1) \\ &\equiv 2x^2 + 3 \mod 5 \end{aligned}$$

Kriptográfiai alkalmazás: titokmegosztás

Probléma: Szeretnénk szétosztani n résztvevő között titok darabokat, hogy

- bármely k résztvevő ki tudja számolni az eredeti titkot;
- k-nál kevesebb résztvevő ne tudjon semmilyen információt meg a titokról.



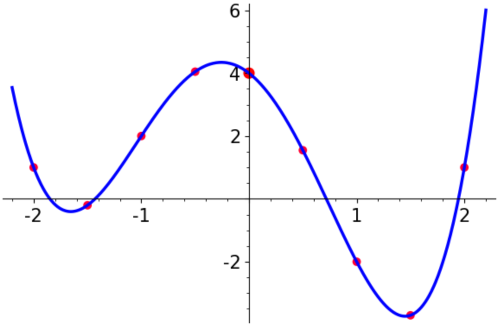
Példa

Legyen $n = k = 2$ és $s \in \mathbb{Z}_2$ egy titkos bit.
Válasszunk egy $r \in \mathbb{Z}_2$ bitet véletlenszerűen, és A kapja meg r-et, B kapja meg $r + s \bmod 2$-t.

Kriptográfiai alkalmazás: titokmegosztás

Megoldás:

- Legyen $q > n$ egy prímhatvány és $s \in \mathbb{F}_q$ a titok.
- Legyen $f \in \mathbb{F}_q[x]$, hogy $\deg f = k - 1$ és $f(0) = s$.



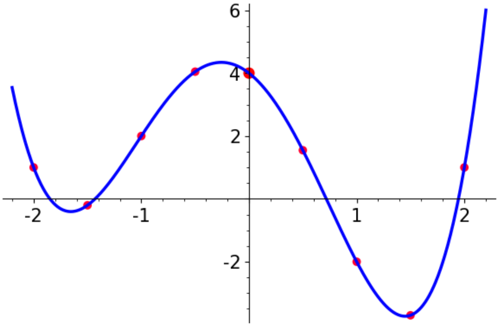
- Az i-edik résztvevő kapja meg a $(i, f(i))$ párost ($i = 1, \ldots, n$).
- Ha k résztvevő kiszámolja a Lagrange interpolációs polinomot a saját pontjaikon keresztül, akkor az egyértelműség miatt ez f lesz és $f(0) = s$.

Kriptográfiai alkalmazás: titokmegosztás

Példa:

- Legyen $n = 6$ és $k = 4$. Válasszuk $q = 7$-et.
- Legyen $0 \in \mathbb{F}_7$ a titok.
- Legyen

$$f = x^3 + 3x^2 + x \in \mathbb{F}_7[x].$$



- Osszuk szét a résztvevők között az $(i, f(i))$ párokat:

$$(1,5),\ (2,1),\ (3,1),\ (4,4),\ (5,2),\ (6,1)$$

- Ekkor bármely 4 pár meghatározza f-et.