Polinomok alapjai

Diszkrét modellek alkalmazásai

1. Alapfogalmak

1.1. Definíció. A **polinom** egy olyan matematikai kifejezés, amelyben csak az alábbiak szerepelnek:

- konstansok (pl. számok),
- egy változó (pl. x),
- összeadás, kivonás, szorzás,
- hatványozás $\mathbb{N}$-beli kitevővel,
- zárójelek.

Példa. A $3x^5 - 5x^3 + x + 1/2$, az $x^2(x+3)^5$ és a 15 polinomok, de nem polinom az $1/x$ (mert osztás van benne), az x^{-5} (mert a kitevő negatív) és a $\sqrt{x}$ (mert a négyzetgyök nem megengedett).

Megjegyzés: lehet általánosabban is definiálni a polinomot, ha megengedünk egynél több változót is, például akkor az $x^3 + xy^2 + y$ egy *kétváltozós polinom*. Ekkor a fenti definíció az *egyváltozós polinom*ot definiálja. Ebben a tárgyban azonban csak az utóbbiakkal foglalkozunk, ezért nem tesszük ki külön az "egyváltozós" jelzőt.

1.2. Definíció. Jelölje $K[x]$ azon polinomok halmazát, melyekben x a változó, és minden konstans a K halmazból való. Elnevezés: $K[x]$ a K **fölötti** polinomok halmaza.

Példa. $\mathbb{R}[x]$ a valós polinomok halmaza, és ennek részhalmaza $\mathbb{Z}[x]$, amelyben a konstansok csak egész számok lehetnek. Például $2x^2 - 5 \in \mathbb{Z}[x]$ és $\sqrt{2}x + 3/2 \in \mathbb{R}[x]$, de $\sqrt{2}x + 3/2 \notin \mathbb{Z}[x]$.

Ugyanazt a polinomot többféle alakban is felírhatjuk, például:

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

Ha egyértelmű felírást szeretnénk, akkor a következő alakot használhatjuk:

1.3. Definíció. Egy $p \in K[x]$ polinom **kanonikus alakja** a következő:

$$p = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_2 x^2 + a_1 x + a_0,$$

ahol $\forall a_k \in K$ és $a_n \neq 0$.

Példa. $p = (2x+1)^2$ kanonikus alakja $p = 4x^2 + 4x + 1$.

Bármely polinomot kanonikus alakra tudunk hozni a következőképpen: bontsuk fel a zárójeleket, a tagokon belüli szorzásokat hajtsuk végre (pl. $x \cdot 2x \cdot 3 = 6x^2$), az azonos kitevőjű tagokat vonjuk össze, és a tagokat rendezzük kitevő szerint csökkenő sorrendbe.

1.4. Definíció. A fenti kanonikus alakban:

- a_k-k a polinom **együtthatói** [*coefficient*] (konkrétan a_k a polinom ***k*-adfokú együtthatója**);
- n a polinom **fokszáma** [*degree*] (jelölés: $\deg p$);
- a_n a polinom **főegyütthatója** [*leading coefficient*];
- a_0 a polinom **konstans tagja** [*constant term*].

Példa. $p = 2x^3 - 6x + 4$ együtthatói 2, 0, -6 és 4 (a 0 a hiányzó x^2-es taghoz tartozik), fokszáma 3, főegyütthatója 2 és konstans tagja 4.

Van azonban egy polinom, amely nem írható fel a fenti módon definiált kanonikus alakban: a 0 (mert kitötöttük, hogy $a_n \neq 0$). Ezért ezt külön kell kezelni:

1.5. Definíció. A $0 \in K[x]$ polinom neve **nullpolinom**, kanonikus alakja 0, és fokszáma $-\infty$.

(Megjegyzés: azért $-\infty$, hogy kisebb legyen bármely más polinom fokszámánál. Nem definiálhatjuk 0-nak, mert akkor a nullpolinomra nem működnének bizonyos megállapítások, amelyek minden más polinomra igazak, lásd például a szorzatpolinom fokszámát a következő jegyzetben. Más források nem definiálják a nullpolinom fokszámát, a Sage pedig -1-nek definiálja.)

Még néhány speciális eset:

1.6. Definíció.

- $p \in K[x]$ **konstans polinom**, ha $\deg p \leq 0$.
- $p \in K[x]$ **lineáris polinom**, ha $\deg p \leq 1$.

Példa. Konstans polinom a 2 és a 0, és lineáris polinomok a $2x - 3$, az x, a 2 és a 0.

2. Gyűrű fölötti polinomok

Eddig még nem volt szó arról, hogy a polinomok $K[x]$ jelölésében a K pontosan milyen halmaz lehet. Például gyakran valamelyik ismert számhalmaz: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ vagy $\mathbb{C}$.

Ha a polinomokat a lehető legáltalánosabban szeretnénk tárgyalni, akkor csak annyit fogunk feltenni, hogy K egy tetszőleges *egységelemes kommutatív gyűrű*. (A gyűrűkről és azok tulajdonságairól az előző jegyzetben volt szó.)

Példa. $\mathbb{Z}_5[x]$ a modulo 5 maradékosztályok ($\mathbb{Z}_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$) fölötti polinomok halmaza (lásd: Kongruenciák), pl. $p = \overline{4}x^2 + \overline{2}x + \overline{3} \in \mathbb{Z}_5[x]$. Ez hasonlóan működik, mint $\mathbb{Z}[x]$, csak az együtthatókkal mindig modulo 5 kell számolni, pl. $p + p = \overline{3}x^2 + \overline{4}x + \overline{1}$, mert $\overline{4} + \overline{4} = \overline{3}$ stb.

Megjegyzés: a K gyűrűről azért kötöttük ki, hogy kommutatív és egységelemes legyen, mert ezek nélkül már az alapfogalmakkal is problémák lennének. Például ha nem lenne kommutatív, akkor nem tudnánk minden polinomot kanonikus alakra hozni, hiszen már a $2x \cdot 2x = 4x^2$ átalakításhoz is felhasználtuk, hogy $x \cdot 2 = 2 \cdot x$. Ha pedig nem lenne egységelem, akkor nem tudnánk pl. az x polinomnak a főegyütthatójáról beszélni (ami $\mathbb{Z}[x]$-ben 1, hiszen $x = 1x$).

Könnyen belátható, hogy $K[x]$ megörökli a K alaphalmaz legtöbb tulajdonságát:

2.1. Tétel ($K[x]$ tulajdonságai)**.**

1. *Ha K gyűrű, akkor $K[x]$ is gyűrű.*
2. *Ha K kommutatív gyűrű, akkor $K[x]$ is kommutatív gyűrű.*
3. *Ha K egységelemes gyűrű, akkor $K[x]$ is egységelemes gyűrű (ugyanazzal az egységelemmel).*
4. *Ha K nullosztómentes gyűrű, akkor $K[x]$ is nullosztómentes gyűrű.*
5. *Ha K integritási tartomány, akkor $K[x]$ is integritási tartomány.*

Van viszont egy tulajdonság, amely nem öröklődik: a $K[x]$ nem lehet *test*, akkor sem, ha K test. Ez azért van, mert a legtöbb polinomnak, például az $x \in K[x]$-nek nincs multiplikatív inverze (hiszen bármilyen polinommal is szorozzuk x-et, sosem kapunk egységelemet, ami egy konstans polinom – vagy másképpen: az $1/x$ nem polinom).

Példa. $\mathbb{Z}[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ és $\mathbb{C}[x]$ integritási tartomány, de egyik sem test.

Példa. $\mathbb{Z}_p[x]$, ahol p prímszám, szintén integritási tartomány, de nem test (hiába test a $\mathbb{Z}_p$).

3. Polinomok Sage-ben

Sage-ben többféleképpen is számolhatunk polinomokkal. A "naív" módszer az, hogy a Sage általános szimbolikus kifejezéseit használjuk:

```
sage: (2*x - 1)*(x^2 + 2)
(x^2 + 2)*(2*x - 1)
sage: expand(_)
2*x^3 - x^2 + 4*x - 2
sage: type(_)
<class 'sage.symbolic.expression.Expression'>
```

(Emlékeztető: `x` egy beépített *szimbolikus változó*, mintha `var("x")`-szel hoztuk volna létre, lásd a SageMath bevezetés c. jegyzetet.)

Ez így azonban kissé nehézkes (például szorzás után mindig `expand()` kell), és polinomokra nem a leghatékonyabb megoldás. Vannak azonban a Sage-ben kifejezetten polinomokra optimalizált struktúrák: `ZZ["x"]`, `QQ["x"]` stb., amelyek megfelelnek a matematikai $\mathbb{Z}[x]$-nek, $\mathbb{Q}[x]$-nek stb.:

```
sage: P = ZZ["x"]
sage: p = P(2*x - 1)    # szimbolikus kifejezés konvertálása polinommá
sage: p
2*x - 1
sage: q = P([2, 0, 1])  # polinom létrehozása együtthatókból (első a konstans tag)
sage: q
x^2 + 2
sage: p * q             # nem kell expand() (és sokkal gyorsabb)
2*x^3 - x^2 + 4*x - 2
sage: type(_)
<class 'sage.rings.polynomial.[...]'>
```

Vigyázat, itt `x` két különböző dolgot jelent: a beírt parancsokban `x` továbbra is egy szimbolikus változó (típusa: `Expression`), viszont a válaszokban `x` a polinomok változóját jelenti (típusa: polinom). Ezeket ne keverjük össze:

```
sage: p*(x^2 + 2)     # NE csináljuk! (polinom * szimbolikus kifejezés)
(x^2 + 2)*(2*x - 1)
sage: type(_)         # elrontottuk az optimalizált polinomot
<class 'sage.symbolic.expression.Expression'>
```

Megjegyzés: kissé leegyszerűsítve, a Sage a szimbolikus kifejezéseket műveletek sorozatával ábrázolja, például az x^2+2-t úgy, hogy "x-et emeljük négyzetre, és adjunk hozzá 2-t". Ez elég általános, de nehéz vele hatékonyan számolni. A `ZZ["x"]`-hez hasonló optimalizált polinomokat viszont az együtthatók sorozatával ábrázolja, pl. x^2+2-t úgy, hogy $2, 0, 1$. Ez sokkal hatékonyabb számítást tesz lehetővé (lásd a következő jegyzetet).

Hogy ne keverjük a szimbolikus kifejezésekel a polinomokkal, beállíthatjuk, hogy ezentúl az `x` is polinom típusú legyen:

```
sage: P = ZZ["x"]    # legyen P az egész polinomok halmaza
sage: x = P.gen()    # legyen x a P-beli polinomok változója
```

Sőt, van egy szintaxis, amellyel P-t és x-et egyszerre is beállíthatjuk:

```
sage: P.<x> = ZZ[]   # ugyanaz, mint: P = ZZ["x"]; x = P.gen()
sage: P
Univariate Polynomial Ring in x over Integer Ring
sage: type(x)              # x-et is felülírta
<class 'sage.rings.polynomial.[...]'>
sage: (2*x - 1)*(x^2 + 2)  # most már ezek is polinomok
2*x^3 - x^2 + 4*x - 2
```

Az együtthatók nemcsak számok lehetnek, például számolhatunk $\mathbb{Z}_5[x]$-ben is, azaz modulo 5:

```
sage: P.<x> = Zmod(5)[]
sage: p = 9*x^2 - 3*x + 33
sage: p
4*x^2 + 2*x + 3
sage: p + p
3*x^2 + 4*x + 1
```

Egy polinomnak le tudjuk kérdezni különböző tulajdonságait:

```
sage: P.<x> = ZZ[]
sage: p = 2*x^3 - 6*x + 4
sage: p.degree()
3
sage: p.list()     # együtthatók listája (konstans tagtól kezdve)
[4, -6, 0, 2]
sage: p[1]         # elsőfokú együttható
-6
sage: p.leading_coefficient()   # vagy: p.lc()
2
sage: p.constant_coefficient()  # vagy: p[0]
4
```

4. Gyökök

4.1. Definíció. Egy $p \in K[x]$ polinom c helyen felvett **helyettesítési értéke** az az érték, amelyet úgy kapunk, hogy p-ben x helyére c-t írunk, és elvégezzük a műveleteket. Jelölés: $p(c)$.

Példa. Ha $p = 2x^2 - 3x + 1$ és $c = 2$, akkor $p(2) = 2 \cdot 2^2 - 3 \cdot 2 + 1 = 3$.

Példa. Nem kell, hogy $c \in K$ legyen: ugyanezen $p = 2x^2 - 3x + 1 \in \mathbb{Z}[x]$ polinomot kiértékelhetjük a $c = 1/3 \notin \mathbb{Z}$ helyen is: $p(1/3) = 2 \cdot (1/3)^2 - 3 \cdot (1/3) + 1 = 2/9$.

4.2. Definíció. A c érték a $p \in K[x]$ polinom **gyöke** [*root*], ha $p(c) = 0$.

Példa. $c = 1$ egy gyöke a $p = 2x^2 - 3x + 1$ polinomnak, mert $p(1) = 2 \cdot 1^2 - 3 \cdot 1 + 1 = 0$.

Példa. Ugyanezen $p \in \mathbb{Z}[x]$ polinomnak gyöke a $c = 1/2 \notin \mathbb{Z}$ is: $p(1/2) = 2 \cdot (1/2)^2 - 3 \cdot (1/2) + 1 = 0$.

Példa. A $q = x^2 + 1 \in \mathbb{R}[x]$ polinomnak nincsenek valós gyökei, csak komplexek: $x_1 = i$ és $x_2 = -i$.

4.3. Tétel. *$c \in K$ akkor és csak akkor gyöke $p \in K[x]$-nek, ha $\exists q \in K[x] : p = (x-c)\,q$.*

Példa. A fenti $p = 2x^2 - 3x + 1$-nek gyöke $c = 1$, és valóban: $p = (x-1)(2x-1)$.

4.4. Definíció. A fenti tételben szereplő $x - c \in K[x]$ polinom a c-hez tartozó **gyöktényező**.

Vagyis c akkor és csak akkor gyöke p-nek, ha p-ből kiemelhető az $x - c$ gyöktényező.

Előfordulhat, hogy a kiemelés után kapott q polinomnak is gyöke ugyanaz a c. Ekkor q-ból is kiemelhető a gyöktényező: $q = (x-c)\,r$, vagyis $p = (x-c)^2\,r$, tehát p-ből többször is kiemelhető $x - c$. Ekkor azt mondjuk, hogy c **többszörös gyöke** p-nek, egészen pontosan:

4.5. Definíció. A $c \in K$ érték a $p \in K[x]$ polinom ***k*-szoros gyöke**, ha van olyan $q \in K[x]$, amellyel p felírható $p = (x-c)^k\,q$ alakban, de q-nak már nem gyöke a c. Azt is mondjuk, hogy ekkor a c gyök **multiplicitása** k.

Példa. A $p = 2x^3 - 6x + 4$ polinomnak kétszeres gyöke a $c = 1$, mert $p = (x-1)^2\,(2x+4)$, de $2x + 4$-nek már nem gyöke az 1.

Vagyis c egy k-szoros gyök, ha pontosan k-szor emelhető ki az $x - c$ gyöktényező.

A gyöktényezők kiemelhetőségéből következik egy nagyon fontos tétel:

4.6. Tétel. *Ha K integritási tartomány (például számgyűrű: $K = \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$), akkor egy n-edfokú $p \in K[x]\backslash\{0\}$ polinomnak legfeljebb n gyöke lehet K-ban. Ez igaz úgy is, ha a gyököket multiplicitással számoljuk, azaz a gyökök multiplicitásainak az összege is legfeljebb n.*

Példa. Egy harmadfokú valós polinomnak legfeljebb 3 gyöke lehet. És ha van egy kétszeres gyöke (mint a fenti p-nek a $c = 1$), akkor az "kétszer számít", azaz azonkívül már csak egy gyöke lehet.

(Bizonyítás: emeljünk ki annyi gyöktényezőt p-ből, amennyit csak lehet: $p = (x-c_1)(x-c_2)\cdots(x-c_m)\,q$, ahol q-nak már nincs gyöke. Mik lehetnek ennek a p-nek a gyökei? Ha $p(c) = 0$, akkor a szorzat valamelyik tényezője 0 (mert K integritási tartomány, azaz nullosztómentes). De a q nem lehet 0, mert annak nem volt gyöke, így csak valamelyik $(c - c_k)$ lehet 0, azaz a c gyök csak $c_1, c_2, \ldots, c_m$ valamelyike lehet. Ezekből viszont legfeljebb n lehet, mert $n = \deg p$, és minden kiemeléskor eggyel csökken a maradék fokszáma.)

Megjegyzés: a tételnek fontos feltétele, hogy K-ban ne legyen nullosztó (azaz integritási tartomány legyen, lásd a definíciót az előző jegyzetben). Ellenkező esetben lehet több gyöke is:

Példa. $\mathbb{Z}_6[x]$-ben (ahol vannak nullosztók: $\overline{2}\cdot\overline{3} = \overline{0}$) a $p = x^2 + x$ másodfokú polinomnak nem kettő, hanem *négy* gyöke van: $\overline{0}, \overline{2}, \overline{3}, \overline{5} \in \mathbb{Z}_6$.

Nézzünk néhány speciális esetet a gyökszámra vonatkozóan:

- Másodfokú polinomnak ($p = ax^2 + bx + c$) legfeljebb két gyöke lehet (két egyszeres, vagy egy kétszeres gyök), ahogy azt a megoldóképletből is tudjuk.
- Elsőfokú polinomnak, azaz egy $p = ax + b$ alakú polinomnak legfeljebb egy gyöke lehet (és csak egyszeres): $x = -b/a$ (azért "legfeljebb", mert $\mathbb{Z}$-ben ez az osztás nem mindig végezhető el).
- Nulladfokú polinomnak (azaz nemnulla konstans polinomnak, pl. $p = 5$) nincs gyöke.
- A nullpolinomnak ($p = 0$) viszont minden $c \in K$ érték gyöke (ezért kellett ezt kizárni a tételből).

Korábban megismertük a polinomok kanonikus alakját. Most nézzünk egy másik fontos alakot:

4.7. Definíció. Egy $p \in K[x]$ polinom **gyöktényezős alakja** a következő:

$$p = a(x - c_1)(x - c_2)\cdots(x - c_m),$$

ahol $a, c_1, c_2 \ldots, c_m \in K$ és $a \neq 0$.

Példa. A kanonikus alakban felírt $p = 2x^3 - 6x + 4$ polinom gyöktényezős alakja $p = 2(x-1)^2(x+2)$.

Ez az alak azért fontos, mert leolvasható belőle a polinom összes gyöke, multiplicitással együtt.

De gyöktényezős alak nem mindig létezik, csak ha a polinomnak van legalább n gyöke a K alaphalmazban (multiplicitással számolva). Ahhoz pedig, hogy *egyértelműen* létezzen (a sorrendtől eltekintve), *pontosan* n gyök kell. A fenti tétel csak annyit garantál, hogy *legfeljebb* n gyöke van, és azt is csak integritási tartomány fölött. Ráadásul az, hogy hány gyöke van, függ az alaphalmaztól:

Példa. A $p = 16x^4 - 1$ polinomnak

- $\mathbb{Z}$-ben nincs gyöke;
- $\mathbb{Q}$-ban és $\mathbb{R}$-ben két egyszeres gyöke van: $x_1 = 1/2$ és $x_2 = -1/2$;
- $\mathbb{C}$-ben pedig négy gyöke van: $x_1 = 1/2$, $x_2 = -1/2$, $x_3 = i/2$, $x_4 = -i/2$;

így tehát csak $\mathbb{C}$-ben van gyöktényezős alakja (és az a sorrendtől eltekintve egyértelmű):

$$p = 16(x - 1/2)(x + 1/2)(x - i/2)(x + i/2).$$

Példa. $\mathbb{Z}_6[x]$-ben, ami nem integritási tartomány, $p = x^2 + x$-nek négy gyöke van (lásd fent), és valóban, a gyöktényezős alak sem egyértelmű: $x^2 + x = (x - \overline{2})(x - \overline{3}) = x(x - \overline{5})$.

Az utolsó ezelőtti példában kitüntetett szerepe volt a komplex számok halmazának, $\mathbb{C}$-nek. A következő tétel azt mondja, hogy nemcsak itt, hanem *mindig* ilyen speciális a $\mathbb{C}$:

4.8. Tétel (Az algebra alaptétele)**.** *Minden n-edfokú $p \in \mathbb{C}[x] \setminus \{0\}$ polinomnak – multiplicitással számolva – pontosan n gyöke van $\mathbb{C}$-ben.*

Az algebra alaptétele tehát garantálja, hogy *bármely* komplex együtthatós (nemnulla) polinomnak egyértelműen létezik gyöktényezős alakja. (De annak előállítása általában nagyon nehéz feladat.)

Vigyázat: ne keverjük az **algebra** alaptételét a **számelmélet** alaptételével – ez utóbbi a számok prímtényezős felbontásának egyértelműségéről szólt, lásd az Osztók, prímszámok c. jegyzetet.

Sage-ben a `p.roots()` tagfüggvény számítja ki egy polinom gyökeit:

```
sage: P.<x> = ZZ[]
sage: p = 2*x^3 - 6*x + 4
sage: p.roots()
[(-2, 1), (1, 2)]    # a -2 egyszeres, az 1 kétszeres gyök
sage: p.roots(multiplicities=False)
[-2, 1]              # multiplicitások nélkül
sage: p(-2)          # ellenőrzés behelyettesítéssel
0
sage: p = 16*x^4 - 1
sage: p.roots()
[]                   # nincs egész gyöke
sage: p.roots(QQ)    # megadhatunk egy bővebb alaphalmazt is
[(1/2, 1), (-1/2, 1)]
sage: p.roots(QQ, multiplicities=False)
[1/2, -1/2]
sage: p.roots(RR)    # RR-ben a Sage csak közelítőleg tud számolni
[(-0.500000000000000, 1), (0.500000000000000, 1)]
sage: p.roots(CC)    # CC-ben is
[(-0.5000000000, 1), (0.5000000000, 1), (-0.5000000000*I, 1), (0.5000000000*I, 1)]
```

5. Lagrange-interpoláció

Az alábbiakban *test* fölötti polinomokról lesz szó (pl. $\mathbb{Q}$ vagy $\mathbb{R}$, de nem $\mathbb{Z}$, lásd az előző jegyzetet.)

Láttuk, hogy egy nemnulla n-edfokú polinomnak legfeljebb n gyöke lehet. Ez azt is jelenti, hogy ha egy *legfeljebb* n-edfokú polinomnak $n{+}1$ gyöke van, akkor az nem lehet más, csak a nullpolinom (0) (amelynek minden c gyöke). Ezt az állítást általánosíthatjuk gyökök helyett helyettesítési értékekre:

5.1. Tétel. *Ha két legfeljebb n-edfokú polinom $n{+}1$ helyen megegyezik, akkor a két polinom egyenlő.*

Példa. Ha p és q legfeljebb másodfokú polinomok, és három helyen megegyeznek: $p(1) = q(1)$, $p(2) = q(2)$ és $p(5) = q(5)$, akkor a tétel alapján $p = q$. Lineáris polinomokhoz két érték is elég (szemléletesen: két pont meghatároz egy egyenest), konstans polinomokhoz pedig egy is elegendő.

(A tétel bizonyítása nagyon egyszerű: vegyük a két polinom különbségét, ami a kérdéses $n{+}1$ helyen 0-t vesz fel, vagyis $n{+}1$ gyöke van, azaz csak a nullpolinom lehet.)

Tehát egy n-edfokú polinomot egyértelműen meghatározza $n{+}1$ helyettesítési értéke.

Most nézzük meg, hogyan számíthatjuk ki ezt az egyértelműen létező polinomot az $n{+}1$ értékből. Első lépésként nézzük azt a speciális esetet, amikor majdnem minden érték nulla, kivéve egyet. Például keressük meg azt a p másodfokú polinomot, amelyre $p(1) = 0$, $p(2) = 0$ és $p(5) = 8$. Az első két feltételt könnyű teljesíteni: $p := (x-1)(x-2)$. De a harmadik érték még nem jó: $p(5) = (5-1)(5-2) = 12 \neq 8$. Ezért szorozzuk meg a polinomot egy olyan c-vel, hogy $c \cdot p(5) = 8$ legyen, azaz $c := 8/p(5) = 8/12 = 2/3$, mert ez a gyököket nem változtatja meg, viszont a harmadik értéket "megjavítja". Tehát legyen inkább $p := 2/3 \cdot (x-1)(x-2) = 2x^2/3 - 2x + 4/3$.

De mi a helyzet, ha nincsenek nullák? Például melyik p másodfokú polinomra lesz $p(1) = 4$, $p(2) = 2$ és $p(5) = 8$? Ehhez alkalmazzuk a fenti módszert háromszor, és adjuk össze az eredményeket:

$$p_1(1) = 4,\ p_1(2) = 0,\ p_1(5) = 0 \implies p_1 = 4 \cdot \frac{(x-2)(x-5)}{(1-2)(1-5)} = x^2 - 7x + 10$$

$$p_2(1) = 0,\ p_2(2) = 2,\ p_2(5) = 0 \implies p_2 = 2 \cdot \frac{(x-1)(x-5)}{(2-1)(2-5)} = -\frac{2}{3}x^2 + 4x - \frac{10}{3}$$

$$p_3(1) = 0,\ p_3(2) = 0,\ p_3(5) = 8 \implies p_3 = 8 \cdot \frac{(x-1)(x-2)}{(5-1)(5-2)} = \frac{2}{3}x^2 - 2x + \frac{4}{3}$$

$$p(1) = 4,\quad p(2) = 2,\quad p(5) = 8 \implies p = p_1 + p_2 + p_3 \qquad = x^2 - 5x + 8$$

Ezt a módszert hívjuk **Lagrange-interpoláció**nak. Általában:

5.2. Tétel (Lagrange-interpoláció)**.** *Ha egy test fölötti legfeljebb n-edfokú p polinom $n{+}1$ különböző helyen adott $p(x_1) = y_1,\ p(x_2) = y_2,\ \ldots,\ p(x_{n+1}) = y_{n+1}$ értékeket vesz föl, akkor:*

$$p = \sum_{i=1}^{n+1} y_i \prod_{\substack{j=1 \\ j \neq i}}^{n+1} \frac{x - x_j}{x_i - x_j}.$$

Megjegyzés: azért kell test, hogy az osztásokat mindig el tudjuk végezni. Tehát pl. $\mathbb{Z}[x]$-ben nem működik az interpoláció, csak $\mathbb{Q}[x]$-ben, $\mathbb{R}[x]$-ben stb. Test fölött viszont *bármely* $x_1, \ldots, x_{n+1}$ és $y_1, \ldots, y_{n+1}$ értékekre egyértelműen létezik ilyen polinom (ha az x_i-k mind különbözőek).

A Lagrange-interpolációra a Sage-nek van egy beépített függvénye:

```
sage: P.<x> = QQ[]    # ZZ[] nem jó!
sage: P.lagrange_polynomial([(1,4), (2,2), (5,8)])
x^2 - 5*x + 8
```

6. Shamir-féle titokmegosztás

Tegyük fel, hogy van egy titkos információ (egy szám, például egy titkosításhoz használt kulcs), amelyet szeretnénk megosztani több ember között (például egy vállalat munkatársai között).

Ennek a legegyszerűbb módja, ha minden résztvevőnek odaadjuk a titkot. Ezzel persze az a probléma, hogy ha bármelyikük visszaél vele, vagy ellopják tőle, akkor az egész közös titok kompromittálódik. Jobb lenne egy olyan módszer, ahol külön-külön egyikük sem fér hozzá a titokhoz.

A másik véglet az, hogy a titkos információt egyenlő részekre osztjuk, és minden résztvevő kap egy-egy részt. Ekkor külön-külön egyikük sem tud visszaélni a saját részével – sőt, egy kisebb csoportjuk sem –, csak minden résztvevő együttes közreműködésével lehet hozzáférni a titokhoz. Ezzel viszont az a probléma, hogy ha bármelyikük elveszti a saját részét (vagy átmenetileg elérhetetlen), akkor a közös titkot nem lehet helyreállítani.

De van egy másik probléma is ezzel a módszerrel: bár semelyik résztvevő nem rendelkezik a *teljes* titokkal, de annak részeivel igen, így mégis közelebb vannak a titok megfejtéséhez. Például ha egy számzáras lakatnak négyszámjegyű kódja van, akkor aki semmit nem tud a kódról, annak $10^4 = 10000$ lehetőséget kell végigpróbálgatnia a kinyitásához (legrosszabb esetben); aki viszont ismeri a kód egyik számjegyét, annak már csak $10^3 = 1000$ lehetőséget kell végigpróbálnia, azaz tízszer gyorsabban tudja kinyitni; két számjegy ismeretében pedig százszor gyorsabb lesz.

Az ideális megoldás olyan lenne, hogy a titok helyreállításához az n résztvevőből k-ra van szükség (pl. ötből háromra); ha bármelyik k résztvevő jelen van, akkor vissza tudják állítani a titkot; de ha csak legfeljebb $k-1$ résztvevő van jelen, akkor nem tudják megfejteni, sőt, semennyivel nem kerülnek közelebb a megfejtéséhez, mint ha egyetlen résszel sem rendelkeznének.

Erre ad megoldás a **Shamir-féle titokmegosztás** [*Shamir's secret sharing (SSS)*].

Legyen n a résztvevők száma, amelyből k-ra lesz szükség a visszaállításhoz ($1 \leq k \leq n$). Legyen továbbá $S \in \mathbb{Z}$ a megosztandó titok, amit "elrejtünk" egy $k-1$-edfokú polinomba a következőképpen:

$$p = a_{k-1}x^{k-1} + \ldots + a_2x^2 + a_1x + S,$$

ahol a konstans tag az S titok, a többi együttható $(a_1, \ldots, a_{k-1})$ pedig véletlen egész számok. Ezt a polinomot kiértékeljük n különböző helyen, például $p(1), p(2), \ldots, p(n)$, és minden résztvevőnek adunk egyet-egyet (egy-egy (x_i, y_i) párt). Ekkor bármely k résztvevő a k helyettesítési értékből egyértelműen vissza tudja állítani a polinomot a Lagrange-interpoláció segítségével (lásd fent), és így megkapják a konstans tagját, S-et is. Viszont k-nál kevesebb résztvevő nem tudja visszaállítani a polinomot, hiszen a hiányzó értékeket bárhogy kitölthetik, mindig különböző polinomokat kapnak, tehát nem tudhatják, melyik volt az eredeti.

Példa. Legyen $n = 5$ résztvevő, amelyből $k = 3$ kell a visszaállításhoz. Legyen a titok az $S = 67$ érték, és generáljunk még két véletlen együtthatót, pl. $a_1 = 38$ és $a_2 = 13$, amelyből megkapjuk a következő másodfokú polinomot: $p = 13x^2 + 38x + 67$. Ezt értékeljük ki öt helyen:

$$p(1) = 118, \quad p(2) = 195, \quad p(3) = 298, \quad p(4) = 427, \quad p(5) = 582,$$

és mindenkinek adjunk egyet-egyet. Ekkor bármelyik három résztvevő vissza tudja állítani p-t, például az 1-es, a 2-es és az 5-ös a következőképpen (Lagrange-interpolációval, lásd fent):

$$p = 118 \cdot \frac{(x-2)(x-5)}{(1-2)(1-5)} + 195 \cdot \frac{(x-1)(x-5)}{(2-1)(2-5)} + 582 \cdot \frac{(x-1)(x-2)}{(5-1)(5-2)} = 13x^2 + 38x + 67.$$

Valójában azonban nincs szükség a teljes p polinomra, csak a konstans tagjára, S-re, amely megegyezik a $p(0)$ helyettesítési értékkel, ezért azt sokkal gyorsabban is ki lehet számítani:

$$S = p(0) = 118 \cdot \frac{(-2)(-5)}{(1-2)(1-5)} + 195 \cdot \frac{(-1)(-5)}{(2-1)(2-5)} + 582 \cdot \frac{(-1)(-2)}{(5-1)(5-2)} = 67.$$

Azonban a fent vázolt módszerrel ebben a formában még van egy probléma. Ez abból adódik, hogy egész számokkal számoltunk, pedig a Lagrange-interpolációnál kikötöttük, hogy ahhoz test kell.

Ez nemcsak egy elvi probléma, hanem konkrét támadást is lehetővé tesz! Tegyük fel, hogy a fenti példában az ötből két résztvevő összefog. Ők ugyan a teljes titkot nem tudják kiszámítani (ahhoz hárman kellenének), de ha ügyesek, akkor annak bizonyos tulajdonságait mégis. Ugyanis a két értékükből, pl. $p(1)$-ből és $p(5)$-ből, és abból, hogy egy $p = ax^2 + bx + S$ alakú polinomról van szó, ahol $a, b \in \mathbb{Z}$, a következőket tudják levezetni:

$$\begin{aligned} p(5) &= 25a + 5b + S = 582 \\ p(1) &= a + b + S = 118 \\ p(5) - p(1) &= 24a + 4b = 464 \quad \Longrightarrow \quad b = 116 - 6a \\ \Longrightarrow \quad p(1) &= a + (116 - 6a) + S = 118 \quad \Longrightarrow \quad S = 5a + 2. \end{aligned}$$

Vagyis megtudták, hogy a titkos érték 5-tel osztva 2-t ad maradékul, azaz $S \equiv 2 \pmod 5$. Ha tehát meg akarják találni S-et, akkor csak ötödannyi lehetőséget kell végigpróbálniuk.

Ezt a trükköt az tette lehetővé, hogy az együtthatók egész számok, ahol az osztás nem mindig végezhető el. Ha racionális számok lennének, akkor a fenti $S = 5a + 2$ összefüggésből semmi nem derülne ki S-ről, hiszen bármilyen S-re létezne olyan $a \in \mathbb{Q}$, amely kielégíti (nevezetesen: $a = (S - 2)/5$).

Akkor miért nem használunk racionális számokat együtthatóknak? Ez számos egyéb okból nem lenne praktikus: egyrészt kényelmetlen velük számolni, másrészt a titok tipikusan egész szám, harmadrészt a véletlenszám-generálás is problémás (egyáltalán milyen eloszlást használnánk?).

A gyakorlatban a Shamir-féle titokmegosztást $\mathbb{Z}_p[x]$-ben szokták végezni, ahol p egy olyan nagy prímszám, amelybe belefér S, a titok. (A $\mathbb{Z}_p$-ről az előző jegyzetben láttuk, hogy prímszám modulusra testet alkot, azaz az osztás mindig elvégezhető.)

Példa. Legyen továbbra is $n = 5$, $k = 3$ és $S = 67$, és generáljunk ismét egy másodfokú polinomot, de most nem $\mathbb{Z}[x]$-ben, hanem $\mathbb{Z}_{89}[x]$-ben:

$$p = \overline{13}x^2 + \overline{38}x + \overline{67} \in \mathbb{Z}_{89}[x].$$

Ekkor az öt helyettesítési érték a következő (ugyanazok, mint fent, csak modulo 89):

$$p(\overline{1}) = \overline{29}, \quad p(\overline{2}) = \overline{17}, \quad p(\overline{3}) = \overline{31}, \quad p(\overline{4}) = \overline{71}, \quad p(\overline{5}) = \overline{48}.$$

A visszaállítás is ugyanúgy történik, csak most $\mathbb{Q}$ helyett $\mathbb{Z}_{89}$-ben kell számolni. Például $p(1)$-ből, $p(2)$-ből és $p(5)$-ből a következőképpen:

$$\begin{aligned} S &= \overline{29} \cdot \frac{(-\overline{2})(-\overline{5})}{(\overline{1} - \overline{2})(\overline{1} - \overline{5})} + \overline{17} \cdot \frac{(-\overline{1})(-\overline{5})}{(\overline{2} - \overline{1})(\overline{2} - \overline{5})} + \overline{48} \cdot \frac{(-\overline{1})(-\overline{2})}{(\overline{5} - \overline{1})(\overline{5} - \overline{2})} = \\ &= \overline{29} \cdot \overline{10} \cdot \overline{4}^{-1} + \overline{17} \cdot \overline{5} \cdot \overline{86}^{-1} + \overline{48} \cdot \overline{2} \cdot \overline{12}^{-1} = \overline{28} + \overline{31} + \overline{8} = \overline{67}. \end{aligned}$$

Mivel $\mathbb{Z}_p$ test, ezért a fent leírt támadás itt nem működik: bár itt is kijön, hogy $S = \overline{5}a + \overline{2}$, de itt ez semmit nem árul el S-ről, hiszen az $5a \equiv S - 2 \pmod{89}$ lineáris kongruencia bármely S esetén megoldható (lásd: Kongruenciák). A $\mathbb{Z}_p$ előnye továbbá, hogy abban a véletlenszám-generálás is triviális, hiszen $\mathbb{Z}_p$-nek véges sok eleme van.

7. Szerző

Ezt a jegyzetet Uray M. János írta, részben felhasználva az alábbi forrásokat:

[1] https://compalg.elte.gitlab-pages.hu/dimoa-web/tematika/dimoa

[2] https://en.wikipedia.org/wiki/Polynomial

[3] https://en.wikipedia.org/wiki/Lagrange_polynomial

[4] https://en.wikipedia.org/wiki/Shamir%27s_secret_sharing

[5] A. Shamir (1979): How to share a secret. *Communications of the ACM*, 22 (11), pp. 612–613. https://dl.acm.org/doi/10.1145/359168.359176

Hibákat, észrevételeket itt lehet jelezni: uray.janos@inf.elte.hu.