KOMBINATORIKA ElŐADÁS
Matematika BSc hallgatók számára

Polinomok, k elemű részhalmazok

Előadó: Hajnal Péter 2017.

1. k elemű részhalmazok száma

Egy n elemű halmaznak hány k elemű részhalmaza van?

Középiskolás nyelvezettel: Adott n különböző tárgy, amelyből egy k tárgyat tartalmazó csomagot állítunk össze. Hányféleképpen tehetjük ezt meg? A csomag szerepe a kérdésben az, hogy kódolja hogy a kiválasztás sorrendje lényegtelen. Néha ezt hangsúlyozzák is. Az absztrakt, részhalmazos nyelvezet ezt a fontos feltételt magában foglalja, egy halmaz elemeinek nincs sorrendje ($\{a, b, c\} = \{a, c, b\} = \{c, b, a\}$).

Mint az összes részhalmaz megszámolásánál most is meg kell győződnünk, hogy kérdésünk korrekt-e, azaz egy halmaz részhalmazainak száma „csupán" elemszámától függ-e. Két A és B azonos elemszámú halmaz elemei között létesítsünk egy $\phi : A \to B$ párbaállító leképezést. Mint láttuk ez a leképezés természetes módon hozzárendel minden A-beli részhalmazhoz egy B-beli részhalmazt mint párt. Azt kell észrevennünk, hogy minden részhalmaz azonos elemszámú párjával. Így a fenti leképezést megszorítva A adott (k) elemű részhalmazaira egy párbaállító leképezést kapunk A k elemű részhalmazai és B k elemű részhalmazai között.

Definíció. Egy n elemű halmaz k elemű részhalmazainak számát $\binom{n}{k}$-val jelöljük.

Megjegyzeeük, hogy $\binom{n}{k}$ számok minden n, k természetes számra értelmezettek. Például $\binom{1024}{2015} = 0$, hiszen egy 1024 elemű halmaznak nincs 2015 elemű részhalmaza. $\binom{n}{k}$ pontosan akkor nem-nulla/pozitív, ha $0 \leq k \leq n$.

2. Polinomok

Az $x^2 + x - 7$, $x^3 - 2x^2 + 3x - 7$ alakú kifejezések megszokottak matematikai tanulmányaink során. Ezeket polinomoknak nevezzük. A szó görög eredetű, eredeti jelentése „több tag". A *polinom* a matematikában szakkifejezéssé vált, magyarul *többtagúnak* nevezzük. A polinomokkal kapcsolatos alapismereteket az alábbiakban összefoglaljuk és pontosítjuk.

A „többtagú" jelentése: egy polinom egyszerűbb elemekből van összerakva. Ezek az egyszerűbb alkotó elemek az úgynevezett *egytagúak*, idegen szóval *monomok*. A polinomokban ilyen monomokat kötünk össze „+" jelek segítségével.

Példa. A $P = 5 - 3x + 2x^3$ polinom az 5, $(-3)x$ és $2x^3$ monomok összege.

Példa. A $Q = x^2 + x^3 + x^5 + x^7 + x^{11}$ polinom az x^2, x^3, x^5, x^7 és x^{11} monomok összege.

Egy monom egy szám – amit a *monom együtthatójának* nevezünk – és egy betűs hatvány szorzata. A betű kitevője a *monom foka*, vagy a *monom típusa*. Két monom, akkor ugyanaz, ha típusuk (azaz kitevőjük) és együtthatójuk is ugyanaz.

Megjegyzés. Az eddigi példánk mindegyike egyetlen betűt használt, de vannak „több betűre épülő polinomok” is. Ezekben a monomokban az együttható mellett a különböző betűk hatványainak szorzata van.

A fentiek után azt mondhatjuk, hogy egy polinom különböző típusú monomok összege.

Érdemes néhány egyszerűsítő megállapodást megfogalmaznunk. A fenti definícióknak eleget tevő polinom például $5x^0 + 2x^3 + (-3)x^1$. A polinomok ismerősei számára világos, hogy ez ugyanaz, mint az első példában szereplő $5 - 3x + 2x^3$ polinom. Az x^1 betűs hatványt x-nek, az $5x^0$ monomot 5-nek írtuk és a -3 együttható „zárójelét felbontottuk” és a monomok sorrendjét felcseréltük. A fentiekkel egyező polinom $2x^3 + 0x^2 - 3x + 5$, azaz a 0 együtthatós tagok elhagyhatók (illetve beszúrhatók). Ezekhez a jelölésekhez mindenki hozzászokott (amennyiben most kezd a polinomok tanulmányozásához, akkor hozzá kell szoknia).

A fentiek után azt mondhatjuk, hogy két polinom egyenlő, ha 0 együtthatós tagjainak elhagyása után mindkettő ugyanazoknak a monomoknak az összege. Hogy polinomok egyenlősége könnyen ellenőrizhető legyen, a polinomokat jól megállapított szabályok szerint írjuk le (ezt a következetesség is kívánja): a monomokat a kitevőjük nagysága szerint rendezzük. A nagyság szerinti sorrend kétféle lehet (növekvő vagy csökkenő), ennek megfelelően kétféle megállapodás is lehetséges. Mi a kitevők növekvő sorrendje mellett döntöttünk. Ennek megfelelően egy x betűt használó polinom általános alakja

$$a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} + a_nx^n.$$

(Mivel 0 együtthatós monomok a polinomhoz hozzáadhatók, illetve belőlük elhagyhatók, ezért feltehetjük, hogy a kitevők 0-tól n-ig nőnek és $a_n \neq 0$.)

A polinomok azonosíthatók együtthatóik sorozatával:

$$\begin{aligned} p \equiv (&p \text{ konstans tagja, } p \text{ lineáris/első fokú tagjának együtthatója,}\\ &p \text{ kvadratikus/négyzetes tagjának együtthatója,}\\ &p \text{ kubikus/köbös/harmadfokú tagjának együtthatója,} \ldots). \end{aligned}$$

Így a polinomok felfoghatók úgy mint végtelen számsorozatok, amelyeknek egy idő után minden eleme 0. Matematikailag talán ez a „legtisztább”, probléma mentesebb leírás, de ez egy lényeges távolodás (absztrakció) a minden napi gyakorlattól.

⋆

A továbbiakban bevezethetjük a polinomok helyettesítési értékét, definiálhatnánk a polinom-függvényt. Továbbá az analízisben megismert fogalmakat alkalmazhatnánk polinomokra. Polinom-függvényeket, függvényként összeadhatunk, szorozhatunk, oszthatunk. Az összeg és a szorzat szintén egy polinom által leírható függvény lesz. A hányados vétele már kivezethet a polinomok köréből. Ezt az utat úgy írhatjuk le, mint a polinomok analitikus vizsgálata. Mi nem ezt az utat követjük.

A polinomok alapműveleteit bevezethetjük másképpen is. Leírjuk, hogy két polinom összege, ami egy polinom lesz milyen együttható sorozata lesz a két összeadandó együttható sorozatától függően. Így anélkül, hogy tudnánk két polinom által jelentett két függvényt fel tudjuk írni az összegpolinomot. Hasonlóan cselekedhetünk a szorzásnál is. Ezt az utat szokátk formális, vagy algebrai szemléletnek nevezni. Mi ezt követjük.

A két szemlélet közül egyik sem magassabb rendű a másiknál. Jól kiegészítik egymást és különböző kérdéseknél mindegyiknek meg lehet a maga előnye. Mi azért választottuk az algebrai tárgyalást mert ez ad lehetőséget, hogy egy harmadik szemel'elt módot is megmutassunk. Ez a kombinatorikus szemlélet mód.

Célunk nem az, hogy egy matematikailag pontos bevezetést adjunk. Feltesszük, hogy az olvasó már ismeri a polinomokat, dolgozott polinomokkal. Szeretnénk tudatosítani a munka alatt felmerült és talán ki nem mondott problémákat.

$\star \quad \star \quad \star$

Két polinom összegében egy adott típusú monom együtthatója az összeadás egy-egy tagjában szereplő megfelelő típusú tagok együtthatóinak összege. Eddig az együtthatókról nem említettünk semmit, azon túl, hogy azok számok. Mi általában valós számokat használunk együtthatóként. A fentiek alapján a polinomokat akkor tudunk összeadni, ha az együtthatóikat össze tudjuk adni. Azt is mondhatjuk, hogy a polinomok összeadását visszavezetjük az együtthatók összeadására.

Példa. $(2x^3 - 3x + 5) + (-x^2 + 3x + 2) = (5x^0 + (-3)x^1 + 0x^2 + 2x^3) + (2x^0 + 3x^1 + (-1)x^2 + 0x^3) = (5 + 2) + ((-3) + 3)x + (0 + (-1))x^2 + (2 + 0)x^3 = 7 - x^2 + 2x^3$.

$\star$

A szorzás definíciója előtt először definiáljuk a *monomok szorzatát.* Az αx^i és βx^j monom szorzata is egy monom lesz, együtthatója $\alpha \cdot \beta$ és kitevője $i+j$. Ezekután *két polinom szorzatát* úgy számoljuk ki, hogy mindegyikből kiveszünk egy-egy monomot, ezeket összeszorozzuk, majd az összes lehetséges módon nyert szorzat monomokat összeadjuk (összegyűjtjük).

Példa. $(5 - 3x + 2x^3) \cdot (2 + 3x - x^2) = (5)(2) + (5)(3x) + (5)(-x^2) + (-3x)(2) + (-3x)(3x) + (-3x)(-x^2) + (2x^3)(2) + (2x^3)(3x) + (2x^3)(-x^2) = (10) + (15x) + (-5x^2) + (-6x) + (-9x^2) + (3x^3) + (4x^3) + (6x^4) + (-2x^5) = 10 + 9x - 14x^2 + 7x^3 + 6x^4 - 2x^5$.

$\star \quad \star \quad \star$

Tegyük fel, hogy a P polinom egyetlen határozatlant használ, x-et. Ekkor $[x^i]P$ az i típusú monom együtthatója P-ben. Ha P az első példában szereplő polinom, akkor $[x^2]P = 2$. Ha P leírásában ilyen típusú monom nem szerepel, akkor a megfelelő együttható értékét 0-nak vesszük. Így $[x^i]P$ minden i természetes számra értelmezve van. Mivel egy P polinomban véges sok nem nulla együtthatójú monom szerepel ezért az $[x^i]P$ $(i = 1, 2, \ldots)$ sorozat egy idő után azonosan 0 értéket vesz fel.

Két polinom egyenlőségét a következőképpen fogalmazhatjuk meg: P és Q polinomok egyenlők, ha minden i természetes számra $[x^i]P = [x^i]Q$. Ezt úgy is kifejezhetjük, hogy egy polinom azonosítható együtthatóinak sorozatával.

Egy P polinom *fokszáma* $\deg P = \max\{i : [x^i]P \neq 0\}$.

⋆

Ha polinomokkal dolgozunk, meg kell adnunk, hogy milyen számok lehetnek az együtthatók és milyen határozatlant vagy határozatlanokat használunk.

Matematikai tanulmányaink alatt az általános és középiskolában mindenki találkozik az egész számokkal, racionális számokkal, valós számokkal. Egyetemen, illetve más tanulmányok során komplex számokkal, kvaterniókkal, oktánokkal, p-adikus számokkal, Gauss egészekkel, algebrai számokkal, $\bmod p$ számokkal is találkozhatunk. $0, 1, 2$ felfogható mint egész szám és felfogható mint $\bmod 3$ szám. A $1 + 2 = 0$ egyenlőség $\bmod 3$ számolva helyes, míg a benne szereplő számokat egészeknek fogva fel az egyenlőség természetesen nem igaz. Láttuk, hogy az együtthatók közötti számolási szabályok fontosak. Ezekre építve definiáljuk a polinomokkal való számolási szabályokat is.

Az első példában P egy x határozatlanú, egész együtthatós polinom. Ezt úgy jelöljük, hogy $P \in \mathbb{Z}[x]$. $\mathbb{Z}[x]$ az x határozatlanú, egész együtthatós polinomokat tartalmazza. Tehát az együtthatók leírása után ($\mathbb{Z}$ az egész számok szokásos jelölése) egy szögletes zárójelben a határozatlant tüntetjük fel. Ha tehát $P \in \mathbb{Z}[x]$, akkor $[x^2]P$ egy egész szám. $R = -\frac{1}{3} + \frac{1}{2}y^2 \in \mathbb{Q}[y]$, azaz az R polinomban y a határozatlan és az együtthatók racionálisak. $S = \pi + \sqrt{2}x^3 \in \mathbb{R}[x]$, azaz az S polinomban x a határozatlan és az együtthatók valósak.

Megjegyezzük, hogy gyakran választásunk van arra, hogy az együtthatók milyen algebrai struktúrából kerülnek ki. Egy egész együtthatós polinom felfogható valós vagy komplex együtthatós polinomként is. Az együtthatókkal való alapműveletek értéke nem függ attól, hogy valós, komplex vagy „csak” egész számoknak tekintjük őket. Figyelnünk kell azonban arra, hogy milyen kérdést vizsgálunk. A válasz függhet attól, hogy milyen együtthatókat engedünk meg. Erre egy példa lehet másodfokú polinomok faktorizációja: Ha $1 + x^2$-t $\mathbb{R}[x]$ egy elemének tekintjük, akkor azt nem írhatjuk fel két ($\mathbb{R}[x]$-beli) elsőfokú polinom szorzataként; ha $1 + x^2$-t $\mathbb{C}[x]$ egy elemének tekintjük, akkor $1 + x^2 = (i + x)(-i + x)$.

A továbbiakban csak valós együtthatós polinomokkal foglalkozunk.

⋆

Új jelöléseinkkel írjuk le a polinomok összegének és szorzatának definícióját.

Legyen $P, Q \in \mathbb{R}[x]$ két polinom. Összegük $P + Q$. Ahhoz, hogy ezt definiáljuk meg kell mondanunk, hogy mik $P+Q$ együtthatói. Az ismert definíciót jelöléseinkkel a következőképpen formalizálhatjuk:

$$[x^n](P + Q) = [x^n]P + [x^n]Q.$$

A két polinom szorzata $P \cdot Q$. A szorzatot a következő formula definiálja:

$$[x^n](P \cdot Q) = \sum_{i+j=n} [x^i]P \cdot [x^j]Q.$$

Az összegzésben természetesen i és j természetes számok.

⋆ ⋆ ⋆

Az összadás és szorzás kommutatív, asszociatív és disztributív. Azaz $P, Q \in \mathbb{R}[x]$ esetén $P+Q = Q+P$, $(P+Q)+R = P+(Q+R)$, $PQ = QP$, $(PQ)R = P(QR)$ és $(P+Q)R = PR + QR$.

Ezek ellenőrzése egyszerű. Például $P \cdot Q = Q \cdot P$ ellenőrzéséhez azt kell megnéznünk, hogy a két oldal esetén egy bizonyos típusú tag együtthatói azonosak-e. Az ellenőrizendő állítást az együtthatókra felírva olyan egyenlőségeket kapunk, amelyekben csak az együtthatók szerepelnek:

$$[x^n](PQ) = \sum_{i,j\in\mathbb{N}: i+j=n} [x^i]P[x^j]Q,$$

illetve

$$[x^n](QP) = \sum_{i,j\in\mathbb{N}: i+j=n} [x^i]Q[x^j]P.$$

A két szám egyenlőségét kell ellenőrizni, aely ellenőrzés folyamán a számokra megismert számolási szabályok alkalmazhatók.

Megjegyzés. A képzett olvasó esetleg tudja, hogy a számfogalom a komplex számokon túl is kiterjeszthető. bevezethetők a kvaterniók, amelyek szorzása már nem lesz kommutatív. A kvaternió együtthatójú polinomokról is beszélhetünk és ezekre is alkalmazható az összeadás és szorzás definíciója. Ebben az esetben a polinomok szorzása nem lesz kommutatív.

A fent ismertetett számolási szabályok közül egy ellenőrzését részletesen is elvégezzük.

1. Tétel. *Legyen $P, Q, R \in \mathbb{R}[x]$. Ekkor $(PQ)R = P(QR)$.*

Bizonyítás. Azt kell igazolnunk, hogy $[x^n](PQ)R = [x^n]P(QR)$ minden n természetes számra. Az egyenlőség bal és jobb oldalát külön alakítjuk.

$$\begin{aligned}
[x^n](PQ)R &= \sum_{i,j\in\mathbb{N}: i+j=n} [x^i](PQ)[x^j]R \\
&= \sum_{i,j\in\mathbb{N}: i+j=n} \left(\sum_{k,l\in\mathbb{N}: k+l=i} [x^k]P[x^l]Q \right) [x^j]R \\
&= \sum_{i,j\in\mathbb{N}: i+j=n} \sum_{k,l\in\mathbb{N}: k+l=i} [x^k]P[x^l]Q[x^j]R \\
&= \sum_{k,l,j\in\mathbb{N}: k+l+j=n} [x^k]P[x^l]Q[x^j]R.
\end{aligned} \tag{1}$$

A $[x^n]P(QR)$ együttható kiszámítása hasonlóan elvégezhető és ugyanerre az alakhoz jutunk. ∎

Az asszociativitás fontos következménye, hogy beszéhetünk a PQR hármas szorzatról. A kommutativitás miatt a tényezők sorrendje is tetszőleges, így egy három elemű polinomhalmaz esetén is jól értelmezett szorzatuk. A fenti bizonyítás egy kiszámítási módot is ad a hármas szorzatra. Mindegyik polinomot fogjuk fel, mint egy-egy zárójelbe írt monomok összegét. A szorzatot úgy kapjuk, hogy az összes lehetséges módon kiválasztunk egy-egy monomot a három zárójelből, összeszorozzuk azokat, majd az így kapott monomokat összegyűjtjük. Ez a szabály n-tényezős szorzatra is elmondható. Azaz

$$[x^n](PQR\dots YZ) = \sum_{i+j+k+\dots+s+t=n} [x^i]P[x^j]Q[x^k]R\dots[x^s]Y[x^t]Z.$$

Azaz

> Többtényezős szorzatban egy monom együtthatóját úgy határozzuk meg, hogy
> (1) Minden zárójelből úgy választunk ki egy-egy monomot, úgy hogy az ezekben szereplő határozatlan hatványainak szorzata a kiválasztott típusú legyen.
> (2) Ekkor a kiválasztott monomok együtthatóit összeszorozzuk.
> (3) Ezt az összes lehetséges módon megtesszük, az eredményeket összegezzük.
> A megfelelő együttható-szorzatok összege lesz a szorzatban a keresett együttható.

⋆ ⋆ ⋆

Az alábbiakban egy feladattal világítjuk meg a polinomokkal kapcsolatos eddigi fogalmakat

2. Feladat. *Lehetséges-e két kockát úgy „cinkelni” (tehát az egyes számok dobásának valószínűségét úgy megváltoztatni), hogy a feldobások után kapott számokat összeadva 2-től 12-ig minden lehetséges összeg bekövetkezésének valószínűsége ugyanannyi legyen?*

Először is nevezzük el a keresett valószínűségeket. Jelentse $p_1, p_2, p_3, p_4, p_5, p_6$, illetve $q_1, q_2, q_3, q_4, q_5, q_6$ az egyes kockák esetén a megfelelő szám valószínűségét. Annak valószínűségét hogy a két kockával együtt dobva a kapott számok összege n legyen, jelöljük s_n-nel ($n = 2, 3, \dots, 12$). Egyszerűen látható, hogy $s_n = \sum_{i,j\in\{1,2,\dots,6\}:i+j=n} p_i q_j$, ahol

Eddig három véges sorozatot vezettünk be. Fűzzük össze ezeket a sorozatokat x hatványaival egy-egy polinommá: $P = p_1x + p_2x^2 + p_3x^3 + p_4x^4 + p_5x^5 + p_6x^6$, $Q = q_1x+q_2x^2+q_3x^3+q_4x^4+q_5x^5+q_6x^6$ és $S = s_2x^2+s_3x^3+s_4x^4+\dots s_{12}x^{12}$. Ezzel három $\mathbb{R}[x]$-beli polinomhoz jutunk, amelyekben az i típusú monom együtthatója egy i eredményű dobás valószínűségét fejezi ki. Ekkor a valószínűségek közti összefüggést nagyon tömören fejezhetjük ki: $PQ = S$.

A feladat olyan p_i és q_i számok létezését kérdezi, amelyeknél $s_2 = s_3 = s_4 = \dots = s_{12} = \frac{1}{11}$ teljesüljön. A polinomok nyelvén ez azt jelenti, hogy olyan $P, Q \in \mathbb{R}[x]$ polinomokat keresünk, amelyekre

$$PQ = \frac{x^2}{11}(1 + x + x^2 + x^3 + \dots + x^{10}) \tag{1}$$

teljesül.

A feladat eredeti, „hétköznapi” szövegét lefordítottuk a „polinomok” nyelvére. A fordításunk nem tökéletes. A kiinduló sorozatok úgynevezett valószínűségi eloszlások. Azaz például a p_i számok nem-negatívak és összegük 1. Így például a P polinom együtthatói nem-negatívak és az $x = 1$ helyettesítéssel az értéke 1.

Beláthatjuk, hogy nincsenek ilyen P és Q valós együtthatós polinomok. Tegyük fel, hogy mégis vannak. Ekkor az (1) egyenletet $11(x-1)$-gyel szorozva és x^2-tel egyszerűsítve

$$11(x-1)\frac{P}{x}\frac{Q}{x} = x^{11} - 1$$

is teljesül.

Ebből az egyenlőségből ellentmondásra következtetünk. Indoklásunk az analitikus szemléletet használja. Az egyenlet bal oldala és jobb oldala is definiál egy-egy függvényt. Nevezzük ezeket b és $j : \mathbb{R} \to \mathbb{R}$ függvényeknek. A két oldal, mint polinom azonos, így azonos valós függvényeket definiálnak.

A jobb oldal által definiált j függvény egy szigorúan monoton függvény. Így pontosan egy (valós) gyöke van. Ez $x = 1$ és ennek a gyöknek multiplicitása 1. A bal oldal által definiált b függvénynek legalább 3 valós gyöke van (az esetleges multiplicitásokat is számolva), hiszen P/x és Q/x is ötödfokú polinom, azaz biztos van valós gyökük.

Az ellentmondás igazolja, hogy a kért cinkezés nem lehetséges.

Megjegyezzük, hogy a megoldás módszere nem teljesen homogén, analitikus és algebrai személet keveredett benne. Ennek oka az egyszerűség volt. Algebrai eszközökkel kimutathattuk volna, hogy $1 + x + x^2 + \ldots + x^{10}$ nem írható fel két ötödfokú polinom szorzataként $\mathbb{R}[x]$-ben.

3. Binomiális tétel

A binom magyarul két tagot jelent. Az alapkérdés, amit az alábbiakban megoldunk, hogy hogyan lehet kéttagú kifejezéseket hatványozni. A legegyszerűbb binom kifejezés, az $1 + x$ hatványainak meghatározása elegendő célunk eléréséhez.

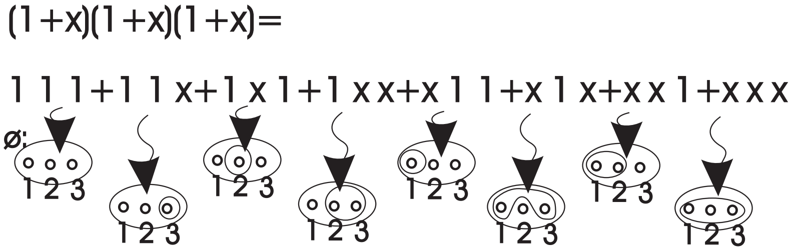
3. Tétel (Binomiális tétel).

$$(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i.$$

Megjegyzés. Azaz az $\binom{n}{k}$ számok az együtthatók az $1 + x$ binom hatványaiban. Ezekután mgadahatjuk szokásos elnevezésüket: binomiális együtthatók.

Bizonyítás. Végezzük el az $(1 + x)(1 + x) \ldots (1 + x)$ polinom szorzást. Ehhez válasszunk ki minden tényezőből egy-egy tagot. Minden tényező esetén a választható tag 1 vagy x.

n tényezőnk van. Ezek azonosíthatók a $U = \{1, 2 \ldots, n\}$ halmaz elemeivel. Az i-edik tényező esetén a két választható tagnak „nyilvánítsunk egy jelentést”. Ha az 1-et választjuk, akkor az jelentse azt, hogy az i elemet nem rakjuk bele U egy részhalmazába, ha pedig az x-et választjuk, akkor ez jelentse azt, hogy az i elemet belerakjuk U egy részhalmazába. Ezzel a „jelentéssel” a tényezőkből történő monomok választása megfelel az U halmazból egy részhalmaz kiválasztásával és fordítva. A következő ábra egy 3-elemű halmaz esetén mutatja ezt be.



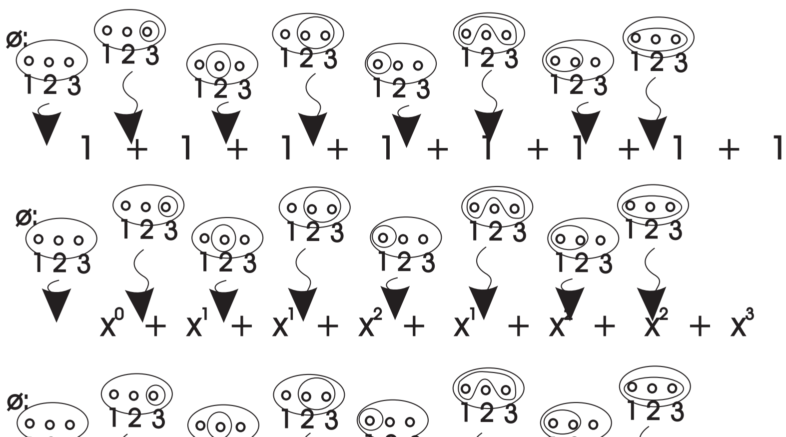
1. ábra.

Egy részhalmaznak megfelelő tag kitevője a halmaz elemszáma lesz, azaz H-nak $x^{|H|}$ monom felel meg. Így az x^k típusú monomok száma annyi lesz, amennyi az $\{1, 2, \ldots, n\}$ halmaz k-elemű részhalmazainak száma. ■

A fenti tétel után érthető, hogy az $\binom{n}{k}$ számok neve *binomiális együtthatók*.

Foglaljuk össze a fenti megoldás ötletét: A polinomok szorzásának definíciója bizonyos monomok összegyűjtését kívánja. Mi jelentést adtunk az egyes monomoknak, esetünkben ezek részhalmazokat azonosítottak. Egy monom típusa megegyezett a megfelelő részhalmaz egy paraméterével (esetünkben elemszámával). Így a polinom rendezése után, az egyes együtthatók egy adott paraméterrel (elemszámmal) rendelkező halmazokat „számolták össze”.

A következő hétköznapi analógia talán jobban megvilágítja a helyzetet: Gondoljunk arra, hogy az $\{1, 2, \ldots, n\}$ halmaz összes részhalmaza „felsorakozik és elhalad előttünk”. Amikor megszámoljuk a részhalmazokat, akkor mindegyik „elvonuló” részhalmaz esetén egy 1-est jegyzünk fel (egy vonást húzunk), majd amikor végeztünk, akkor ezek összessége megadja a keresett számot. Az alábbi ábra egy 3-elemű halmaz esetén mutatja be ezt.



2. ábra.

A mi polinomunk ennél érzékenyebb. Minden részhalmaz elvonulása esetén egy, a részhalmaz nagyságával megegyező típusú monomot jegyzünk fel. Ezen monomokat foglalja magába a szorzat-polinom. Tehát a feljegyzés nemcsak azt a tény foglalja magában, hogy elhaladt előttünk egy részhalmaz, hanem azt is, hogy mekkora volt a részhalmaz. Persze mindkét esetben feljegyzésünk feledékeny volt, hogy pontosan melyik részhalmaz vonult el, az a feljegyzésből nem derül ki. Ha pontos „kódolást” kívánunk, akkor megtehettük volna, hogy az $x^k = x^k \cdot 1^{n-k}$ monomban szereplő tényezők sorrendjénél figyelembe vesszük melyik tényező melyik zárójelből jött. Az így kapott (például $x11x1xx11$) monom „emlékezik”, hogy melyik részhalmazból eredt.

A binomiális tétel fenti bizonyításának ötlete nagyon fontos. Ennek az ötletnek egy további alkalmazását tekintjük. Ez a Kürschák József matematikai emlékverseny 1987. évi versenyéből való.

4. Feladat. *A és B a következő játékot játssza: az első 100 pozitív egész közül véletlenszerűen kiválasztanak k darabot és ha ezek összege páros, akkor A nyer, egyébként B. A k milyen értékeire lesz egyenlő A és B nyerési esélye?*

Ebben a feladatban a valószínűségszámítási nyelvezet nem lényeges eszköz. Érdemes kiküszöbölnünk a véletlennel kapcsolatos kifejezéseket. Az $\{1, 2, \ldots, 100\}$ halmaznak $\binom{100}{k}$ darab k-elemű részhalmaza van. Ezek közül bizonyosakba eső számok összege páros. Legyen ezek száma a_k. A többi részhalmaz esetén a benne lévő számok összege páratlan. Ezek száma legyen b_k. Nyilvánvalóan $a_k + b_k = \binom{100}{k}$. A nyerési esélye $a_k / \binom{100}{k}$, míg B nyerési esélye $b_k / \binom{100}{k}$ (jó esetek száma osztva az összes esetek számával). A feladat ennek a két nyerési esélynek az összehasonlításával kapcsolatos. A két esély nagyságrendi viszonya azonos az a_k és b_k számok nagyságrendi viszonyával. Ez pedig kiolvasható az $\omega_k = a_k - b_k$ számok előjeléből: Ha $\omega_k < 0$, akkor B nyerési esélye nagyobb; ha $\omega_k = 0$, akkor A és B nyerési esélye azonos; Ha $\omega_k > 0$, akkor A nyerési esélye nagyobb. Tehát a feladat kérdésének egy átfogalmazása: határozzuk meg azokat a k számokat ($k = 0, 1, \ldots, 100$), amelyekre $\omega_k = 0$. Mi ennél többet fogunk dolgozni: pontosan meghatározzuk az ω_k értékeket.

Példa. $\omega_0 = 1$. Egyetlen 0-elemű halmaz van, az üreshalmaz. Az eddigiekben erről nem szóltunk, de az elfogadott megállapodás szerint az „üres-halmaz elemeinek összegét” és általában az üres összegeket 0-nak definiáljuk. Tehát az üres-halmaz A-nak kedvez.

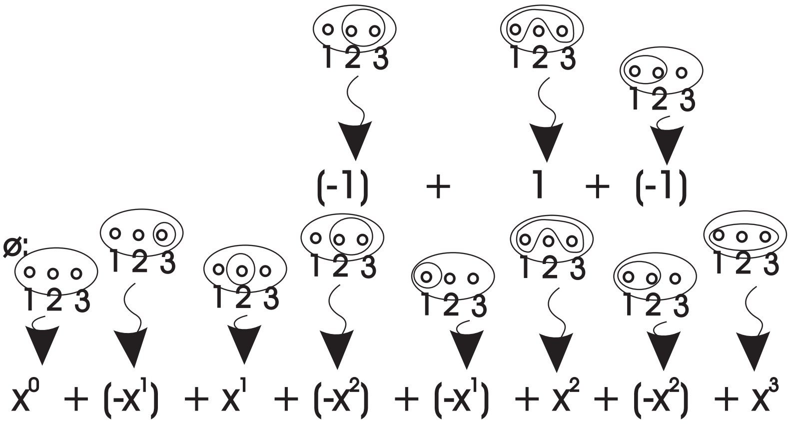
$\omega_1 = 50 - 50 = 0$. A 100 darab 1-elemű halmaz között 50 darab tartalmaz páros számot és 50 darab tartalmaz páratlan számot.

$\omega_2 = 2\binom{50}{2} - 50 \cdot 50 = -50$. Egy két elemű halmazban lévő számok összege akkor lesz páros, ha az 50 páros szám közül választottunk kettőt, illetve ha az 50 páratlan szám közül választottunk kettőt. Páratlan összeghez egy páros és egy páratlan számot kell választanunk.

A feladat megoldásához a $P(x) = \omega_0 + \omega_1 x + \ldots + \omega_{100} x^{100}$ polinomot fogjuk vizsgálni. Mielőtt ehhez hozzákezdenénk, vizsgáljuk meg az analóg polinomot az $a_k + b_k = \binom{100}{k}$ sorozat esetén. Ez a

$$\binom{100}{0} + \binom{100}{1} x + \binom{100}{2} x^2 + \ldots + \binom{100}{100} x^{100}$$

polinom lesz. A binomiális tétel megmondja, hogyan írható fel ez a polinom szorzat alakban: $(1+x)^{100}$. A bizonyítás ötelete alkalmazható problémánk esetén is. Az $\omega_k = a_k - b_k$ számokat is értelmezzük úgy, mint egy összeszámolást. Ez kissé furcsának tünhet, hiszen értéke negatív is lehet. Az előző megszámlási történetet úgy módosítjuk, hogy az elhaladó részhalmazok esetén, ha az összeg páros, akkor egy 1-est, ha páratlan, akkor egy -1-est jegyzünk fel. Az összes k-elemű részhalmaz elvonulása után feljegyzéseink összege éppen ω_k lesz:



3. ábra.

Ha feljegyzéseink közben érzékenyebbek vagyunk és lejegyezzük a megfelelő részhalmaz elemszámát is, akkor $-x^k$ és x^k-monomokat írunk le. Az „összes részhalmaz elvonulása” után a feljegyzett monomok összege a $P(x) = \omega_0 + \omega_1 x + \ldots + \omega_{100} x^{100}$ polinom lesz.

A $P(x)$ polinom egyenlő lesz a 100 tényezőből álló $(1-x)(1+x)(1-x)(1+x)\ldots(1-x)(1+x)$ polinom-szorzattal. Legyen a hozzárendelés az i-edik tényező 1 tagjánál a „nem választjuk ki az i elemet”, míg a $(-1)^i x$ tagnál a „kiválasztjuk az i elemet”. A polinom szorzás definíciójából eredő monom-szorzatok újból egy részhalmaz kiválasztásának felelnek meg. A megfelelő szorzat kitevője a halmaz elemszáma. De lesz egy előjel is. Ez azt mondja meg, hogy páros sokszor vagy páratlan sokszor választottunk $-x$-es monomot. Azaz a kiválasztott részhalmazban páros vagy páratlan sokszor szerepel páratlan szám. Azaz a részhalmazban szereplő számok összege páros vagy páratlan. Tehát egy részhalmaznak megfelelő monom-szorzat egyenlő lesz a részhalmazhoz tartozó „feljegyzéssel”.

Azaz

$$\begin{aligned}\omega_0 + \omega_1 x + \ldots + \omega_{100} x^{100} =&(1-x)(1+x)(1-x)(1+x)\ldots(1-x)(1+x) = \\ &(1-x)^{50}(1+x)^{50} = (1-x^2)^{50} = \sum_{i=0}^{50}(-1)^i\binom{50}{i}x^{2i}.\end{aligned}$$

Polinom egyenlőség két végén szereplő polinomok egyenlők, azaz a megfelelő együtthatóik egyenlők. Azaz

$$\omega_k = \begin{cases} 0, & k = 2l+1 \\ \binom{50}{2l}, & k = 4l \\ -\binom{50}{2l+1}, & k = 4l+2. \end{cases}$$

Ebből kiolvasható, hogy páratlan k esetén a játék igazságos, 4-gyel osztható k esetén A nyerési esélye jobb, míg a maradék esetekben ($k \equiv 2 \pmod 4$) B nyerési esélye jobb.

4. A Pascal-háromszög

Egy n elemű halmazra gondoljunk úgy, hogy van egy speciális eleme s. (Például halmaunk lehet egy osztálykirándulás résztvevőinek halmaza: az osztályfönök és a gyerekek.) Ekkor k elemű részhalmazai csoportosíthatók aszerint, hogy a speciális elem/s (az osztályfönök) benne van-e a halmazban. Így az összeszámolandó objektumokat (k elemű részhalmazok) két diszjunkt részre bontottuk/a megszámolandó objektumok listáját két részlistára szedtük szét. A két részlista milyen hosszú? A speciális elemet nem tartalmazó részhalmazokhoz $n-1$ elemből (nem-speciális elemek) kell kiválasztani k-t. A speciális elemet tartalmazó részhalmazokhoz $n-1$ elemből (nem-speciális elemek) kell kiválasztani $k-1$-t, emleyekl a speciális elemmel együtt kiadják a kiválasztandó k elemet.

Az összeadási alapelv alapján kapjuk, hogy az alábbi tételt.

5. Tétel. *(i)*

$$\binom{n}{0} = \binom{n}{n} = 1,$$

(ii) Ha $0 < k < n$, akkor

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}.$$

Valójában a fenti gondolatmenet (ii)-t indokolja. Az (i) rész a binomiális együtthatók definíciójából nyilvánvaló. A két állítást azért foglaltuk össze egy tételben, mert így a binomiális együtthatók ($\binom{n}{k}$ számok) közül az érdekesek ($0 \leq k \leq n$) egy teljes/rekurzív leírását kapjuk. Ezen számok egy tetszetős, háromszög alalkú táblázatban fogalalhatók össze. A táblázat szélső elemei 1-ek. Minden nem szélső elemnek lesz egy ÉNy-i és egy ÉK-i szomszéda, értéke ezen két felső szomszéd összege. A számtáblázat neve *Pascal-háromszög*.

$$\begin{array}{ccccccccccccccc}
 & & & & & & & 1 & & & & & & & \\
 & & & & & & 1 & & 1 & & & & & & \\
 & & & & & 1 & & 2 & & 1 & & & & & \\
 & & & & 1 & & 3 & & 4 & & 1 & & & & \\
 & & & 1 & & 4 & & 6 & & 4 & & 1 & & & \\
 & & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & & \\
 & 1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1 & \\
1 & & 7 & & 21 & & 35 & & 35 & & 21 & & 7 & & 1
\end{array}$$

Összefoglalva a rekurziót és binomiális tételt: Ha $(1+x)^n$ hatványt kifejtjük, akkor az együtthatók éppen a Pascal-háromszög $1, n, \ldots$ kezdetű sorában találhatók meg.

5. A Pascal-hármszög számainak paritása

6. Tétel. *Legyen a egy páros és b egy páratlan szám. Ekkor $\binom{a}{b}$ páros.*

Bizonyítás. Az állítást szemeléletesen fogjuk demonstrálni. Megadunk egy A a elemű halmazt és ennek b elemű részhalmazait párokba állítjuk. Az A halmaz elemei legyenek egy $(a/2) \times 2$-es sakktábla mezői. Erre a táblára úgy gondolunk, mint egy „házra”, amelynek $a/2$ szintje van (ezek a sorok) és minden szinten kettő lakás található (ez a megfelelő sorban lévő két mező). Az első és a második oszlopot közös határának egyenesére vonatkozó τ tükrözés táblázatunknak (házunknak) egy szimmetriája, amely felcseréli a házunk bal és jobb oldalát. Az A halmaz b elemű részhalmazai számukra b darab lakásból áló lakáshalmazok lesznek házunkban. Egy b elemű L lakáshalmazhoz rendeljük hozzá $\tau(L)$-et mint párt, az L-beli lakások tükörképeit. Így egy L-től különböző b elemű lakáshalmazt kaptunk, amely párja a kiinduló L lesz. A fenti állításban az egyetlen nem nyilvánvaló állítás, hogy L és $\tau(L)$ különbözik. Ez abból következik, hogy b páratlan. Azaz házunkban kell lennie olyan emeletnek, amelyen lévő két lakásból pontosan egy eleme L-nek. Ez az emelet megkülönbözteti L-et és $\tau(L)$-et. ■

Ha b páros, akkor a fenti bizonyítás nem működik. az $(L, \tau(L))$ párosításnál lesznek olyan L lakáshalmazok, amelyek párjai önmaguk lesznek. Ezek az L halmazok azonban könnyen leírhatók. azok a lakáshalmazok lesznek, amley elemei teljes emeletekből állnak össze. Azaz az $a/2$ emeletből kell $b/2$ emeletet kiválasztani, hogy az összes ilyen halmazt megkapjuk. Tehát a bizonyításbeli τ leképezés $\binom{a/2}{b/2}$ halmazt kiválaszt és a többit párokba állítja. Ez az észrevétel könnyen megfogalmazható a számelmélet nyelvén és így kapjuk a következő tételt.

7. Tétel. *legyen a és b két páros szám. Ekkor $\binom{a}{b}$ és $\binom{a/2}{b/2}$ azonos paritású (azaz egyszerre páros és egyszerre páratlan). Jelöléssel*

$$\binom{a}{b} \equiv \binom{a/2}{b/2} \pmod 2.$$

A fenti gondolatok különösebb gond nélkül páratlan a esetére is elismételhetők.

8. Tétel. *Legyen a egy páratlan szám ($a = 2k+1$).*
(i) Ha b páros ($b = 2\ell$), akkor $\binom{a}{b} \equiv \binom{k}{\ell} \pmod 2$,
(ii) Ha b páratlan ($b = 2\ell + 1$), akkor $\binom{a}{b} \equiv \binom{k}{\ell} \pmod 2$.

Bizonyítás. Először definiálunk egy a elemű halmazt. Ez egy „k emeletes, emeletenként két lakásos ház lakásaiból” és „külön lakásból” álló halmaz. Ismét definiálhatjuk a τ leképezést. Egy L lakáshalmazra úgy kapjuk meg $\tau(L)$-t, hogy L az emeletes házba eső részére a bal és jobb oldalt felcserélve új lakáshalmazra térünk át, míg a külön lakást tekintve nem változtatjuk meg L-et (ha a külön lakás L eleme volt, akkor $\tau(L)$-nek is eleme lesz; ha a külön lakás nem volt L eleme, akkor $\tau(L)$-nek sem lesz eleme). Milyen L-re lesz $L = \tau(L)$? Ez akkor és csak akkor teljesül, ha L-nek az emletes házba eső része teljes emeletekből ál össze. Azaz (i) esetén L-et ℓ teljes emelet alkotja, míg (ii) esetén L-et ℓ teljes emelet és a külön lakás alkotja.

Ebből a bizonyítandó adódik. ■

A fenti négy állítás egyetlen formulában is megfogalmazható. Ehhez felhasználjuk, hogy minden természetes szám felírható $2k + \epsilon$ alakban, ahol $\epsilon \in \{0, 1\}$. Ekkor

$$\binom{2k+\epsilon}{2\ell+\varepsilon} \equiv \binom{k}{\ell}\binom{\epsilon}{\varepsilon} \pmod 2.$$

Ezt az állítást ismételten alkalmazva minden binomiális együttható paritását gyorsan meghatározhatjuk.

Példa. Legyen $p = 2$. Ekkor $\binom{7}{2} = \binom{3\cdot 2+1}{1\cdot 2+0} \equiv \binom{3}{1}\binom{1}{0} \pmod 2$. Hasonlóan $\binom{3}{1} = \binom{1\cdot 2+1}{0\cdot 2+1} \equiv \binom{1}{0}\binom{1}{1} \pmod 2$. Összefoglalva $\binom{7}{} = \binom{111_2}{010_2} \equiv \binom{1}{0}\binom{1}{1}\binom{1}{0} \pmod 2$.

A fenti rövid példa alapján is felismerhetjük az általános szabályt.

9. Tétel. *Legyen $0 \le k \le n$. Írjuk fel n-et és k-t is kettes számrendszerben. k felírását egészítsük ki elején 0-kal úgy, hogy a felírásának hossza azonos legyen n kettes számrendszerbeli alakjával. Legyen ez a két felírás $n = \overline{a_1a_2\ldots a_s}_2$, $k = \overline{b_1b_2\ldots b_s}_2$. Ekkor*

$$\binom{n}{k} \equiv \binom{a_1}{b_1}\binom{a_2}{b_2}\cdots\binom{a_s}{b_s} \pmod 2.$$

Azaz $\binom{n}{k}$ akkor és csak akkor páros, ha van olyan $1 \le i \le s$, hogy $a_i = 0$ és $b_i = 1$.

10. Következmény. *A Pascal háromszög $\binom{n}{k}$ alatti számokat ($k = 0, 1, \ldots, n-1, n$) tartalmazó sora akkor és csak akkor tartalmaz csupa páratlan számot, ha $n = 2^\ell - 1$ alakú.*

⋆ ⋆ ⋆

Eredményeink nem csak a paritásra alkalmazhatók. Binomiális együtthatók egy prímszámmal való osztási maradékaira hasonló állítások igazak.

11. Tétel. *Legyen p egy prímszám és a, b, α, β természetes számok, ahol $\alpha, \beta < p$. Ekkor*

$$\binom{ap+\alpha}{bp+\beta} \equiv \binom{a}{b}\binom{\alpha}{\beta} \pmod p.$$

Bizonyítás. Legyen C egy $ap+\alpha$ elemű halmaz. Legyen $C = C_1 \cup C_2 \cup \ldots \cup C_a \cup \bar{C}$, ahol a C_i halmazok elemszáma p és az $\bar{C}$ halmaz elemszáma α. (Az elemszámokból kiolvasható, hogy a fenti halmazoknak nincs közös elemük, idegen szóval *diszjunktok.*)

$\binom{ap+\alpha}{bp+\beta}$ az C halmaz $bp+\beta$ elemszámú részhalmazainak száma. Legyen A a C halmaz $bp+\beta$ elemszámú részhalmazainak halmaza. Legyen B a C halmaz azon $bp+\beta$ elemszámú részhalmazainak halmaza, amelyek b darab C_i halmazt teljesen és a $\bar{C}$ halmaz β darab elemét tartalmazzák. Tehát B elemei speciális A-beli elemek ($B \subset A$). Legyen $X = Y = B$.

A bizonyítás befejezéséhez $A - X$ elemeit kell p elemű osztályokba sorolnunk. Ehhez C elemeit szemléltessük a következőképpen. Vegyünk egy szabályos p-szög alapú egyenes hasábot. Ennek alaplapjának a síkjára, mint vízszintes síkra hivatkozunk. Ennek palástján a darab vízszintes síkkal kimetszünk a darab szabályos p-szöget. Ennek ap csúcsával reprezentáljuk $C_1 \cup \ldots \cup C_a$ elemeit, ahol az egyes C_i halmazok az egy szinten lévő csúcsoknak felelnek meg. Így A egy eleme, C egy $ap+\alpha$ elemszámú részhalmaza, felfogható úgy, hogy az egyenes hasábon kijelölt pontok egy részhalmaza és esetleg néhány pont $\bar{C}$-ből. X elemei azok a részhalmazok, amelyek a hasábról pontosan b darab teljes szintet tartalmaznak. Tehát $A-X$ elemei esetén a „hasábból jövő hozzájárulás” nem teljes szintekből áll össze. Ennek következményeképpen, ha A hasábbeli rész elforgatásával egymásba vihető részhalmazok kerülnek egy osztályba, akkor p elemű osztályok alakulnak ki. ■

12. Következmény. *Legyen* $x = (x_1x_2\dots x_k)_p$ *és* $y = (y_1y_2\dots y_k)_p$ *az* x *és* y *természetes számok* p *számrendszerben való felírásai. (A két felírás hossza ugyanaz. Ezt elérhetjük úgy, hogy a rövidebb felírást nullákkal kiegészítjük az elején.) Ekkor*

$$\binom{x}{y} \equiv \binom{x_1}{y_1}\binom{x_2}{y_2}\dots\binom{x_k}{y_k} \pmod{p}.$$

Tanulmányozzuk a Pascal-háromszög elemeinek adott számmal való osztási maradékát. A megállapított összefüggéseket bizonyítsuk be!