

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 polinomot* 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.

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 $\sqrt{2}x + 3/2 \notin \mathbb{Z}[x]$.

Ebben a jegyzetben K valamelyik számhalmazt jelöli: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$. (Később majd általánosítjuk.)

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:

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

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

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

Egy polinomot kanonikus alakra hozhatunk, ha a zárójeleket felbontjuk, a tagokon belüli szorzásokat végrehajtjuk (pl. $x \cdot 2x \cdot 3 = 6x^2$), az azonos kitevőjű tagokat összevonjuk, és a tagokat kitevő szerint csökkenő sorrendbe rendezzük.

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, 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 kitöltöttük, 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, például a lenti 1.7 Tétel. 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.

1.7. Tétel (fokszám változása műveletvégzéskor). Ha $p, q \in K[x]$, akkor:

1. $\deg(p + q) \leq \max(\deg p, \deg q)$ (és egyenlőség van, ha $\deg p \neq \deg q$);
2. $\deg(p - q) \leq \max(\deg p, \deg q)$ (és egyenlőség van, ha $\deg p \neq \deg q$);
3. $\deg(p \cdot q) = \deg p + \deg q$.

Példa. Ha $p = 2x - 1$ és $q = x^2 + 2$, akkor $\deg p = 1$ és $\deg q = 2$, és valóban:

- $p + q = x^2 + 2x + 1$, így $\deg(p + q) = 2 = \max(1, 2)$,
- $p \cdot q = 2x^3 - x^2 + 4x - 2$, így $\deg(p \cdot q) = 3 = 1 + 2$.

(Megjegyzés: ezek a nullpolinomra is teljesülnek, például $0 \cdot x^2 = 0$, és valóban, a fokszámokra $-\infty + 2 = -\infty$.)

2. Polinomok Sage-ben

Polinomokra egyrészt használhatjuk a Sage általános szimbolikus kifejezéseit:

```
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*, 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: ha x -et írunk, az továbbra is szimbolikus változó, ezeket ne keverjük a polinomokkal:

```
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 $\mathbb{Z}\mathbb{Z}["x"]$ -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.

Hogy ne keverjük a kétféle x -et, beállíthatjuk, hogy x ezentúl polinom típusú legyen:

```
sage: P = ZZ["x"]    # legyen P 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
sage: var("x")       # x visszaállítása
sage: type(x)
<class 'sage.symbolic.expression.Expression'>
```

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
```

3. Helyettesítési érték

3.1. 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 $p = x^2 - 3x + 5$ és $c = 2$, akkor $p(2) = 2^2 - 3 \cdot 2 + 5 = 3$.

Példa. Nem kell, hogy $c \in K$ legyen: ugyanezen $p = x^2 - 3x + 5 \in \mathbb{Z}[x]$ polinomot kiértékelhetjük a $c = 1/2 \notin \mathbb{Z}$ helyen is: $p(1/2) = (1/2)^2 - 3 \cdot (1/2) + 5 = 15/4$.

A helyettesítési értéket kiszámíthatjuk a kanonikus alakból, azaz a $p(c) = a_n c^n + \dots + a_1 c + a_0$ felírásból – de ez nem egy hatékony módszer: az $a_n c^n$ -hez n szorzás kell, az $a_{n-1} c^{n-1}$ -hez $n-1$ stb., ami összesen $n + (n-1) + \dots + 2 + 1 = n(n+1)/2$ szorzás, és kell még n összeadás. (Ez például egy tizedfokú polinomra 55 szorzást és 10 összeadást jelent.)

Ezt javíthatjuk úgy, ha jobbról balra számolunk, és mindig megjegyezzük az utolsó c^k értéket, mert akkor a következő c^{k+1} -hez már csak plusz egy szorzás kell: $c^{k+1} = c^k \cdot c$. Így összesen csak $2n-1$ szorzás és n összeadás kell (ami tizedfokú polinomra 19 szorzás és 10 összeadás).

Ennél is hatékonyabb a **Horner-módszer** (vagy *Horner-elrendezés*), amely a polinomot kiemelések sorozatával olyan alakra hozza, amelyből nagyon hatékonyan lehet kiértékelni. Például:

$$\begin{aligned} p &= 2x^4 + 3x^3 - 2x^2 - 4x + 3 = \\ &= (2x^3 + 3x^2 - 2x - 4)x + 3 = \\ &= ((2x^2 + 3x - 2)x - 4)x + 3 = \\ &= (((2x + 3)x - 2)x - 4)x + 3. \end{aligned}$$

Vagyis minden lépésben kiemelünk x -et azokból a tagokból, amelyekből lehet, és ezt addig folytatjuk, amíg minden kitevő el nem tűnik. Általában ez a következő átírást jelenti:

$$\begin{aligned} p &= a_n x^n + a_{n-1} x^{n-1} + a_{n-2} x^{n-2} + \dots + a_2 x^2 + a_1 x + a_0 = \\ &= ((\dots ((a_n x + a_{n-1})x + a_{n-2})x + \dots + a_2)x + a_1)x + a_0. \end{aligned}$$

Ebből a felírásból a behelyettesítés hatékonyan elvégezhető: minden lépésben megszorozzuk az egyik zárójeles kifejezést (legelőször a_n -et) x -szel (vagyis c -vel), majd ehhez hozzáadjuk a következő együtthatót, és így megkapjuk a következő zárójeles kifejezést; ezt folytatva a legvégén eljutunk a teljes helyettesítési értékhez. Ehhez tehát összesen csak n szorzás és n összeadás kell.

Horner-módszer:

Bemenet: a polinom $a_0, a_1, \dots, a_n$ együtthatói és a c érték

$b := a_n$

ciklus $k = n-1$ -től 0-ig

$b := b \cdot c + a_k$

Kimenet: b

Itt b menet közben a fenti felírás egy-egy zárójeles részkifejezését jelenti, például az első lépés után $b = a_n c + a_{n-1}$, aztán $b = (a_n c + a_{n-1})c + a_{n-2}$ stb.

(Megjegyzés: a nullpolinomra így ez az algoritmus nem működik, mert annak nincsenek együtthatói. Ezt megoldhatjuk úgy, ha egyetlen nulla együtthatót adunk meg: $n = 0$ és $a_0 = 0$. Az algoritmushoz ugyanis nem kötelező, hogy $a_n \neq 0$ legyen, azaz lehetnek fölösleges 0-k az együtthatólista végén.)

A helyettesítési értéket Sage-ben a matematikailag hasonló zárójeles jelöléssel számíthatjuk ki, pl. $p(2)$, ahol p egy Sage polinom. (És egyébként a Sage is a Horner-módszert használja.)

4. Gyökök

4.1. 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. Itt sem kell, hogy $c \in K$ legyen: ugyanennek a $p \in \mathbb{Z}[x]$ 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 $x_2 = -i$.

4.2. 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: $p = (x - 1)(2x - 1)$.

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

Vagyis a fenti tételt úgy is megfogalmazhatjuk, hogy c akkor és csak akkor gyöke p -nek, ha p -ből kiemelhető a c -hez tartozó 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:

4.4. Definíció. $c \in K$ a $p \in K[x]$ polinom **k -szoros gyöke**, ha $\exists q \in K[x]$, hogy $p = (x - c)^k q$, 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:

4.5. Tétel. Egy n -edfokú $p \in K[x] \setminus \{0\}$ 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 polinomnak legfeljebb 3 gyöke lehet. Sőt, 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. Ekkor p -nek nem lehet más gyöke, mint $c_1, c_2, \dots, c_m$, mert ha $p(c) = 0$, akkor valamelyik tényező 0, azaz vagy valamelyik $c_i = c$, vagy q -nak mégis lenne gyöke. Viszont minden kiemeléskor csökken a maradék fokszáma, ezért legfeljebb $n = \deg p$ gyöktényező lehet, vagyis legfeljebb n gyök.)

Néhány speciális eset:

- 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).

Fent megismertük a polinomok kanonikus alakját. A gyöktényezők segítségével definiálhatunk egy másik fontos alakot:

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

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

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

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

Ennek az alaknak az a jelentősége, hogy leolvasható belőle a polinom összes gyöke, multiplicitással együtt. (És vegyük észre, hogy a konstans szorzó, $a = 2$ éppen a polinom főegyütthatója.)

Viszont gyöktényezős alak nem mindig létezik. Ehhez ugyanis az kell, hogy a polinomnak az alaphalmazon, K -ban pontosan n gyöke legyen (multiplicitással számolva). A fenti tétel viszont csak azt garantálja, hogy *legfeljebb* n gyöke lehet. Ráadásul az, hogy hány gyöke van, függ az alaphalmaztól, K -tól:

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:

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

A fenti példában tehát kitüntetett szerepe van a komplex számok halmazának, $\mathbb{C}$ -nek. De a következő tétel azt mondja, hogy nemcsak a fenti példában, hanem *mindig* ilyen kitüntetett a $\mathbb{C}$:

4.7. 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 van gyöktényezős alakja. (De annak előállítását általában egy rendkívül nehéz feladat.)

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

Sage-ben egy polinom gyökeit a `roots()` tagfüggvénnyel kereshetjük meg:

```
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 = 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(RR)      # RR-ben a Sage csak közelítőleg tud számolni
[(-0.5000000000000000, 1), (0.5000000000000000, 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

Tudjuk, 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, az ezen az $n+1$ 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:

$$\begin{aligned} p_1(1) = 4, \quad p_1(2) = 0, \quad p_1(5) = 0 &\implies p_1 = 4 \cdot \frac{(x-2)(x-5)}{(1-2)(1-5)} = x^2 - 7x + 10 \\ p_2(1) = 0, \quad p_2(2) = 2, \quad p_2(5) = 0 &\implies p_2 = 2 \cdot \frac{(x-1)(x-5)}{(2-1)(2-5)} = -\frac{2}{3}x^2 + 4x - \frac{10}{3} \\ p_3(1) = 0, \quad p_3(2) = 0, \quad p_3(5) = 8 &\implies p_3 = 8 \cdot \frac{(x-1)(x-2)}{(5-1)(5-2)} = \frac{2}{3}x^2 - 2x + \frac{4}{3} \end{aligned}$$

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

Ezt a módszert hívjuk **Lagrange-interpolációnak**. Általában:

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

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

Az osztások miatt $\mathbb{Z}[x]$ -ben nem működik az interpoláció (például fent is törtekkel kellett számolni), csak $\mathbb{Q}[x]$ -ben, $\mathbb{R}[x]$ -ben stb. Akkor viszont *bármely* $x_1, \dots, x_{n+1}$ és $y_1, \dots, y_{n+1}$ értékekre egyértelműen létezik ilyen polinom (ha 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 (SSS)

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 végtet 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 számszörös lakatnak négy számjegyjű kódja van, akkor aki semmit nem tud a kódról, annak $10^4 = 10000$ lehetőséget kell végigpróbálgatnia a kinyitáshoz (legrosszabb esetben). Ha viszont valaki ismeri a kód egyik számjegyét, akkor neki 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, ahol 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 nemhogy a teljes titkot nem tudják megszerezni, de semennyivel nem kerülnek közelebb a megfejtéséhez, mint ha egyetlen résszel sem rendelkeznének.

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

Megjegyzés: az alábbiakban leírt megoldás ebben a formában még nem teljesen biztonságos, de így könnyebben érthető; a javított változatot majd csak a következő jegyzetben tudjuk megadni.

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:

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

ahol a konstans tag az S titok, a többi együttható ($a_1, \dots, a_{k-1}$) pedig véletlen egész számok. Ezt a polinomot kiértékeljük n különböző helyen, például $p(1), p(2), \dots, p(n)$, és minden résztvevőnek adunk egyet-egyét (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.

Például 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-egyét. 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:

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

6.1. Probléma a titokmegosztással

A fentiekben vázolt módszerrel azonban még mindig van egy probléma: ha két résztvevő összefog, akkor ugyan a teljes titkot nem, de annak bizonyos tulajdonságait ki tudják számítani. 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:

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

Vagyis megtudták, hogy a titkos érték 5-tel osztva 2-t ad maradékkal, azaz $S \equiv 2 \pmod{5}$, tehát ha meg akarják fejteni S -et, akkor csak ötödannyi lehetőséget kell végigpróbálniuk.

A probléma abból adódik, hogy az együtthatók egész számok, ahol az osztás nem mindig végezhető el. Ha ugyanis tetszőleges racionális számok lennének, akkor a fenti $S = 5a + 2$ összefüggésből semmit nem tudnánk meg S -ről, hiszen bármilyen S -re létezne olyan $a \in \mathbb{Q}$, amelyre ez az összefüggés fennáll: $a = (S - 2)/5$. Mivel azonban $\mathbb{Z}$ -ben ez az osztás nem mindig végezhető el, ezért ott ezzel szűkíteni lehet a lehetőségek halmazát.

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

Amire szükségünk lenne, az egy olyan "struktúra", amelyben az osztás mindig elvégezhető, mint $\mathbb{Q}$ -ban, de amelyben könnyű számolni (és véletlen számokat generálni), mint $\mathbb{Z}$ -ben. Erre fogunk megoldást adni a következő jegyzetben.

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.