q-analogoni kombinatoričkih brojeva i identiteta

Jagetić, Dunja

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Dunja Jagetić

q-analogoni kombinatoričkih brojeva i identiteta

Diplomski rad

Voditelj rada:
izv.prof.dr.sc. Vedran Krčadinac

Zagreb, rujan 2015.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____ , predsjednik
2. _____ , član
3. _____ , član

Povjerenstvo je rad ocijenilo ocjenom _____ .

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

1 Uvod

Kombinatorika je matematička disciplina koja proučava konačne skupove i strukture, prebrojava njihove elemente i načine na koji se ti elementi mogu poredati po određenom kriteriju. Naziv dolazi od latinske riječi combinare što znači slagati. Matematičari su se od davnina bavili problemom prebrojavanja elemenata konačnih skupova, a isti se javljaju i danas u svakodnevnom životu, od problema razmještaja ljudi za stolom, slaganja sportskih ekipa, igara na sreću poput Lota, do nešto složenijih problema. U nekim slučajevima elemente skupa je jednostavno prebrojiti, međutim, često ti elementi čine neki pravilnu konfiguraciju ili su zadani pomoću nekog svojstva. Kombinatorika istražuje različite metode rješavanja danih problema. U ovom radu navest ćemo neke od kombinatoričkih metoda, upoznati se s nekim poznatim kombinatoričkim brojevima i identitetima te njihovom primjenom.

Prvo poglavlje uvod je u konačna polja i njihovu konstrukciju. Neka je p^n prim potencija koju ćemo u daljnjem tekstu označavati s q. Konačno polje s q elemenata još nazivamo i Galoisovo polje reda q. Uz prije spomenute kombinatoričke brojeve, u radu ćemo proučavati i njihove q-analogone, odnosno analogone nad konačnim poljima reda q. Počet ćemo s binomnim koeficijentima.

Binomni koeficijenti uvršteni su u program srednjih škola. Uče se u okviru osnovnih kombinatornih principa prebrojavanja: permutacija, varijacija i kombinacija; te u sklopu binomnog teorema. Unutar školskog gradiva učenici se upoznavaju s formulom i prikazom binomnih koeficijenata u obliku trokuta. Takav način zapisa binomnih koeficijenata često se pripisuje Blaiseu Pascalu (17.st.), prema kome je zapis dobio ime Pascalov trokut, međutim, bio je poznat i mnogim matematičarima prije njega. Poseban slučaj binomnog teorema za $n = 2$ znao je grčki matematičar Euklid (4.st.pr.Kr.), a indijski matematičar Pingala (3.st.pr.Kr.) za više eksponente. Sam Pascalov trokut već je bio poznat perzijskim matematičarima Al-Karaji (11.st.) i Omaru Khayyamu (13.st.) te kineskom matematičaru Yangu Huiu (13.st.). Al-Karaji je, također, dao prvi dokaz binomnog teorema. Nakon upoznavaja s binomnim koeficijentima, izvest ćemo formulu za njihove q-analogone u vektorskom prostoru nad konačnim poljem, poznate i pod nazivom Gaussovi koeficijenti.

U kombinatorici je rasprostranjena primjena i Stirlingovih brojeva. Oni se dijele na Stirlingove brojeve prve vrste i Stirlingove brojeve druge vrste. Kroz povijest su često proučavani, međutim, dugo se nije navodilo njihovo ime. Detaljnije ih je opisao tek mađarski matematičar Charles Jordan 1939. godine. Mi ćemo se osvrnuti samo na Stirlingove brojeve druge vrste i njihove q-analogone. Za njih također vrijedi mnoštvo relacija vrlo sličnih onima za

binomne koeficijente.

2 Konačna polja

Definicija 2.1. *Neka su a i b cijeli brojevi. Ako prirodan broj m dijeli razliku $a-b$, onda kažemo da je a* kongruentan *b* modulo *m i pišemo $a \equiv b \pmod{m}$. U protivnom, kažemo da a nije kongruentan b modulo m.*

Propozicija 2.2. *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz. Relacija kongruencije modulo m zadovoljava refleksivnost, simetričnost i tranzitivnost:

1. Iz $m \mid 0$ slijedi $a \equiv a \pmod{m}$.
2. Ako je $a \equiv b \pmod{m}$, onda postoji $k \in \mathbb{Z}$ takav da $a - b = mk$. Sada je $b - a = m \cdot (-k)$, pa je $b \equiv a \pmod{m}$.
3. Iz $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ slijedi da postoje $k, l \in \mathbb{Z}$ takvi da je $a - b = mk$ i $b - c = ml$. Zbrajanjem dobivamo $a - c = m(k + l)$, što povlači $a \equiv c \pmod{m}$.

□

Klasu ekvivalencije $[a]_m$ modulo m čine svi cijeli brojevi koji su kongruentni modulo m cijelom broju a.

Propozicija 2.3. *Neka su a, b, c, d cijeli brojevi.*

1. *Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a+c \equiv b+d \pmod{m}$, $a - c \equiv b - d \pmod{m}$ i $ac \equiv bd \pmod{m}$.*
2. *Ako je $a \equiv b \pmod{m}$ i $d \mid m$, onda je $a \equiv b \pmod{d}$.*
3. *Ako je $a \equiv b \pmod{m}$, onda je $ac \equiv bc \pmod{mc}$ za svaki $c \neq 0$.*

Dokaz.
1. Neka je $a - b = mk$ i $c - d = ml$. Tada je $(a + c) - (b + d) = m(k + l)$ i $(a - c) - (b - d) = m(k - l)$, iz čega slijedi $a + c \equiv b + d \pmod{m}$ i $a-c \equiv b-d \pmod{m}$. Zbog $ac-bd = a(c - d)+d(a - b) = m(al + dk)$ slijedi da je $ac \equiv bd \pmod{m}$.
2. Neka je $m = de$. Tada iz $a - b = mk$ slijedi $a - b = d \cdot (ek)$, pa je $a \equiv b \pmod{d}$.
3. Iz $a - b = mk$ slijedi $ac - bc = (mc) \cdot k$, pa je $ac \equiv bc \pmod{mc}$.

□

Definicija 2.4. *Skup* $\{x_1, ..., x_m\}$ *se zove* potpuni sustav ostataka *modulo* m *ako za svaki* $y \in \mathbb{Z}$ *postoji točno jedan* x_j *takav da je* $y \equiv x_j \pmod{m}$.

Drugim riječima, potpuni sustav ostataka dobivamo tako da iz svake klase ekvivalencije modulo m uzmemo po jedan član.

Neka su a, b cijeli brojevi, a m prirodan broj. Tada se $ax \equiv b \pmod{m}$ zove linearna kongruencija po nepoznanici x. Za nalaženje svih rješenja dane kongruencije, dovoljno je pronaći sve brojeve $x \in \mathbb{Z}$ koji je zadovoljavaju. Dva rješenja x i x' smatramo ekvivalentnima ako je $x \equiv x' \pmod{m}$. Broj rješenja kongruencije je broj neekvivalentnih rješenja.

Neka su x i y dva cijela broja. Označimo sa (x, y) njihov najveći zajednički djelitelj.

Teorem 2.5. *Vrijedi:* $ax \equiv ay \pmod{m}$ *ako i samo ako* $x \equiv y \pmod{\frac{m}{(a,m)}}$. *Specijalno, ako je* $ax \equiv ay \pmod{m}$ *i* $(a, m) = 1$, *onda je* $x \equiv y \pmod{m}$.

Dokaz. Ako je $ax \equiv ay \pmod{m}$, onda postoji $z \in \mathbb{Z}$ takav da je $ay - ax = mz$. Imamo da je $\frac{a}{(a,m)}(y - x) = \frac{m}{(a,m)}z$, odnosno $\frac{m}{(a,m)}$ dijeli $\frac{a}{(a,m)}(y - x)$. Kako su brojevi $\frac{a}{(a,m)}$ i $\frac{m}{(a,m)}$ relativno prosti, zaključujemo da $\frac{m}{(a,m)}$ dijeli $y - x$, odnosno da je $x \equiv y \pmod{\frac{m}{(a,m)}}$.

Obrnuto, ako je $x \equiv y \pmod{\frac{m}{(a,m)}}$, onda iz svojstava kongruencije slijedi $ax \equiv ay \pmod{\frac{am}{(a,m)}}$. Kako je m djelitelj od $\frac{am}{(a,m)}$, dobivamo $ax \equiv ay \pmod{m}$. □

Teorem 2.6. *Neka je* $\{x_1, ..., x_m\}$ *potpuni sustav ostataka modulo* m, *te neka je* $(a, m) = 1$. *Tada je* $\{ax_1, ..., ax_m\}$ *također potpuni sustav ostataka modulo* m.

Dokaz. Za dokaz teorema dovoljno je pokazati da je $ax_i \not\equiv ax_j \pmod{m}$ za $i \neq j$. Pretpostavimo da je $ax_i \equiv ax_j \pmod{m}$. Tada teorem 2.5 povlači da je $x_i \equiv x_j \pmod{m}$, tj. $i = j$. □

Teorem 2.7. *Kongruencija* $ax \equiv b \pmod{m}$ *ima rješenja ako i samo ako* $d = (a, m)$ *dijeli* b. *Ako je ovaj uvjet zadovoljen, onda gornja kongruencija ima točno* d *rješenja modulo* m.

Dokaz. Ako $ax \equiv b \pmod{m}$ ima rješenje, onda postoji $y \in \mathbb{Z}$ takav da je $ax - my = b$. Očito $d = (a, m)$ dijeli b. Obrnuto, pretpostavimo da $d \mid b$. Neka je $a' = \frac{a}{d}$, $b' = \frac{b}{d}$, $m' = \frac{m}{d}$. Trebamo riješiti kongruenciju $a'x \equiv b' \pmod{m'}$. Prema teoremu 2.6 slijedi da ona ima točno jedno rješenje modulo m', tj. svaki ostatak modulo m' (pa tako i b') se dobiva točno za jedan x iz potpunog sustava ostataka modulo m'.

Ako je x' neko rješenje od $a'x' \equiv b' \pmod{m'}$, onda su sva rješenja $ax \equiv b \pmod{m}$ u cijelim brojevima dana sa $x = x' + nm'$, za $n \in \mathbb{Z}$, a sva međusobno neekvivalentna rješenja sa $x = x' + nm'$, gdje je $n = 0, 1, ..., d-1$. Dakle, ako d dijeli b, onda kongruencija $ax \equiv b \pmod{m}$ ima točno d rješenja modulo m. □

Neka su $[a]_m$ i $[b]_m$ klase ekvivalencije modulo m. Operacije $+$ i $\cdot$ definirane su na način

$$[a]_m + [b]_m = [a + b]_m ,$$
$$[a]_m \cdot [b]_m = [a \cdot b]_m .$$

Neka je $a \equiv a' \pmod{m}$ i $b \equiv b' \pmod{m}$. Slijedi $a+b \equiv a'+b' \pmod{m}$ i $a \cdot b \equiv a' \cdot b' \pmod{m}$. Dakle, definicije zbrajanja i množenja klasa ekvivalencije modulo m su dobre, odnosno, ne ovise o izboru predstavnika.

Teorem 2.8. *Skup ostataka modulo m uz operacije zbrajanja i množenja čini komutativni prsten s jedinicom $(\mathbb{Z}_m, +, \cdot)$.*

Dokaz. $(\mathbb{Z}_m, +, \cdot)$ je prsten ako:

1. $(\mathbb{Z}_m, +)$ je Abelova grupa,
2. $(\mathbb{Z}_m, \cdot)$ je polugrupa,
3. vrijedi zakon distributivnosti.

Svojstva operacija modulo m slijede iz svojstva zbrajanja i množenja cijelih brojeva. Skup brojeva $\mathbb{Z}$ s obzirom na operacije zbrajanja i množenja čini prsten. Slijedi da i skup ostataka modulo m uz operacije zbrajanja i množenja, $(\mathbb{Z}_m, +, \cdot)$, čini prsten. Budući da je množenje u $\mathbb{Z}$ komutativno i ima neutralni element 1, prsten $(\mathbb{Z}_m, +, \cdot)$ ima ista svojstva. □

Definicija 2.9. *Prirodan broj $p > 1$ koji je djeljiv samo s 1 i sa samim sobom zove se* prost broj *ili* primbroj.

Teorem 2.10. *$(\mathbb{Z}_m, +, \cdot)$ je polje ako i samo ako je m prost broj.*

Dokaz. Prema teoremu 2.8 $(\mathbb{Z}_m, +, \cdot)$ je uvijek komutativan prsten s jedinicom. Da bi $(\mathbb{Z}_m, +, \cdot)$ bio polje, njegov svaki element mora imati multiplikativni inverz. Tvrdnju ćemo dokazati u oba smjera. Neka je prvo $\mathbb{Z}_p$ polje. Pretpostavimo da m nije prost broj, odnosno da je $m = a \cdot b$ za neke $a, b \in \mathbb{Z}$, $1 < a, b < m$. Sada slijedi

$$[a]_m \cdot [b]_m = [m]_m = [0]_m$$

$$[a]_m^{-1} \mid [a]_m \cdot [b]_m = [0]_m$$
$$[b]_m = [0]_m$$

Budući da je prema pretpostavci $[b]_m \neq [0]_m$, dobili smo kontradikciju. Dakle, m mora biti prost broj.

S druge strane, neka je m prost broj. Uzmimo da je $[a]_m \neq [0]_m$, $a \in \{1, ..., m-1\}$. Riješimo sada sljedeću kongruenciju $[a]_m \cdot [x]_m = [1]_m$. To znači da $ax \equiv 1 \pmod{m}$, odnosno $(a, m) = 1$. Sada, iz teorema 2.7 slijedi da ta kongruencija ima jedinstveno rješenje. Dakle postoji $[b]_m = [a]_m^{-1}$. Prema tome, ako je m prost broj, svaki element $(\mathbb{Z}_m, +, \cdot)$ ima multiplikativni inverz pa je $(\mathbb{Z}_m, +, \cdot)$ polje. □

To polje se obično označava sa $\mathbb{Z}_p$, gdje je p prost broj.

Pretpostavimo da je $q = p^n$ prim potencija. Tada polje F reda q možemo konstruirati pomoću normiranog ireducibilnog polinoma nad $\mathbb{Z}_p$, stupnja n.

Definicija 2.11. *Polinom $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ zovemo normirani polinom ako je $a_n = 1$.*

Definicija 2.12. *Za polinom $f \in \mathbb{Z}_p[x]$ kažemo da je reducibilan nad $\mathbb{Z}_p$ ako postoje polinomi $g, h \in \mathbb{Z}_p[x]$, $\operatorname{st} g$, $\operatorname{st} h \geq 1$ takvi da je $f = g \cdot h$. Ako polinom f nije reducibilan, onda kažemo da je on ireducibilan nad $\mathbb{Z}_p$.*

Neka je
$$f(x) = x^n + b_{n-1}x^{n-1} + ... + b_1 x + b_0$$
ireducibilni polinom. Elementi polja su oblika

$$c_0 + c_1 x + ... + c_{n-1}x^{n-1}$$

za $c_0, c_1, ..., c_{n-1} \in \mathbb{Z}_p$.

Zbrajanje je definirano očito, kao zbrajanje polinoma iz $\mathbb{Z}_p[x]$. Množenje definiramo na način da budu ispunjena svojstva polja. U tu svrhu koristimo sljedeći teorem.

Teorem 2.13. *(*Teorem o dijeljenju polinoma s ostatkom*) Za svaka dva polinoma $f, g \in \mathbb{F}[x]$, $g \neq 0$ postoje jedinstveni polinomi $q, r \in \mathbb{F}[x]$ takvi da vrijedi*
$$f = g \cdot q + r.$$
U slučaju da je $r \neq 0$, tada vrijedi $\operatorname{st} r < \operatorname{st} g$.

Dokaz za polje $\mathbb{R}$ se može naći u knjizi [9], a isti dokaz vrijedi i za proizvoljno polje $\mathbb{F}$. Mi ćemo teorem koristiti za polje $\mathbb{F} = \mathbb{Z}_p$ da bismo definirali množenje u polju reda p^n.

Pri definiranju nove operacije množenja, ulogu analognu onoj prim broja p kod operacija modulo p ovdje će imati odabrani ireducibilni polinom $f(x)$ stupnja n. Polinom će se pomnožiti standardno pa će se onda uzeti ostatak pri dijeljenju umnoška polinomom $f(x)$. Na taj način dobivamo polje reda p^n.

Primjerice, konstruirajmo polje reda 4. Tada imamo svega četiri polinoma stupnja manjeg od 2: 0, 1, x i $1 + x$, a za operaciju množenja treba nam ireducibilni polinom stupnja 2. Taj polinom ne smije imati nultočke u polju $\mathbb{Z}_2$ pa lako vidimo da to mora biti polinom $f(x) = x^2 + x + 1$. Sada je npr. $(x+1)(x+1) = x^2+1 \equiv x \pmod{f(x)}$. Operacije zbrajanja i množenja nad zadanim poljem prikazane su sljedećim tablicama:

$+$	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

$\cdot$	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

Na taj način, pomoću ireducibilnih polinoma stupnja n nad $\mathbb{Z}_p$, konstruiramo konačno polje reda p^n. Egzistenciju i jedinstvenost konačnog polja reda p^n slijedi iz sljedećeg teorema.

Teorem 2.14. *(*Galoisov teorem*) Konačno polje reda m postoji ako i samo ako je m prim potencija. Svaka dva konačna polja istog reda su izomorfna.*

Ovaj teorem nećemo dokazivati. Dokaz se može naći u knjizi [2].

Polje sa q elemenata zovemo Galoisovo polje reda q. Postoje dvije standardne oznake za Galoisovo polje, to su $\mathbb{F}_q$ i $GF(q)$. Mi ćemo se koristiti oznakom $\mathbb{F}_q$.

3 Binomni i q-binomni koeficijenti

3.1 Definicija i osnovna svojstva binomnih koeficijenata

Neka je S konačni skup sa n elemenata.

Definicija 3.1. Binomni koeficijent $\binom{n}{k}$ *je broj k-članih podskupova konačnog n-članog skupa S.*

Propozicija 3.2.

$$\binom{n}{k} = \frac{n(n-1)...(n-k+1)}{k(k-1)...1} = \frac{n!}{k!(n-k)!}$$

Dokaz. Dokaz ćemo provesti jednostavnim prebrojavanjem na koliko načina možemo iz n-članog skupa odabrati k elemenata. Za prvi element očito postoji n mogućih izbora, za drugi element $(n-1)$ izbora, sve do k-tog elementa za koji postoji $(n-k+1)$ mogućih izbora. Prema principu produkta dobili smo $n(n-1)...(n-k+1) = \frac{n!}{(n-k)!}$ mogućnosti. Izračunali smo broj mogućnosti u slučaju da su elementi uređeni. Međutim, elementi u podskupu nisu uređeni, tj. ne razlikujemo koji element je prvi, koji drugi itd. kao što smo naveli iznad. Stoga, dobiveni broj moramo podijeliti s brojem različitih redoslijeda k elemenata koje smo izabrali. Tako smo za prvi element imali k izbora, za drugi element $k-1$ izbora, sve do k-tog elementa za koji nam je ostao zadnji i jedini izbor. Ukupno je to $k!$ izbora za redoslijed te time moramo podijeliti prije dobiveni broj, što znači da iz n-članog skupa možemo odabrati k elemanata na $\binom{n}{k} = \frac{n!}{k!(n-k)!}$ načina. □

Primjer. Neka je $n = 4$ i $k = 2$. Imamo li primjerice skup $\{a, b, c, d\}$, moguće je odabrati sljedeće dvočlane podskupove: $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$ i $\{c, d\}$. Takvih je ukupno 6, što se jednostavnije može dobiti uvrštavanjem u formulu:

$$\binom{4}{2} = \frac{4 \cdot 3}{1 \cdot 2} = 6.$$

Iz dobivene formule za binomne koeficijente slijedi niz identiteta koje se mogu dokazati na više načina, i algebarski, uvrštavanjem u formulu, i kombinatorno. Navest ćemo neke od njih.

Propozicija 3.3.

$$\binom{n}{k} = \binom{n}{n-k}$$

Dokaz. 1. način - algebarski dokaz.

$$\binom{n}{n-k} = \frac{n(n-1)...(n-n+k+1)}{(n-k)(n-k-1)...1} = \frac{n(n-1)...(k+1)}{(n-k)!}$$

$$= \frac{n(n-1)...(k+1)k!}{(n-k)!k!} = \frac{n!}{(n-k)!k!} = \binom{n}{k}$$

2. način - kombinatorni dokaz. Primjerice, uzmimo ekipu od n igrača koji su došli na utakmicu. Od tih n igrača trebamo odabrati k-članu ekipu koja će izaći na teren, dok će ostali sjediti na klupi. Odabir k igrača koji će izaći na teren ekvivalentan je odabiru $n-k$ igrača koji će ostati sjediti na klupi. Matematički gledano, uspostavljamo bijekciju između k-članih podskupova A n-članog skupa S i njihovih komplementa A^c od $n-k$ članova. Ta bijekcija je $f : \mathcal{P}_k \to \mathcal{P}_{n-k}$, $f(A) = A^c = S \backslash A$. Radi se zaista o bijekciji jer ta funkcija ima inverznu funkciju $f^{-1} : \mathcal{P}_{n-k} \to \mathcal{P}_k$, $f^{-1}(A) = A^c = S \backslash A$. Zbog svojstva komplementa $(A^c)^c = A$ vrijedi $f^{-1} \circ f = id_{\mathcal{P}_k}$ i $f \circ f^{-1} = id_{\mathcal{P}_{n-k}}$. □

Propozicija 3.4.

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

Dokaz. 1. način - algebarski dokaz.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n \cdot (n-1)!}{k \cdot (k-1)!(n-k)!}$$

$$k\binom{n}{k} = n \cdot \frac{(n-1)!}{(k-1)!(n-k)!}$$

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

2. način - kombinatorni dokaz. Poslužimo se ponovno sportskim žargonom. Između n igrača želimo odabrati k-članu ekipu u kojoj će jedan igrač biti kapetan momčadi. Prema propoziciji 3.2, ekipu možemo odabrati na $\binom{n}{k}$ načina. Za svaki mogući izbor ekipe, kapetana možemo odabrati na još k načina. To odgovara lijevoj strani izraza. S druge strane, možemo prvo izabrati kapetana na n načina, a nakon toga izabrati ostatak ekipe. To znači da ćemo između preostalih $n-1$ igrača odabrati ostatak ekipe, odnosno $k-1$ član. Na ovaj način dobili smo desnu stranu izraza.

Općenito, dvama različitim načinima brojanja, odnosno principom dvostrukog prebrojavanja, dobivamo isti rezultat. Neka je S n-člani skup iz kojeg izabiremo neki njegov k-člani podskup A koji sadrži neki element x

koji se nečime ističe. Dakle, neka je $|S| = n$ i prebrojavamo skup parova $\{(A, x) \mid A \subseteq S, |A| = k, x \in A\}$. Sada je svejedno biramo li prvo podskup A, a zatim x unutar njega što možemo na $\binom{n}{k} \cdot k$ načina, ili prvo biramo x, a zatim ostatak podskupa A što možemo učiniti na $n \cdot \binom{n-1}{k-1}$ načina. Time smo dokazali tvrdnju. □

Propozicija 3.5. *(*Pascalov identitet*)*

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

Dokaz. 1. način - algebarski dokaz.

$$\begin{aligned}\binom{n}{k-1} + \binom{n}{k} &= \frac{n!}{(k-1)!(n-k+1)!} + \frac{n!}{k!(n-k)!} \\ &= \frac{n! \cdot k + n!(n-k+1)}{k!(n-k+1)!} = \frac{n!(k+n-k+1)}{k!(n-k+1)!} \\ &= \frac{n!(n+1)}{k!(n-k+1)!} = \frac{(n+1)!}{k!(n+1-k)!} = \binom{n+1}{k}\end{aligned}$$

2. način - kombinatorni dokaz. Uzmimo razred od $n+1$ učenika, od kojih je jedan na neki način izdvojen od ostalih i želimo izabrati tim od k učenika. Postoji $\binom{n+1}{k}$ mogućih kombinacija. To možemo napraviti na dva načina. Prvi način je tako da uključimo izdvojenog učenika te izaberemo $k-1$ učenika između preostalih n, za što postoji $\binom{n}{k-1}$ mogućih kombinacija. Drugi način je da izdvojenog učenika izbacimo iz kombinacija za tim te izaberemo cijeli k-člani tim izmedu preostalih n učenika, za što postoji $\binom{n}{k}$ mogućih kombinacija. To odgovara desnoj strani izraza, čime smo dokazali tvrdnju.

Općenito, imamo $(n+1)$-člani skup S te istaknemo element $x_0 \in S$. Ukupan broj k-članih podskupova od S iznosi $| \mathcal{P}_k(S) | = \binom{n+1}{k}$. Skup $\mathcal{P}_k(S)$ možemo podijeliti na dva međusobno disjunktna skupa $\mathcal{P}_k(S) = \mathcal{P}_1 \cup \mathcal{P}_2$, pri čemu je $\mathcal{P}_1$ skup svih k-članih podskupova od S koji sadrže x_0, $\mathcal{P}_1 = \{A \in \mathcal{P}_k(S) \mid x_0 \in A\}$ i takvih ima $| \mathcal{P}_1 | = \binom{n}{k-1}$, te $\mathcal{P}_2$ skup svih k-članih podskupova od S koji ne sadrže x_0, $\mathcal{P}_2 = \{A \in \mathcal{P}_k(S) \mid x_0 \notin A\}$ i takvih ima $| \mathcal{P}_2 | = \binom{n}{k}$. Iz toga slijedi $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$. □

Binomni koeficijenti često se zapisuju u trokutaskom poretku na sljedeći

način:

$$\binom{0}{0}$$

$$\binom{1}{0} \quad \binom{1}{1}$$

$$\binom{2}{0} \quad \binom{2}{1} \quad \binom{2}{2}$$

$$\binom{3}{0} \quad \binom{3}{1} \quad \binom{3}{2} \quad \binom{3}{3}$$

$$\binom{4}{0} \quad \binom{4}{1} \quad \binom{4}{2} \quad \binom{4}{3} \quad \binom{4}{4}$$

$$\binom{5}{0} \quad \binom{5}{1} \quad \binom{5}{2} \quad \binom{5}{3} \quad \binom{5}{4} \quad \binom{5}{5}$$

Takav zapis binomnih koeficijenata poznat je kao Pascalov trokut. Trokut konstruiramo na način da je binomni koeficijent $\binom{n}{k}$ k-ti element u n-tom retku trokuta, pri čemu i retke i elemente u njima počinjemo brojati od 0. Izračunamo li te binomne koeficijente dobit ćemo sljedeći trokut:

$$1$$

$$1 \quad 1$$

$$1 \quad 2 \quad 1$$

$$1 \quad 3 \quad 3 \quad 1$$

$$1 \quad 4 \quad 6 \quad 4 \quad 1$$

$$1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1$$

Iz Pascalova identiteta 3.5 slijedi da je svaki element trokuta jednak zbroju dvaju elemenata iznad njega. Primjerice, $\binom{5}{2} = \binom{4}{1} + \binom{4}{2}$, odnosno $10 = 4+6$. Nadalje, prvi i zadnji element u svakom retku jednak je 1, budući da je $\binom{n}{0} = \binom{n}{n} = 1$. Na taj način jednostavno je konstruirati trokut do željenog retka.

3.2 Definicija i osnovna svojstva q-binomnih koeficijenata

Neka je $V = (\mathbb{F}_q)^n$ n-dimenzionalni vektorski prostor nad konačnim poljem $\mathbb{F}_q$. Broj vektora u V očito je jednak q^n.

Definicija 3.6. Gaussov koeficijent $\begin{bmatrix} n \\ k \end{bmatrix}_q$ *je broj k-dimenzionalnih potprostora vektorskog prostora V.*

Propozicija 3.7.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)...(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)...(q-1)}$$

Dokaz. Uređena k-torka vektora linearno je nezavisna ako i samo ako nijedan vektor ne leži u potprostoru razapetim prethodnim vektorima. Prema tome, prvi vektor može biti bilo koji osim nulvektora ($q^n - 1$ mogućnosti); drugi mora ležati izvan 1-dimenzionalnog potprostora određenog prvim vektorom ($q^n - q$ mogućnosti); i, općenito, i-ti vektor mora ležati izvan $(i-1)$-dimenzionalnog potprostora određenog prethodnim vektorima ($q^n - q^{i-1}$ mogućnosti). Množenjem tih brojeva dobit ćemo broj linearno nezavisnih k-torki vektora iz V i on je jednak $(q^n-1)(q^n-q)...(q^n-q^{k-1})$.

Sada je k-dimenzionalan potprostor određen s k linearno nezavisnih vektora i te smo prebrojali. Međutim, potprostor može imati mnogo različitih baza. Stoga, taj broj moramo podijeliti brojem linearno nezavisnih k-torki u k-dimenzionalnom potprostoru, koji dobijemo na isti način, stavljajući u formulu k na mjesto n.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^n-q)\dots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\dots(q^k-q^{k-1})}$$

$$= \frac{q \cdot q^2 \cdot \ldots \cdot q^{k-1}(q^n-1)(q^{n-1}-1)\dots(q^{n-(k-1)}-1)}{q \cdot q^2 \cdot \ldots \cdot q^{k-1}(q^k-1)(q^{k-1}-1)\dots(q-1)}$$

$$= \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}$$

Time smo dobili traženu formulu. □

Primjer. Neka je $n = 4$ i $k = 2$. Uvrštavanjem u formulu dobit ćemo

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{(q^4-1)(q^3-1)}{(q^2-1)(q-1)} = \left(q^2+1\right)\left(q^2+q+1\right) = q^4+q^3+2q^2+q+1.$$

Korolar 3.8. *Broj regularnih $n \times n$ matrica nad $\mathbb{F}_q$ jednak je*

$$(q^n - 1)(q^n - q) \ldots \left(q^n - q^{n-1}\right)$$

Dokaz. Kvadratna matrica je regularna ako i samo ako su joj retci linearno nezavisni. U dokazu prethodne propozicije prebrojali smo sve linearno nezavisne n-torke. □

Regularne $n \times n$ matrice formiraju grupu, takozvanu opću linearnu grupu $GL(n, q)$.

Definicija 3.9. *Produkt vektora $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$ iz V je skalar $x \cdot y = \sum_{i=1}^{n} x_i y_i$. Kažemo da su x i y ortogonalni ako je $x \cdot y = 0$.*

Produkt ima slična svojstva kao skalarni produkt na realnom vektorskom prostoru:

1. simetričnost: $x \cdot y = y \cdot x$, $\forall x, y \in V$ i
2. bilinearnost: $(\alpha x + \beta y) \cdot z = \alpha(x \cdot z) + \beta(y \cdot z)$, $\forall x, y, z \in V$, $\alpha, \beta \in \mathbb{F}_q$.

Svojstvo pozitivnosti nema smisla jer u konačnom polju nemamo uređaj. Osim toga, produkt vektora sa samim sobom može biti nula i za vektore različite od nulvektora. Naprimjer, za $x = (1, 1) \in (\mathbb{F}_2)^2$ je $x \cdot x = 0$.

Definicija 3.10. *Neka je A potprostor od V te neka je $A^\perp = \{x \in V \mid x \cdot y = 0, \forall y \in A\}$.*

Lema 3.11. *Ako je $\dim A = k$, onda je $A^\perp$ potprostor dimenzije $n - k$.*

Dokaz. Neka vektori $a_1, a_2, \ldots, a_k \in A$ čine bazu potprostora A. Za vektor $x \in V$ vrijedi $x \in A^\perp$ ako i samo ako je $x \cdot a_i = 0$, za $i = 1, \ldots, k$. Nužnost je očita jer vektori $a_1, \ldots, a_k$ pripadaju potprostoru A. Za dovoljnost primijetimo da se svaki vektor $y \in A$ može napisati kao linearna kombinacija $y = \sum_{i=1}^{k} \alpha_i a_i$. Ako je $x \in V$ ortogonalan na $a_1, \ldots, a_k$, onda vrijedi $x \cdot y = x \cdot (\sum_{i=1}^{k} \alpha_i a_i) = \sum_{i=1}^{k} \alpha_i (x \cdot a_i) = 0$, pa je ortogonalan i na y. Prema tome, $A^\perp$ je skup rješenja sustava homogenih linearnih jednadžbi $x \cdot a_i = 0$, $i = 1, \ldots, k$. Riječ je o potprostoru dimenzije $n - k$ jer su vektori $a_1, \ldots, a_k$ linearno nezavisni. □

Usprkos tome što je $\dim A + \dim A^\perp = n$, $A^\perp$ ne mora biti ortogonalni komplement od A. Presjek $A \cap A^\perp$ nije uvijek trivijalan, a suma $A + A^\perp$ može biti pravi potprostor od V.

Lema 3.12. *Za svaki potprostor $A \leq V$ vrijedi $\left(A^\perp\right)^\perp = A$.*

Dokaz. Inkluzija $A \subseteq \left(A^{\perp}\right)^{\perp}$ slijedi direktno iz definicije 3.10. Po lemi 3.11 to su potprostori iste dimenzije k, pa vrijedi jednakost. □

Propozicija 3.13.

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ n-k \end{bmatrix}_q$$

Dokaz. 1. način - algebarski dokaz

$$\begin{bmatrix} n \\ n-k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-n+k+1}-1)}{(q^{n-k}-1)(q^{n-k-1}-1)\dots(q-1)}$$

$$= \frac{(q^n-1)(q^{n-1}-1)\dots(q^{k+1}-1)}{(q^{n-k}-1)(q^{n-k-1}-1)\dots(q-1)} \cdot \frac{(q^k-1)(q^{k-1}-1)\dots(q-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}$$

$$= \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)} = \begin{bmatrix} n \\ k \end{bmatrix}_q$$

2. način - kombinatorni dokaz. Jednakost slijedi iz bijekcije između k-dimenzionalnih potprostora A prostora V i $(n-k)$-dimenzionalnih potprostora $A^{\perp}$ prostora V. Označimo s $\mathcal{L}_k(V)$ skup svih k-dimenzionalnih potprostora vektorskog prostora V. Definirajmo funkciju $f : \mathcal{L}_k(V) \to \mathcal{L}_{n-k}(V)$, $f(A) = A^{\perp}$. Ta funkcija jest bijekcija budući da ima svoju inverznu funkciju $f^{-1} : \mathcal{L}_{n-k}(V) \to \mathcal{L}_k(V)$, $f^{-1}(A) = A^{\perp}$. Zbog svojstva $\left(A^{\perp}\right)^{\perp} = A$ iz leme 3.12 vrijedi $f^{-1} \circ f = id_{\mathcal{L}_k(V)}$ i $f \circ f^{-1} = id_{\mathcal{L}_{n-k}(V)}$. □

Propozicija 3.14.

$$\left(q^k-1\right) \begin{bmatrix} n \\ k \end{bmatrix}_q = (q^n-1) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$$

Dokaz. 1. način - algebarski dokaz

$$(q^n-1) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q = (q^n-1) \frac{(q^{n-1}-1)(q^{n-2}-1)\dots(q^{n-1-k+1+1}-1)}{(q^{k-1}-1)(q^{k-2}-1)\dots(q-1)}$$

$$= \frac{q^k-1}{q^k-1} \cdot (q^n-1) \frac{(q^{n-1}-1)(q^{n-2}-1)\dots(q^{n-k+1}-1)}{(q^{k-1}-1)(q^{k-2}-1)\dots(q-1)}$$

$$= \left(q^k-1\right) \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)} = \left(q^k-1\right) \begin{bmatrix} n \\ k \end{bmatrix}_q$$

2. način - kombinatorni dokaz. Gledamo skup svih parova (A, x) koji se sastoje od k-dimenzionalnih potprostora A prostora V i nekog elementa x tog potprostora, različitog od nulvektora: $\{(A, x) \mid A \leq V, \dim A = k, x \in A, x \neq$

$0\}$. Odabir takvog para možemo izvršiti na način da prvo izaberemo $A \leq V$, a zatim unutar njega vektor x, ili tako da prvo izaberemo $x \in V$ i potom ga nadopunimo do k-dimenzionalnog potprostora A. Neka je V' direktan komplement od $[x]$, odnosno $V = [x] \oplus V'$, $\dim V' = n-1$. Sada imamo bijekciju između k-dimenzionalnih potprostora A prostora V, koji sadrže x i proizvoljnih $(k-1)$-dimenzionalnih potprostora od V', $A \longmapsto A \cap V'$. Proizvoljni $(k-1)$-dimenzionalni potprostor od V' možemo izabrati na $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ načina. Dakle, odaberemo li prvo A, zatim unutar njega vektor x, to možemo učiniti na ukupno $\begin{bmatrix} n \\ k \end{bmatrix}_q \left(q^k - 1\right)$ načina, a odaberemo li prvo $x \in V$, a zatim $(k-1)$-dimenzionalan potprostor od V', to možemo učiniti na $(q^n - 1) \begin{bmatrix} n-1 \\ k-1 \end{bmatrix}_q$ načina. Na oba načina prebrojili smo elemente istog skupa parova, pa su rezultati jednaki. □

Propozicija 3.15.

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n \\ k \end{bmatrix}_q$$

Dokaz. 1. način - algebarski dokaz.

$$\begin{bmatrix} n \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)\dots(q^{n-k}-1)}{(q^{k-1}-1)\dots(q-1)} + q^k \cdot \frac{(q^n-1)\dots(q^{n-k+1}-1)}{(q^k-1)\dots(q-1)}$$

$$= \frac{(q^n-1)\dots(q^{n-k}-1)(q^k-1) + q^k(q^n-1)\dots(q^{n-k+1}-1)}{(q^k-1)\dots(q-1)}$$

$$= \frac{(q^n-1)\dots(q^{n-k}-1)\cdot\left[q^k-1+q^k(q^{n-k+1}-1)\right]}{(q^k-1)\dots(q-1)}$$

$$= \frac{(q^n-1)\dots(q^{n-k}-1)\cdot\left[q^k-1+q^{n+1}-q^k\right]}{(q^k-1)\dots(q-1)}$$

$$= \frac{(q^{n+1}-1)(q^n-1)\dots(q^{n-k}-1)}{(q^k-1)\dots(q-1)} = \begin{bmatrix} n+1 \\ k \end{bmatrix}_q$$

2. način - kombinatorni dokaz. Neka je V $(n+1)$-dimenzionalni vektorski prostor nad $\mathbb{F}_q$ i $x_0 \in V$, $x_0 \neq 0$ čvrsti vektor. Skup svih k-dimenzionalnih potprostora od V ima $\begin{bmatrix} n+1 \\ k \end{bmatrix}_q$ članova i možemo ga podijeliti na dva disjunktna podskupa: potprostore koji sadrže x_0 i potprostore koji ne sadrže x_0. Označimo $\mathcal{P}_1 = \{A \leq V \mid \dim A = k, x_0 \in A\}$, $\mathcal{P}_2 = \{A \leq V \mid \dim A = k, x_0 \notin A\}$. Očito je $\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = |\mathcal{P}_1| + |\mathcal{P}_2|$, pa preostaje prebrojiti skupove $\mathcal{P}_1$ i $\mathcal{P}_2$. Neka je V' direktni komplement od $[x_0]$, tj. $V = [x_0] \oplus V'$. Slično kao u

dokazu propozicije 3.14, imamo bijekciju između k-dimenzionalnih potprostora od V koji sadrže x_0 i proizvoljnih $(k-1)$-dimenzionalnih potprostora od V'. Stoga je $|\mathcal{P}_1| = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q$. Da bismo prebrojali elemente od $\mathcal{P}_2$, primijetimo da direktni komplement V' nije jedinstven. Broj različitih direktnih komplemenata dobivamo tako da prebrojimo dopune vektora x_0 do baze $\{x_0, x_1, \ldots, x_n\}$ od V i podijelimo s brojem uređenih baza od V':

$$\frac{(q^{n+1}-q)(q^{n+1}-q^2)\ldots(q^{n+1}-q^n)}{(q^n-1)(q^n-q)\ldots(q^n-q^{n-1})} = q^n.$$

Svaki k-dimenzionalni potprostor A koji ne sadrži x_0 leži u nekom direktnom komplementu V', pa parova (A, V') ima ukupno $q^n \cdot \begin{bmatrix} n \\ k \end{bmatrix}_q$. Broj potprostora iz $\mathcal{P}_2$ dobijemo tako da podijelimo taj broj s brojem direktnih komplemenata V' kroz fiksni A,

$$\frac{(q^{n+1}-q^{k+1})(q^{n+1}-q^{k+2})\ldots(q^{n+1}-q^n)}{(q^n-q^k)(q^n-q^{k+1})\ldots(q^n-q^{n-1})} = q^{n-k}.$$

Dakle,

$$|\mathcal{P}_2| = \frac{q^n}{q^{n-k}} \begin{bmatrix} n \\ k \end{bmatrix}_q = q^k \cdot \begin{bmatrix} n \\ k \end{bmatrix}_q.$$

Time je jednakost dokazana. □

Analogno Pascalovom trokutu, konstruirat ćemo q-Pascalov trokut.

$$\begin{bmatrix} 0 \\ 0 \end{bmatrix}_q$$

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}_q \qquad \begin{bmatrix} 1 \\ 1 \end{bmatrix}_q$$

$$\begin{bmatrix} 2 \\ 0 \end{bmatrix}_q \qquad \begin{bmatrix} 2 \\ 1 \end{bmatrix}_q \qquad \begin{bmatrix} 2 \\ 2 \end{bmatrix}_q$$

$$\begin{bmatrix} 3 \\ 0 \end{bmatrix}_q \qquad \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q \qquad \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q \qquad \begin{bmatrix} 3 \\ 3 \end{bmatrix}_q$$

$$\begin{bmatrix} 4 \\ 0 \end{bmatrix}_q \qquad \begin{bmatrix} 4 \\ 1 \end{bmatrix}_q \qquad \begin{bmatrix} 4 \\ 2 \end{bmatrix}_q \qquad \begin{bmatrix} 4 \\ 3 \end{bmatrix}_q \qquad \begin{bmatrix} 4 \\ 4 \end{bmatrix}_q$$

Izračunavajući q-binomne koeficijente dobivamo sljedeći trokut:

$$
\begin{array}{ccccccc}
 & & & 1 & & & \\
 & & 1 & & 1 & & \\
 & 1 & & 1+q & & 1 & \\
1 & & 1+q & & 1+q & & 1 \\
 & & +q^2 & & +q^2 & & \\
1 & 1+q & & 1+q & & 1+q & 1 \\
 & +q^2+q^3 & & +2q^2+q^3+q^4 & & +q^2+q^3 &
\end{array}
$$

Iz propozicije 3.15 slijedi da se svaki koeficijent $\begin{bmatrix} n \\ k \end{bmatrix}_q$ u trokutu dobiva zbrajanjem koeficijenta iznad lijevo i koeficijenta iznad desno pomnoženog s q^k. Primjerice, $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \begin{bmatrix} 3 \\ 1 \end{bmatrix}_q + q^2 \cdot \begin{bmatrix} 3 \\ 2 \end{bmatrix}_q$, odnosno $\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = 1 + q + q^2 + q^2 \cdot (1 + q + q^2) = 1 + q + q^2 + q^2 + q^3 + q^4 = 1 + q + 2q^2 + q^3 + q^4$.

Gaussovi koeficijenti imaju kombinatornu interpretaciju za sve pozitivne cjelobrojne vrijednosti $q > 1$, ne samo za prim potencije. Promatrat ćemo matrice $A = (a_{ij})$ u kanonskom obliku, za koje vrijede sljedeća tri uvjeta:

- svaki redak matrice A ili je jednak nuli ili mu je prvi nenul element jednak 1 (takozvani "vodeći 1")
- za svaki $i > 1$, ako je i-ti redak različit od nule, tada je $(i-1)$-vi redak također različit od nule, a njegov vodeći 1 je lijevo u odnosu na vodeći 1 i-tog retka
- ako stupac sadrži vodeći 1 nekog retka, tada su mu svi ostali elementi jednaki nuli

Slijedi nekoliko primjera matrica u kanonskom obliku:

$$
\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 0 & 0 & \dots \\ 0 & 1 & 0 & \dots \\ 0 & 0 & 0 & \dots \\ \vdots & \vdots & \vdots & \ddots \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.
$$

Propozicija 3.16. *Bilo koja matrica nad poljem može se dovesti u kanonski oblik pomoću elementarnih transformacija nad recima. Dvije matrice imaju isti kanonski oblik ako i samo ako im reci razapinju isti potprostor.*

Dokaz. Zamjenom redaka možemo postići da redak u kojem se nenul element pojavljuje u stupcu s najmanjim indeksom bude prvi redak. Zatim množenjem s recipročnim skalarom taj prvi nenul element pretvorimo u 1, te poništimo sve elemente ispod njega dodavanjem prvog retka pomnoženog odgovarajućim skalarom. Postupak ponavljamo s drugim retkom itd. dok ne dobijemo matricu u kanonskom obliku.

Elementarnim transformacijama nad recima ne mijenja se potprostor razapet recima matrice. Zato ako se dvije matrice elementarnim transformacijama nad recima mogu dovesti u isti oblik, onda im reci razapinju isti potprostor. Obrnuto, pretpostavimo da reci dviju matrica u kanonskom obliku razapinju isti potprostor. Tada se prvi redak druge matrice može prikazati kao linearna kombinacija redaka prve matrice, a zbog vodećih jedinica i zbog ostalih svojstava kanonskih matrica zaključujemo da je jednak prvom retku prve matrice. Analogno zaključujemo da drugi redak druge matrice mora biti jednak drugom retku prve matrice itd. dok ne dobijemo da su te dvije matrice jednake. □

Propozicija 3.17. *Retci matrice nad poljem u kanonskom obliku su linearno nezavisni ako i samo ako je zadnji redak različit od nule.*

Dokaz. Ako je bilo koji redak matrice jednak nuli, onda su reci očito linearno zavisni. Obrnuto, neka je zadnji redak matrice u kanonskom obliku različit od nule. Tada su zbog svojstva matrica u kanonskom obliku i svi prethodni reci različiti od nule i sadrže jedinicu na mjestu na kojem svi ostali reci imaju nule. Zato su reci takve matrice linearno nezavisni. □

Zbog prethodne dvije propozicije broj $k \times n$ matica u kanonskom obliku nad poljem $\mathbb{F}_q$ bez nulredaka jednak je broju k-dimenzionalnih potprostora vektorskog prostora $V = (\mathbb{F}_q)^n$, a to je Gaussov koeficijent $\begin{bmatrix} n \\ k \end{bmatrix}_q$.

Primjer. Neka je $n = 4$ i $k = 2$. Iz formule slijedi:

$$\begin{bmatrix} 4 \\ 2 \end{bmatrix}_q = \frac{(q^4-1)(q^3-1)}{(q^2-1)(q-1)} = \frac{(q^2-1)(q^2+1)(q-1)(q^2+q+1)}{(q^2-1)(q-1)}$$

$$= (q^2+1)(q^2+q+1) = q^4+q^3+2q^2+q+1.$$

Provjerit ćemo rješenje prebrojavanjem matrica. Mogući su sljedeći oblici:

$$\begin{bmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{bmatrix}, \begin{bmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{bmatrix}, \begin{bmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

$$\begin{bmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{bmatrix}, \begin{bmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

gdje * označava proizvoljan element. Dakle, imamo $q^4+q^3+q^2+q^2+q+1$ matrica.

Neka je sada $q \in \mathbb{N}$, $q \geq 2$ bilo koji prirodni broj (ne nužno prim potencija i Q proizvoljan q-člani skup koji sadrži dva istaknuta elementa 0 i 1. Nad skupom Q ne možemo izgraditi vektorski prostor i ne možemo prebrojavati potprostore, ali svejedno možemo definirati matrice u kanonskom obliku nad Q. Štoviše, broj takvih matrica jednak je izrazu iz propozicije 3.7.

Teorem 3.18. *Broj $k \times n$ matrica u kanonskom obliku bez nulredaka nad proizvoljnim q-članim skupom Q jednak je*

$$\frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}.$$

Dokaz. Neka se vodeće jedinice nalaze u stupcima s indeksima $j_1 < j_2 < \dots < j_k$. U zadnjem retku imamo nule lijevo od vodeće jedinice, a desno može biti bilo koji element iz Q, dakle možemo ga izabrati na q^{n-j_k} načina. Predzadnji redak ima jednu nulu desno od vodeće jedinice u stupcu s indeksom j_k, pa je broj izbora za predzadnji redak jednak $q^{n-j_{k-1}-1}$. Analogno, broj izbora za i-ti redak matrice je q^{n-j_i-k+i}. Ukupan broj takvih matrica je

$$\prod_{1=1}^{k} q^{n-j_i-k+i} = q^{n\cdot k-k^2+\sum_{i=1}^k i-\sum_{i=1}^k j_i} = q^{n\cdot k-\binom{k}{2}-\sum_{i=1}^k j_i},$$

a ukupan broj svih matrica u kanonskom obliku je

$$\sum_{1\leq j_1<j_2<\dots<j_k\leq n} q^{n\cdot k-\binom{k}{2}-\sum_{i=1}^k j_i}.$$

Vidimo da je ovo polinom u varijabli q, koji se s polinomom

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}$$

podudara za sve primpotencije q. Zato su ta dva polinoma jednaka, tj. podudaraju se za sve $q \in \mathbb{N}$, $q \geq 2$. □

Sada možemo dati još jedan dokaz propozicije 3.15, s pomoću matrica u kanonskom obliku.

Dokaz. Neka su $k \times (n+1)$ matrice u kanonskom obliku, bez nulredaka. Podijelimo ih u dvije kategorije: one kojima je vodeći 1 u zadnjem retku zadnjeg stupca i ostale. Prvi tip korespondira $(k-1) \times n$ matricama u kanonskom obliku bez nulredaka, budući da je zadnji stupac i redak jednak nuli, osim donjeg desnog elementa. One drugog tipa čine $k \times n$ matrice u kanonskom obliku bez nulredaka, sa stupcima koji sadrže proizvoljne elemente pridružene s desne strane. Budući da postoji q^k mogućnosti za taj stupac, slijedi formula

$$\begin{bmatrix} n+1 \\ k \end{bmatrix}_q = \begin{bmatrix} n \\ k-1 \end{bmatrix}_q + q^k \begin{bmatrix} n \\ k \end{bmatrix}_q .$$

□

3.3 Binomni i q-binomni teorem

Binom je polinom koji se sastoji od dva člana.

Teorem 3.19. *(*Binomni teorem*)*

$$(1+t)^n = \sum_{k=0}^{n} \binom{n}{k} t^k$$

Dokaz. 1. način. Očito je $(1+t)^n$ polinom n-tog stupnja. Raspišimo ga kao produkt n faktora:

$$(1+t)^n = (1+t)(1+t)\dots(1+t).$$

Ovaj izraz možemo raspisati na način da iz svake zagrade odaberemo 1 ili t na sve moguće načine, odabrani članove pomnožimo i na kraju sve sumiramo. Ako je, primjerice, t uzet iz k faktora, onda je 1 uzet iz preostalih $n-k$ faktora. Time dobijemo izraz t^k koji možemo izabrati na $\binom{n}{k}$ načina. Dakle, koeficijent uz t^k je $\binom{n}{k}$. No, k može varirati od 0 do n iz čega slijedi binomna formula.

2. način. Teorem možemo dokazati i matematičkom indukcijom. Za $n = 0$ očito slijedi $(1+t)^0 = 1$. Pretpostavimo da tvrdnja vrijedi za neki n. Pokažimo da vrijedi i za $n+1$.

$$(1+t)^{n+1} = (1+t)^n(1+t) = \left(\sum_{k=0}^{n} \binom{n}{k} t^k\right)(1+t)$$

$$= \sum_{k=0}^{n} \binom{n}{k} t^k + \left(\sum_{k=0}^{n} \binom{n}{k} t^k\right) t = \sum_{k=0}^{n} \binom{n}{k} t^k + \sum_{k=0}^{n-1} t^{k+1} + \binom{n}{n} t^{n+1}$$

$$= t^0 + \sum_{k=1}^{n} \binom{n}{k} t^k + \sum_{k=1}^{n} \binom{n}{k-1} t^k + t^{n+1} = 1 + \sum_{k=1}^{n} \left[\binom{n}{k} + \binom{n}{k-1} \right] t^k + t^{n+1}$$

$$= 1 + \sum_{k=1}^{n} \binom{n+1}{k} t^k + t^{n+1} = \sum_{k=0}^{n+1} \binom{n+1}{k} t^k$$

Pokazali smo da tvrdnja vrijedi za $n+1$, što znači da vrijedi za bilo koji n. □

Teorem 3.20. *(*q-binomni teorem*) Za svaki $n \geq 1$ vrijedi*

$$\prod_{i=0}^{n-1} (1 + q^i t) = \sum_{k=0}^{n} q^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q t^k$$

Dokaz. Dokaz slijedi matematičkom indukcijom. Za $n = 1$, obje strane jednake su $1 + t$. Pretpostavimo da je tvrdnja istinita za neki n. Tada

$$\prod_{i=0}^{n} (1 + q^i t) = \left(\sum_{k=0}^{n} q^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q t^k \right) \cdot (1 + q^n t)$$

Koeficijent uz t^k jednak je

$$q^{k(k-1)/2} \begin{bmatrix} n \\ k \end{bmatrix}_q + q^{(k-1)(k-2)/2} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q q^n = q^{k(k-1)/2} \left(\begin{bmatrix} n \\ k \end{bmatrix}_q + q^{n-k+1} \begin{bmatrix} n \\ k-1 \end{bmatrix}_q \right)$$

$$= q^{k(k-1)/2} \begin{bmatrix} n+1 \\ k \end{bmatrix}_q$$

kao što se traži. □

Ako Gaussove koeficijente gledamo kao funkciju realne varijable q (gdje su n i k cjelobrojne konstante), tada je

$$\lim_{q \to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \binom{n}{k}.$$

Prema l'Hopitalovom pravilu, imamo

$$\lim_{q \to 1} \frac{q^a - 1}{q^b - 1} = \lim_{q \to 1} \frac{a q^{a-1}}{b q^{b-1}} = \frac{a}{b},$$

za $a, b \neq 0$. Slijedi

$$\lim_{q \to 1} \begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{n\,(n-1) \ldots (n-k+1)}{k\,(k-1) \ldots 1} = \binom{n}{k}.$$

Uzimanjem limesa $q \to 1$ q-binomni teorem prelazi u obični binomni teorem.

4 Stirlingovi brojevi druge vrste i njihovi q-analogoni

4.1 Stirlingovi brojevi druge vrste

Definicija 4.1. *Neka je S dani skup. Svaki podskup $\mathcal{P}$ od $\mathcal{P}(S)\backslash\{\emptyset\}$ zovemo* particijom skupa *S ako su ispunjena sljedeća dva uvjeta:*

1. *unija svih elemenata iz $\mathcal{P}$ jednaka je skupu S.*
2. *ako su A i B različiti elementi iz $\mathcal{P}$, tada je $A \cap B = \emptyset$.*

Primjer. Neka je dan skup $S = \{a, b, c\}$. Tada su particije tog skupa:

$$\mathcal{P}_1 = \{\{a\}, \{b\}, \{c\}\},$$
$$\mathcal{P}_2 = \{\{a, b\}, \{c\}\},$$
$$\mathcal{P}_3 = \{\{a, c\}, \{b\}\},$$
$$\mathcal{P}_4 = \{\{b, c\}, \{a\}\},$$
$$\mathcal{P}_5 = \{\{a, b, c\}\}.$$

Ukupno imamo 5 takvih particija.

Definicija 4.2. Stirlingov broj druge vrste $\left\{ {n \atop k} \right\}$ *prebrojava na koliko načina možemo podijeliti n-člani skup u k nepraznih podskupova.*

Još kažemo da Stirlingov broj druge vrste $\left\{ {n \atop k} \right\}$ prebrojava k-particije n-članog skupa.

Primjer. Neka je $n = 4$ i $k = 2$. Imamo li primjerice skup $\{a, b, c, d\}$, možemo ga podijeliti u dva neprazna podskupa na sljedeće načine:

$$\{\{a, b, c\}, \{d\}\},\ \{\{a, b, d\}, \{c\}\},\ \{\{a, c, d\}, \{b\}\},\ \{\{b, c, d\}, \{a\}\}$$
$$\{\{a, b\}, \{c, d\}\},\ \{\{a, c\}, \{b, d\}\},\ \{\{a, d\}, \{b, c\}\}.$$

Prebrojavanjem vidimo da postoji sedam 2-particija 4-članog skupa, odnosno $\left\{ {4 \atop 2} \right\} = 7$.

Iz definicije slijedi nekoliko specijalnih slučajeva broja $\left\{ {n \atop k} \right\}$:

1. $0 \leq n < k$
   Ovdje trebamo n-člani skup prikazati pomoću k-particija. Budući da skup ima manje elemenata nego podskupova u koje ih moramo raspodijeliti, očito bi postojao barem jedan prazan podskup, što je u kontradikciji s definicijom. Zaključujemo da u tom slučaju n-člani skup ne možemo prikazati k-particijom, tj.

$$\left\{ {n \atop k} \right\} = 0, n < k$$

2. $n = k$
   Ukoliko su n i k jednaki brojevi, vrlo je jednostavno zaključiti kako postoji točno jedna n-particija n-članog skupa i to takva da je u svakom podskupu točno jedan element skupa.

$$\left\{ {n \atop n} \right\} = 1, \forall n \in \mathbb{N}.$$

   Posebno definiramo $\left\{ {0 \atop 0} \right\} = 1$.

3. $k = 0$
   Zanima nas broj svih 0-particija skupa od n elemenata. Očito nemamo niti jednu particiju te vrijedi

$$\left\{ {n \atop 0} \right\} = 0, \forall n \in \mathbb{N}.$$

4. $k = 1$
   Tražimo broj svih 1-particija n-članog skupa. Očito postoji samo jedna takva particija. Zaključujemo

$$\left\{ {n \atop 1} \right\} = 1, \forall n \in \mathbb{N}.$$

5. $k = 2$
   Pogledajmo koliko iznosi $\left\{ {n \atop 2} \right\}$, pri čemu uzimamo da je $n \geq k$. U tom slučaju nam je dovoljno prebrojati koliko postoji podskupova n-članog skupa, a drugi podskup koji s njim daje 2-particiju nas ne zanima, budući da njega dobijemo kao komplement prvog podskupa na cijelom n-članom skupu. Znamo da je broj svih podskupova n-članog skupa jednak 2^n. Međutim, od tog broja oduzimamo 2 jer je u podskupove uračunat prazan skup i cijeli skup koji nemaju svoje komplemente s kojima mogu činiti 2-particiju skupa. Također, prebrojavajući podskupove na taj način dobivamo po dvije iste 2-particije. Primjerice, gledajući skup iz prethodnog primjera, vidimo da je komplement skupa $\{a\}$ na skupu $\{a, b, c, d\}$ skup $\{b, c, d\}$ i obratno. Tako bismo dobili za svaki podskup pa zbog toga dijelimo sve s 2. Dolazimo do zaključka da vrijedi

$$\left\{ {n \atop 2} \right\} = \frac{2^n - 2}{2} = 2^{n-1} - 1.$$

Općenito, Stirlingove brojeve možemo računati koristeći sljedeću rekurzivnu formulu:

Propozicija 4.3.

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k \left\{ {n-1 \atop k} \right\}, n \geq 2.$$

Analogno binomnim koeficijentima i njihovim q-analogonima i za Stirlingove brojeve druge vrste imamo Stirlingov trokut za particije.

$$\begin{array}{ccccccccccccc}
 & & & & & & \left\{ {0 \atop 0} \right\} & & & & & & \\
 & & & & & \left\{ {1 \atop 0} \right\} & & \left\{ {1 \atop 1} \right\} & & & & & \\
 & & & & \left\{ {2 \atop 0} \right\} & & \left\{ {2 \atop 1} \right\} & & \left\{ {2 \atop 2} \right\} & & & & \\
 & & & \left\{ {3 \atop 0} \right\} & & \left\{ {3 \atop 1} \right\} & & \left\{ {3 \atop 2} \right\} & & \left\{ {3 \atop 3} \right\} & & & \\
 & & \left\{ {4 \atop 0} \right\} & & \left\{ {4 \atop 1} \right\} & & \left\{ {4 \atop 2} \right\} & & \left\{ {4 \atop 3} \right\} & & \left\{ {4 \atop 4} \right\} & & \\
 & \left\{ {5 \atop 0} \right\} & & \left\{ {5 \atop 1} \right\} & & \left\{ {5 \atop 2} \right\} & & \left\{ {5 \atop 3} \right\} & & \left\{ {5 \atop 4} \right\} & & \left\{ {5 \atop 5} \right\} & \\
\left\{ {6 \atop 0} \right\} & & \left\{ {6 \atop 1} \right\} & & \left\{ {6 \atop 2} \right\} & & \left\{ {6 \atop 3} \right\} & & \left\{ {6 \atop 4} \right\} & & \left\{ {6 \atop 5} \right\} & & \left\{ {6 \atop 6} \right\}
\end{array}$$

Odnosno:

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 0 & & 1 & & & & & \\
 & & & & 0 & & 1 & & 1 & & & & \\
 & & & 0 & & 1 & & 3 & & 1 & & & \\
 & & 0 & & 1 & & 7 & & 6 & & 1 & & \\
 & 0 & & 1 & & 15 & & 25 & & 10 & & 1 & \\
0 & & 1 & & 31 & & 90 & & 65 & & 15 & & 1
\end{array}
$$

Iz propozocije 4.3 slijedi da je svaki element $\left\{ {n \atop k} \right\}$ trokuta jednak zbroju elementa iznad lijevo i elementa iznad desno pomnoženog s k. Primjerice, $\left\{ {5 \atop 3} \right\} = \left\{ {4 \atop 2} \right\} + 3 \cdot \left\{ {4 \atop 3} \right\}$, odnosno $\left\{ {5 \atop 3} \right\} = 7 + 3 \cdot 6 = 25$.

Ukupni broj svih particija nekog n-članog skupa nazivamo Bellov broj i označavamo ga B_n. Očito vrijedi

$$B_n = \sum_{k=1}^{n} \left\{ {n \atop k} \right\}, \forall n \in \mathbb{N}.$$

Primjer. Uzmimo već spominjani skup $\{a, b, c, d\}$. Nabrojimo sada sve particije tog skupa:
$\{a, b, c, d\}$,
$\{\{a, b, c\}, \{d\}\}, \{\{a, b, d\}, \{c\}\}, \{\{a, c, d\}, \{b\}\}, \{\{b, c, d\}, \{a\}\}, \{\{a, b\}, \{c, d\}\}$,
$\{\{a, c\}, \{b, d\}\}, \{\{a, d\}, \{b, c\}\}$,
$\{\{a, b\}, \{c\}, \{d\}\}, \{\{a, c\}, \{b\}, \{d\}\}, \{\{a, d\}, \{b\}, \{c\}\}, \{\{b, c\}, \{a\}, \{d\}\}, \{\{b, d\}, \{a\}, \{c\}\}$,
$\{\{c, d\}, \{a\}, \{b\}\}$,
$\{\{a\}, \{b\}, \{c\}, \{d\}\}$.
Vidimo da skup ima samo jednu 1-particiju, sedam 2-particija, šest 3-particija i jednu 4-particiju. To su ujedno i ilustracije Stirlingovih brojeva

$$\left\{ {4 \atop 1} \right\} = 1, \left\{ {4 \atop 2} \right\} = 7, \left\{ {4 \atop 3} \right\} = 6, \left\{ {4 \atop 4} \right\} = 1.$$

Ako to sve zbrojimo dobijemo Bellov broj

$$B_4 = \sum_{k=1}^{4} \left\{ {4 \atop k} \right\} = 1 + 7 + 6 + 1 = 15.$$

Jednostavnije, pri izračunavanju Bellova broja B_n možemo se poslužiti Stirlingovim trokutom za particije tako da zbrojimo sve vrijednosti traženog n-tog retka trokuta.

4.2 q-Stirlingovi brojevi druge vrste

Neka je dani n-člani skup $S = \{0, 1, 2, \ldots, n-1\}$. Stirlingov broj druge vrste prebrojava na koliko načina možemo zadani skup podijeliti u k nepraznih podskupova $\mathcal{P} = \{S_0, S_1, \ldots S_{k-1}\}$. Neka je pri tome S_0 element particije koji sadrži 0. Sada možemo definirati težinu particije $w(\mathcal{P})$.

Definicija 4.4.

$$w(\mathcal{P}) := q^{\sum_{i \in S_0} i}.$$

Za svaki skup particija A vrijedi da je težina skupa particija jednaka sumi težina svih particija tog skupa

$$w(A) := \sum_{\mathcal{P} \in A} w(\mathcal{P}).$$

Sljedeća definicija i rezultati koji iz nje proizlaze preuzeti su iz članka [3].

Definicija 4.5. *Neka je $A_{n,k}$ skup svih k-particija n-članog skupa $\{0, 1, 2, \ldots, n-1\}$. q-*Stirlingov broj $\left\{ {n \atop k} \right\}_q$ *jednak je težini skupa $A_{n,k}$*

$$\left\{ {n \atop k} \right\}_q := w(A_{n,k}).$$

Također vrijedi da je $\left\{ {0 \atop 0} \right\}_q := 1$, $\left\{ {0 \atop k} \right\}_q := 0$ i $\left\{ {n \atop 0} \right\}_q := 0$.

Primjer. Neka je $n = 4$ i $k = 2$. Izračunajmo $\left\{ {4 \atop 2} \right\}_q$.

$$\left\{ {4 \atop 2} \right\}_q = w(A_{4,2}) = w(\{\{0\}, \{1, 2, 3\}\}) + w(\{\{0, 1\}, \{2, 3\}\}) + w(\{\{0, 2\}, \{1, 3\}\})$$
$$+ w(\{\{0, 3\}, \{1, 2\}\}) + w(\{\{0, 1, 2\}, \{3\}\}) + w(\{\{0, 1, 3\}, \{2\}\}) + w(\{\{0, 2, 3\}, \{1\}\})$$
$$= 1 + q + q^2 + q^3 + q^3 + q^4 + q^5 = 1 + q + q^2 + 2q^3 + q^4 + q^5.$$

q-Stirlingovi brojevi zadovoljavaju sljedeću rekurzivnu formulu:

Propozicija 4.6.

$$\begin{Bmatrix} n+1 \\ k \end{Bmatrix}_q = \begin{Bmatrix} n \\ k-1 \end{Bmatrix}_q + (k-1+q^n)\begin{Bmatrix} n \\ k \end{Bmatrix}_q .$$

q-Stirlingovi brojevi također se mogu zapisati u trokutastom poretku na sljedeći način:

$$\begin{Bmatrix} 0 \\ 0 \end{Bmatrix}_q$$

$$\begin{Bmatrix} 1 \\ 0 \end{Bmatrix}_q \quad \begin{Bmatrix} 1 \\ 1 \end{Bmatrix}_q$$

$$\begin{Bmatrix} 2 \\ 0 \end{Bmatrix}_q \quad \begin{Bmatrix} 2 \\ 1 \end{Bmatrix}_q \quad \begin{Bmatrix} 2 \\ 2 \end{Bmatrix}_q$$

$$\begin{Bmatrix} 3 \\ 0 \end{Bmatrix}_q \quad \begin{Bmatrix} 3 \\ 1 \end{Bmatrix}_q \quad \begin{Bmatrix} 3 \\ 2 \end{Bmatrix}_q \quad \begin{Bmatrix} 3 \\ 3 \end{Bmatrix}_q$$

$$\begin{Bmatrix} 4 \\ 0 \end{Bmatrix}_q \quad \begin{Bmatrix} 4 \\ 1 \end{Bmatrix}_q \quad \begin{Bmatrix} 4 \\ 2 \end{Bmatrix}_q \quad \begin{Bmatrix} 4 \\ 3 \end{Bmatrix}_q \quad \begin{Bmatrix} 4 \\ 4 \end{Bmatrix}_q$$

Iz propozicije 4.6 slijedi da se svaki q-Stirlingov broj $\begin{Bmatrix} n \\ k \end{Bmatrix}_q$ u trokutu dobiva zbrajanjem broja iznad lijevo i broja iznad desno pomnoženog s $(k-1+q^n)$. Pomoću te činjenice i definicije 4.5 dobivamo sljedeći trokut:

$$1$$

$$0 \qquad 1$$

$$0 \qquad q \qquad 1$$

$$0 \qquad q^3 \qquad 1+q+q^2 \qquad 1$$

$$0 \qquad q^6 \qquad 1+q+q^2+2q^3+q^4+q^5 \qquad 3+q+q^2+q^3 \qquad 1$$

q-Stirlingove brojeve možemo definirati i pomoću q-binomnih koeficijenata. Prisjetimo se q-binomnog teorema:

$$(1+t)(1+qt)\dots(1+q^{n-1}t) = \sum_{i=0}^{n} q^{i(i-1)/2} \begin{bmatrix} n \\ i \end{bmatrix}_q t^i.$$

Zamijenimo li t sa qt, uspoređivanjem koeficijenata uz t^i dobivamo

$$\sum_{1 \le j_1 < j_2 < \dots < j_i \le n} q^{j_1+j_2+\dots+j_i} = q^{(i+1)i/2} \begin{bmatrix} n \\ i \end{bmatrix}_q.$$

Zapišimo particiju $\mathcal{P} \in A_{n+1,k+1}$ u obliku $\mathcal{P} = \{\{0, j_1, \dots, j_i\}, B_1, \dots, B_k\}$. Prema tome dobivamo

$$\begin{Bmatrix} n+1 \\ k+1 \end{Bmatrix}_q = w(A_{n+1,k+1}) = \sum_i \sum_{j_1 < \dots < j_i} q^{j_1+\dots j_i} \begin{Bmatrix} n-i \\ k \end{Bmatrix}.$$

Iz toga slijedi

$$\begin{Bmatrix} n+1 \\ k+1 \end{Bmatrix}_q = \sum_i \begin{bmatrix} n \\ i \end{bmatrix}_q \begin{Bmatrix} i \\ k \end{Bmatrix} q^{\binom{n-i+1}{2}}.$$

Literatura

[1] I.N. Bronštejn i suradnici, *Matematički priručnik*, Golden marketing - Tehnička knjiga, Zagreb, 2004.

[2] P.J. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, London, 1994.

[3] J. Cigler, *A new q-analog of Stirling numbers*, Österreich. Akad. Wiss. Math.-Natur. Kl. Sitzungsber. II **201** (1992), 97–109.

[4] B. Dokić, *Stirlingovi brojevi*, Osječki matematički list **13** (2013), 165–187.

[5] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odsjek, Zagreb, 2002.

[6] T.W. Hungerford, *Algebra*, Springer, New York, 2000.

[7] V. Krčadinac, J. Šiftar, *Konačne geometrije*, PMF - Matematički odsjek, Zagreb, 2013.

[8] I. Nakić, *Diskretna matematika*, PMF - Matematički odsjek, Zagreb, 2012.

[9] B. Pavković, D. Veljan, *Elementarna matematika*, Tehnička knjiga, Zagreb, 1992.

[10] Wikipedija, *Binomni poučak*, dostupno na: `https://hr.wikipedia.org/wiki/Binomni_pou%C4%8Dak` (rujan 2015.).

[11] Ž. Zrno, *Particija skupa i relacija ekvivalencije. Bellovi brojevi*, Osječki matematički list **11** (2011), 57–67.

Sažetak

U matematici postoji mnogo istaknutih nizova brojeva, poput parnih i neparnih brojeva, prostih brojeva, kvadrata i kubova brojeva, Fibonaccijevih brojeva itd. U ovom radu proučavamo neke brojeve specifične za područje kombinatorike, i to binomne koeficijente, q-binomne koeficijente (Gaussove koeficijente), Stirlingove brojeve, q-Stirlingove brojeve te Bellove brojeve.

Binomni koeficijenti $\binom{n}{k}$ brojevi su koji prebrojavaju k-člane podskupove konačnog n-članog skupa. Njihovi q-analogoni, Gaussovi koeficijenti $\begin{bmatrix} n \\ k \end{bmatrix}_q$, prebrojavaju k-dimenzionalne potprostore n-dimenzionalog vektorskog prostora nad konačnim poljem reda q. Stirlingovi brojevi druge vrste $\left\{ {n \atop k} \right\}$ prebrojavaju k-particije n-članog skupa, odnosno na koliko načina možemo podijeliti n-člani skup u k nepraznih podskupova. Bellov broj B_n je ukupan broj svih particija nekog n-članog skupa. q-Stirlingov broj $\left\{ {n \atop k} \right\}_q$ definira se kao težina skupa svih k-particija nekog n-članog skupa.

U diplomskom radu navodimo razne identitete i relacije koje vrijede za spomenute kombinatoričke brojeve. Naglašavamo sličnosti i razlike između brojeva koji prebrojavaju konačne skupove i njihovih analogona nad konačnim poljima.

Summary

In mathematics there are many interesting number sequences, such as odd and even numbers, prime numbers, square and cube numbers, Fibonacci numbers etc. This thesis studies certain numbers which are specific for the area of combinatorics, in particular binomial coefficients, q-binomial coefficients (Gaussian coefficients), Stirling numbers and q-Stirling numbers, along with brief mention of Bell numbers.

The binomial coefficient $\binom{n}{k}$ is the number of k-element subsets of a set of n elements. The q-analogue of the binomial coefficient, also called a Gaussian coefficient $\begin{bmatrix} n \\ k \end{bmatrix}_q$, counts the number of k-dimensional subspaces of an n-dimensional vector space over the finite field of order q. The Stirling number of the second kind $\left\{ {n \atop k} \right\}$ counts k-partitions of an n-element set, in other words the ways to divide a set of n elements into k nonempty subsets. Bell number B_n counts the number of all partitions of an n-element set. The q-Stirling number $\left\{ {n \atop k} \right\}_q$ is defined as a weight of the set of all k-partitions of an n-element set.

In the thesis we give various identities and relations valid for the aforementioned combinatorial numbers. We emphasise similarities and differences between numbers enumerating finite sets and their analogues over finite fields.

Životopis

Rođena sam dana 14.04.1989. godine u Varaždinu. Osnovnu i srednju školu pohađala sam u Ivancu, gdje sam i živjela. Nakon završene osnovne škole, 2002. godine upisujem Srednju školu u Ivancu, smjer opća gimnazija te po njenom završetku 2007. godine upisujem Preddiplomski sveučilišni studij Matematike, smjer nastavnički, na Prirodoslovno-matematičkom fakultetu u Zagrebu. 2011. godine upisujem Diplomski sveučilišni studij Matematika, smjer nastavnički, kojeg upravo završavam. Od 2013. radim kao nastavnica matematike. Radila sam u tri osnovne škole i to OŠ Davorina Trstenjaka u Zagrebu, OŠ Ivana Kukuljevića Sakcinskog u Ivancu i OŠ Brezovica u Brezovici.