Kongruencije za binomne koeficijente

Grgić, Monika

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Monika Grgić

KONGRUENCIJE ZA BINOMNE KOEFICIJENTE

Diplomski rad

Voditelj rada:
doc.dr.sc. Tomislav Pejković

Zagreb, srpanj 2021.

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. _____

Zahvaljujem se svom mentoru, doc. dr. sc. Tomislavu Pejkoviću na uloženom vremenu, strpljenju, razumijevanju i stručnoj pomoći prilikom izrade diplomskog rada.

Želim se zahvaliti svojim roditeljima, sestri, šogoru i prijateljima koji su mi omogućili studiranje i bili podrška na mom obrazovnom putu.

Posebno se zahvaljujem divnim kolegicama na uzajamnoj pomoći, svakoj riječi podrške i osmijehu. Hvala cimerici što mi je studiranje učinila ljepšim.

Hvala i dragom Bogu za svaku uslišanu molitvu i obilje milosti.

Sadržaj

Uvod

U ovom diplomskom radu razmatraju se ostatci pri dijeljenju binomnih koeficijenata s potencijama prostih brojeva.

U prvom poglavlju navedeni su pojmovi i tvrdnje vezani uz djeljivost i binomne koeficijente te je objašnjena konstrukcija Pascalovog trokuta i njegov povijesni razvoj. U drugom poglavlju istaknuti su teoremi Lucasa, Legendrea i Kummera koji se primjenjuju u daljnjem radu.

U iduća dva poglavlja izloženi su klasični i noviji rezultati vezani uz problem ostataka pri dijeljenju binomnih koeficijenta s prostim brojem te su interpretirani unutar Pascalovog trokuta. Najprije su u trećem poglavlju navedeni rezultati za konkretne module, manje prirodne brojeve, a zatim u četvrtom poglavlju rezultati vezani uz module koji su prosti brojevi. U zadnjem poglavlju upoznajemo se s pojmom fraktala te promatramo fraktalnu strukturu Pascalovog trokuta.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004-Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Poglavlje 1

Osnovni pojmovi i tvrdnje

Za razumijevanje i dokazivanje tvrdnji koje se pojavljuju kasnije u radu, potrebni su nam pojmovi poput djeljivosti, kongruentnosti, prostog broja, binomnog koeficijenta itd. Zato su ti i drugi relevantni pojmovi definirani u nastavku, zajedno s osnovnim propozicijama i teoremima.

1.1 Djeljivost

Definicija 1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b djeljiv s a, odnosno a dijeli b, ako postoji cijeli broj k takav da je $b = ka$. To zapisujemo sa $a \mid b$. Ako a ne dijeli b, onda pišemo $a \nmid b$.*

Ako $a \mid b$, kažemo da je a djelitelj od b, a da je b višekratnik od a.

Definicija 1.2. *Prirodan broj p veći od 1 se zove prost ako p nema niti jednog djelitelja d takvog da je $1 < d < p$. Ako prirodan broj veći od 1 nije prost, onda kažemo da je složen.*

Svaki prirodan broj n možemo prikazati u obliku

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \cdots {p_r}^{\alpha_r},$$

gdje su $p_1, \ldots, p_r$ različiti prosti brojevi, a $\alpha_1, \ldots, \alpha_r$ prirodni brojevi. Ovakav prikaz broja n naziva se *kanonski rastav* broja n na proste faktore [6].

Teorem 1.3 (**Osnovni teorem aritmetike**)**.** *Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.*

Dokaz. Dokaz se može naći u [6] na stranici 7. □

Teorem 1.4 (**Teorem o dijeljenju s ostatkom**). *Za proizvoljan prirodni broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r, $0 \leqslant r < a$, takvi da je*

$$b = q \cdot a + r.$$

Dokaz. Promotrimo skup $\{b - am : m \in \mathbb{Z}\}$. Najmanji nenegativni član ovog skupa označimo sa r. Tada je po definiciji $0 \leqslant r < a$ i postoji $q \in \mathbb{Z}$ takav da je $b - qa = r$, tj. $b = qa + r$.

Dokažimo sada jedinstvenost od q i r. Pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete. Pokažimo najprije da je $r_1 = r$. Pretpostavimo da je npr. $r < r_1$. Tada je $0 \leqslant r_1 - r < a$, dok je s druge strane $r_1 - r = b - q_1 a - (b - qa) = a(q - q_1) \geqslant a$. Prema tome je $r_1 = r$, pa je stoga i $q_1 = q$. Dokaz je preuzet iz [6]. □

Svaki prirodan broj možemo prikazati u zadanoj bazi primjenom Teorema o dijeljenju s ostatkom.

Teorem 1.5 (**Prikaz broja u bazi**). *Neka je $b \geqslant 2$ zadani prirodan broj. Za svaki prirodan broj n postoji jedinstven niz znamenaka $(x_k, \ldots, x_1, x_0)$, $x_i \in \{0, 1, \ldots, b-1\}$, $x_k \neq 0$, takav da je*

$$n = x_k \cdot b^k + x_{k-1} \cdot b^{k-1} + \cdots + x_1 \cdot b + x_0.$$

Ovaj zapis nazivamo prikaz broja n u bazi b.

Dokaz. Dokaz se može naći u [15] na stranici 8. □

Definicija 1.6. *Neka su a i b cijeli brojevi. Ako cijeli broj $m \neq 0$ 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 i pišemo $a \not\equiv b \pmod{m}$.*

Još kažemo, a i b su kongruentni modulo m ako daju isti ostatak pri dijeljenju s m. Pojam kongruencije je uveo C. F. Gauss u svom djelu *Disquisitiones Arithmeticae* iz 1801. godine.

Propozicija 1.7. *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu cijelih brojeva.*

Dokaz. Potrebno je dokazati da je dana relacija refleksivna, simetrična i tranzitivna.

(1) Iz $m \mid 0$ slijedi $m \mid (a - a)$, pa vrijedi tvrdnja $a \equiv a \pmod{m}$.

(2) Ako je $a \equiv b \pmod{m}$, onda postoji cijeli broj k takav da je $a - b = mk$. Množenjem jednakosti s -1 dobivamo $b - a = m \cdot (-k)$, pa je $b \equiv a \pmod{m}$.

(3) Iz $a \equiv b \pmod{m}$ i $b \equiv c \pmod{m}$ slijedi da postoje cijeli brojevi k i l takvi da je $a - b = mk$ i $c - b = ml$. Zbrajanjem tih dviju jednakosti dobivamo $a - c = m(k + l)$, što povlači $a \equiv c \pmod{m}$.

□

Uvođenjem relacije kongruencije na skupu cijelih brojeva, definira se modularna aritmetika. Ona se bavi ostatcima dijeljenja cijelih brojeva s fiksiranim cijelim brojem m. Tako možemo govoriti o aritmetici na nekom potpunom sustavu ostataka modulo m, primjerice $\{0, \ldots, m - 1\}$.

1.2 Binomni koeficijenti

Definicija 1.8. *Za nenegativne cijele brojeve n i k, binomni koeficijent* $\binom{n}{k}$ *je broj k-članih podskupova n-članog skupa.*

Broj $\binom{n}{k}$ zove se binomni koeficijent jer se javlja u razvoju n-te potencije binoma $a + b$ što se može vidjeti u teoremu koji slijedi.

Teorem 1.9 (**Binomni teorem**). *Za proizvoljan prirodan broj n i realne brojeve a i b vrijedi*

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k}\, b^k.$$

Dokaz. Dokaz se može pronaći u [20] na stranicama 78 – 79. □

Definicija 1.10. *Umnožak prvih n prirodnih brojeva označavamo s* $n!$*, tj.* $n! = 1 \cdot 2 \cdots n$*. Taj broj nazivamo n faktorijela. Dodatno definiramo* $0! = 1$.

Iz definicije 1.8 odmah slijedi da je svaki binomni koeficijent cijeli broj, a pomoću iduće propozicije možemo ga lako izračunati.

Propozicija 1.11. *Neka su n i k nenegativni cijeli brojevi. Tada za* $0 \leqslant k \leqslant n$ *vrijedi*

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

Dokaz. Prvi element k-članog podskupa n-članog skupa možemo izabrati na n načina. Drugi element biramo na $(n - 1)$ načina. Analogno nastavljamo sve do k-tog elementa kojeg možemo izabrati na $(n - k + 1)$ načina. Koristeći princip produkta, broj mogućih izbora je $n(n - 1) \cdots (n - k + 1)$, no poredak nam nije važan pa dobiveni broj dijelimo s $k!$. □

Propozicija 1.12 (Pascalov identitet)**.** *Neka su n i k prirodni brojevi. Tada vrijedi identitet*

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

Ovaj identitet će se često pojavljivati u radu, pa ćemo ga dokazati na dva različita načina.

Algebarski dokaz Pascalovog identiteta. Vrijedi

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

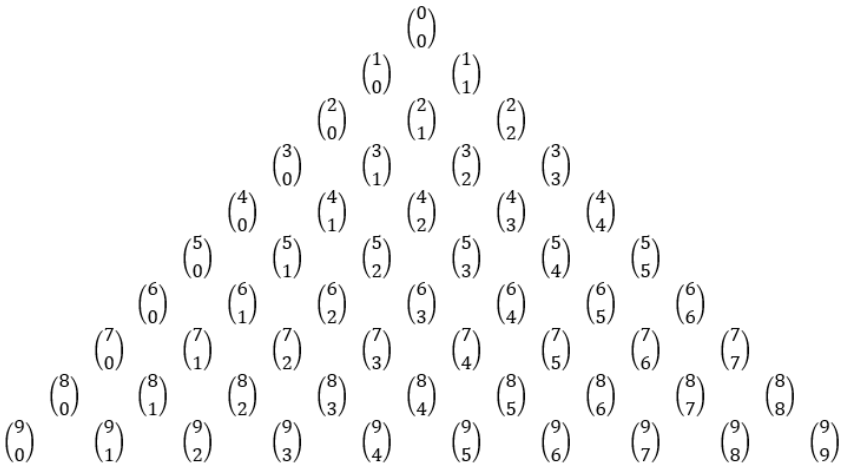
što smo i htjeli dokazati. □

Kombinatorni dokaz Pascalovog identiteta. Lijeva strana jednakosti označava broj k-članih podskupova nekog n-članog skupa. Izdvojimo jedan element a iz tog n-članog skupa. Postoji $\binom{n-1}{k}$ k-članih podskupova kojima a nije element i $\binom{n-1}{k-1}$ k-članih podskupova koji sadrže element a. Prema principu zbroja to je ukupno $\binom{n-1}{k} + \binom{n-1}{k-1}$ različitih k-članih podskupova n-članog skupa. Time smo dokazali dani identitet. □

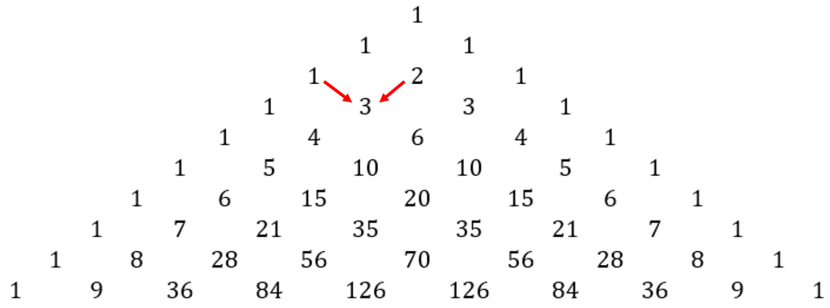
1.3 Pascalov trokut

Slaganjem binomnih koeficijenata $\binom{n}{k}$ u redove uzastopnih vrijednosti gdje na k-tom mjestu u n-tom redu stoji $\binom{n}{k}$, pri čemu numeriramo počevši od 0, dobivamo strukturu trokutastog oblika koju nazivamo Pascalovim trokutom (Slika 1.1). Primjenom Pascalovog identiteta (Propozicija 1.12), brojeve svakog reda konstruiramo iz brojeva prethodnog reda, i to na sljedeći način. U nultom redu nalazi se jedna jedinica, a u prvom redu ispod nje dvije jedinice. Svaki broj u sljedećem redu dobivamo kao zbroj broja gore lijevo i broja gore desno (Slika 1.2).

Korištenjem matematičke indukcije iz navedene konstrukcije Pascalovog trokuta primjenom Pascalovog identiteta možemo dobiti još jedan dokaz da su binomni koeficijenti cijeli brojevi jer je svaki novi red sastavljen od prirodnih brojeva.

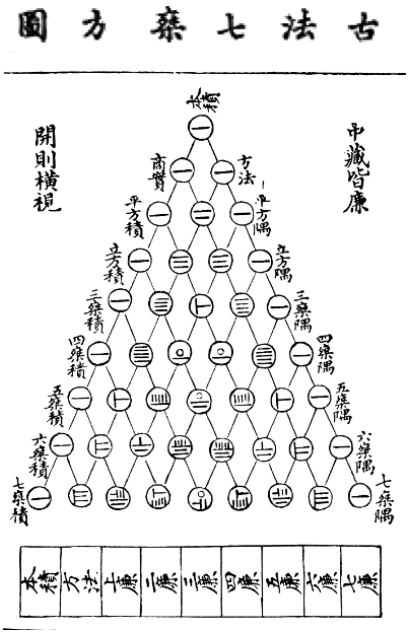


Slika 1.1: Prvih deset redova Pascalovog trokuta sastavljenog od binomnih koeficijenata



Slika 1.2: Prvih deset redova Pascalovog trokuta

Pascalov trokut dobio je ime po francuskom matematičaru, fizičaru i filozofu Blaiseu Pascalu (1623.-1662.). Iako se njegov eksplicitni prikaz javlja u staroj Kini (10.-13. st.), Pascal je prvi koji ga je proučio, objasnio njegovu upotrebu i objedinio rezultate u svom djelu *Traité du triangle arithmétique* (1653.) (vidi u [2, 16]). Kineski matematičar Jia Xian je u 11. st. koristio trokut za izračunavanje drugog i trećeg korijena. Najsličniji Pascalovom trokutu je aritmetički trokut sa šest redova kineskog matematičara Yanga Huia iz 13. st. Iz tog razloga u Kini Pascalov trokut nazivaju "Yang Hui-ev trokut". Godine 1303. matematičar Zhu Shijie u svojem djelu *Siyuan yujian* proširuje trokut na 8 redova (Slika 1.3) [12].



Slika 1.3: Yang Hui-ev trokut

Promatranjem Pascalovog trokuta, možemo uočiti da se na početku i na kraju svakog reda nalaze jedinice. To je zato što se na tim mjestima nalaze binomni koeficijenti $\binom{n}{0} = \binom{n}{1} = 1$, gdje je n broj reda. Štoviše, primijenimo li modularnu aritmetiku na Pascalov trokut, tj. brojeve u trokutu zamijenimo brojevima koji su im kongruentni modulo m, također će na početku i na kraju svakog reda biti jedinice jer je $1 \equiv 1 \pmod{m}$, za svaki prirodan broj m.

Pascalov trokut je simetričan s obzirom na okomitu os što prolazi "vrhom trokuta" jer za sve $n \geqslant m$ vrijedi

$$\binom{n}{n-m} = \frac{n!}{(n-m)!\, m!} = \binom{n}{m}.$$

Ova tvrdnja slijedi i iz činjenice da su m-člani podskupovi n-članog skupa u bijekciji s $(n-m)$-članim podskupovima istog skupa. Naime, svakom podskupu pridružimo njegov komplement.

Poglavlje 2

Teoremi Lucasa, Legendrea i Kummera

Problemi vezani uz primjenu modularne aritmetike na binomne koeficijente imaju bogatu povijest. Mnoge matematičare 19. stoljeća osobito su interesirali ostatci pri dijeljenju binomnih koeficijenata s potencijama prostih brojeva. Matematičari poput A. L. Cauchyja, A. Cayleyja, C. F. Gaussa, E. Kummera, A. M. Legendrea i E. Lucasa otkrili su razne zanimljive teoreme od kojih ćemo neke iskazati i dokazati, ali i primjenjivati kasnije u radu.

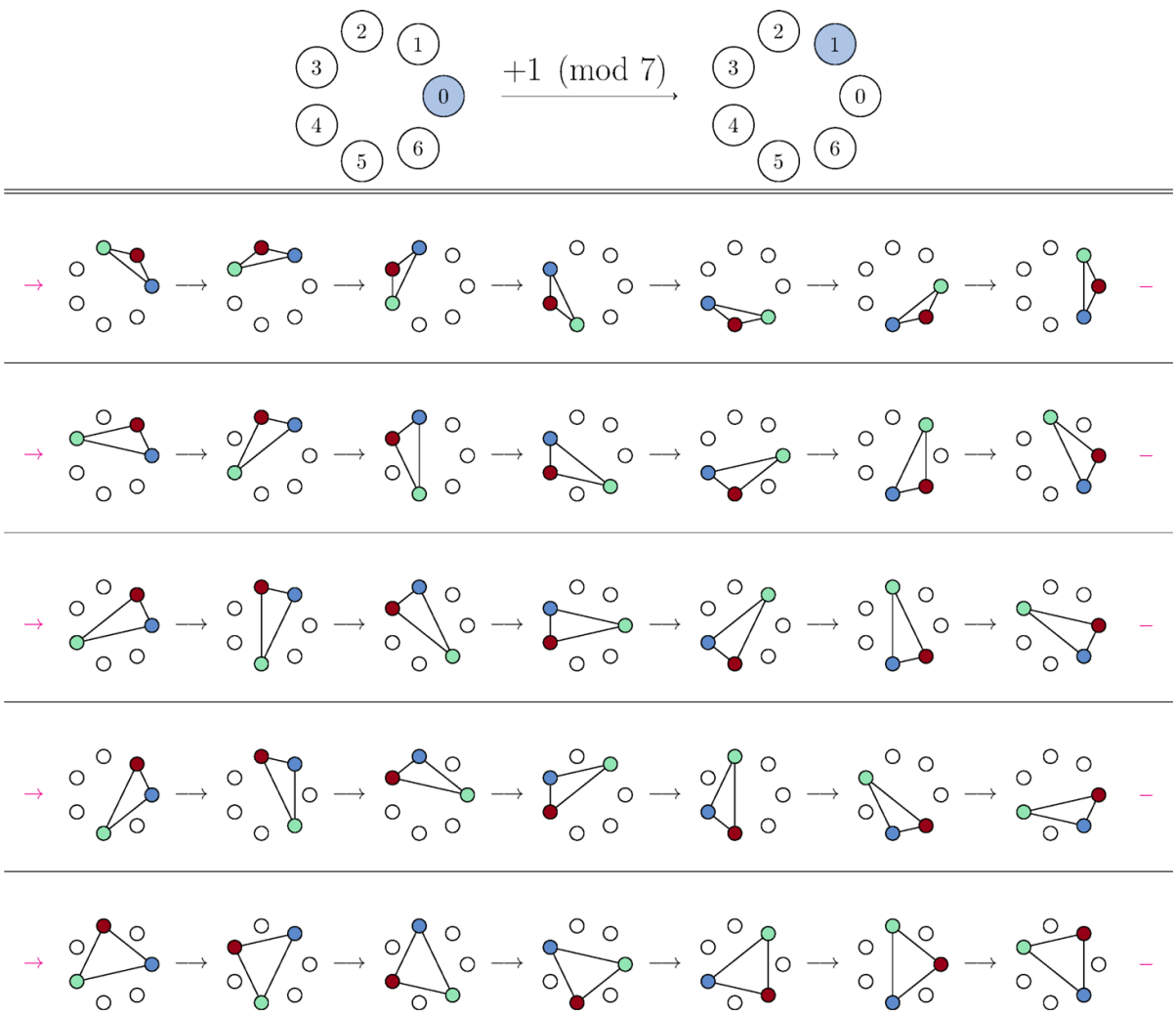
Propozicija 2.1. *Neka je p prost broj. Tada za svaki $k \in \{1, 2, \ldots, p-1\}$ vrijedi*

$$\binom{p}{k} \equiv 0 \pmod{p}.$$

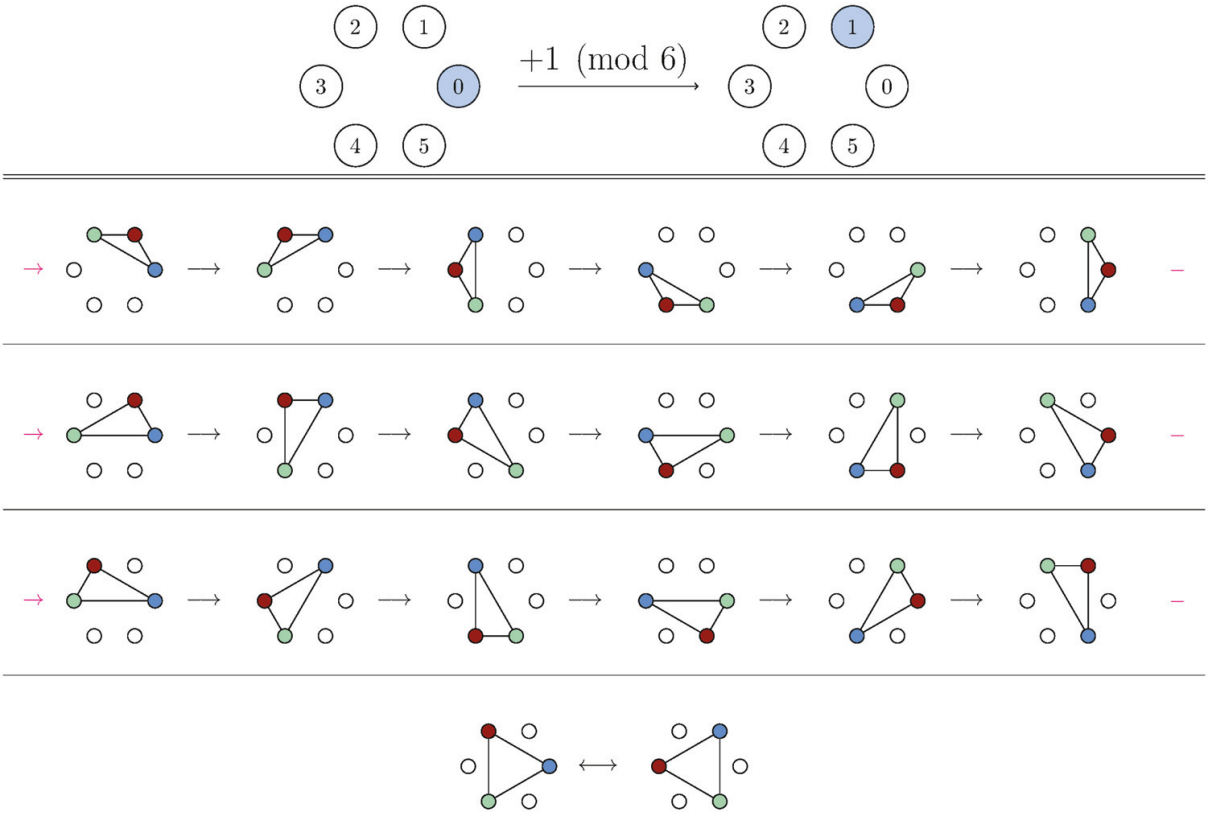
Dokaz I. Prema Propoziciji 1.11 je $\binom{p}{k} = \frac{p!}{k!(p-k)!}$. Budući da je p prost broj i $k \in \{1, 2, \ldots, p-1\}$, a prema tome i $(p-k) \in \{1, 2, \ldots, p-1\}$, nazivnik $k!(p-k)!$ nije djeljiv s p. S druge strane, brojnik $p!$ je djeljiv s p, pa je prema tome i $\binom{p}{k}$ djeljiv s p. Time smo dokazali tvrdnju propozicije. □

Dokaz II. Ova propozicija se može i vizualno dokazati. Promotrimo slučaj kad je $p = 7$ i $k = 3$ (Slika 2.1). Familiju svih tročlanih podskupova skupa $\{0, 1, \ldots, 6\}$ particionirali smo koristeći zbrajanje modulo 7 u 7-člane familije, pa očito $7 \mid \binom{7}{3}$. Ideja ovog dijagrama se može generalizirati za sve proste brojeve p i sve $k \in \{1, 2, \ldots, p-1\}$.

Analogno možemo prikazati da binomni koeficijent $\binom{n}{k}$ ne mora biti nula modulo n kad n i k nisu relativno prosti. Na Slici 2.2 je prikazan slučaj $n = 6$ i $k = 3$.



Slika 2.1: Binomni koeficijent $\binom{7}{3}$ je kongruentan 0 modulo 7.



Slika 2.2: Binomni koeficijent $\binom{6}{3}$ nije kongruentan 0 modulo 6.

Dokaz je preuzet iz članka [7]. □

Propozicija 2.2. *Za svaki realni broj x, nenegativni cijeli broj s i prost broj p vrijedi*

$$(1+x)^{p^s} \equiv 1 + x^{p^s} \pmod{p}.$$

Dokaz. Raspišimo $(1+x)^{p^s}$ koristeći binomni teorem.

$$(1+x)^{p^s} = 1 + \binom{p^s}{1}x + \cdots + \binom{p^s}{p^s-1}x^{p^s-1} + x^{p^s}$$

Pokažimo tvrdnju propozicije koristeći matematičku indukciju.

Baza: za $s = 1$ imamo $(1+x)^p \equiv 1 + x^p \pmod{p}$ jer su zbog prethodne propozicije svi pribrojnici osim prvog i zadnjeg djeljivi s p.

Pretpostavimo da tvrdnja vrijedi za neki prirodan broj s.

Korak:

$$(1+x)^{p^{s+1}} = ((1+x)^p)^{p^s} \overset{\text{baza}}{\equiv} (1+x^p)^{p^s} \overset{\text{pretp.}}{\equiv} 1 + (x^p)^{p^s} = 1 + x^{p^{s+1}} \pmod{p}.$$

Iz pretpostavke indukcije dobivamo da tvrdnja vrijedi za $s+1$, pa je po principu matematičke indukcije tvrdnja istinita za svaki prirodan broj s. □

Zbog Propozicije 2.1 vrijedi $(a+b)^p \equiv a^p + b^p \pmod{p}$. U tom slučaju se eksponenti zaista distribuiraju obzirom na zbrajanje. Mnogi bi učenici voljeli da to vrijedi kao općenita formula $(a+b)^n = a^n + b^n$, no znamo da to nije istina za $n \geqslant 2$.

Za cijeli broj n i prosti broj p označimo sa $v_p(n)$ najveći cijeli broj k za koji $p^k \mid n$. Tako je primjerice, $v_2(40) = 3$ i $v_3(40) = 0$. Idući teoremi i njihovi dokazi su preuzeti iz [10].

Teorem 2.3 (**Kummerov teorem**). *Neka su m, n prirodni brojevi i p prost broj. Tada je $v_p(\binom{m+n}{n})$ broj prijenosa koji se dobije zbrajanjem m i n u bazi p.*

Dokazat ćemo teorem koristeći Legendreovu formulu.

Teorem 2.4 (**Legendreova formula**). *Neka je n prirodni broj i p prost broj. Neka je $s_p(n)$ zbroj svih znamenaka u zapisu broja n u bazi p. Tada je*

$$v_p(n!) = \frac{n - s_p(n)}{p-1}.$$

Dokaz. Neka je $n = a_k p^k + a_{k-1}p^{k-1} + \cdots + a_0$ zapis broja n u bazi p. Stoga je ovdje $s_p(n) = a_k + a_{k-1} + \cdots + a_0$. Među brojevima $1, \ldots, n$ ima $\left\lfloor \frac{n}{p} \right\rfloor$ njih koji su djeljivi s p, ima ih $\left\lfloor \frac{n}{p^2} \right\rfloor$ djeljivih s p^2, $\left\lfloor \frac{n}{p^3} \right\rfloor$ djeljivih s p^3 itd. Zato je eksponent najveće potencije od p koja dijeli $n!$ jednak

$$\begin{aligned}
v_p(n!) &= \left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots \\
&= (a_k p^{k-1} + a_{k-1}p^{k-2} + \cdots + a_1) + (a_k p^{k-2} + a_{k-1}p^{k-3} + \cdots + a_2) + \cdots + (a_k p + a_{k-1}) + a_k \\
&= a_k(p^{k-1} + p^{k-2} + \cdots + 1) + a_{k-1}(p^{k-2} + \cdots + 1) + \cdots + a_1 \\
&= a_k \frac{p^k - 1}{p-1} + a_{k-1}\frac{p^{k-1}-1}{p-1} + \cdots + a_1 \\
&= \frac{a_k(p^k - 1) + a_{k-1}(p^{k-1} - 1) + \cdots + a_1(p-1)}{p-1} \\
&= \frac{a_k p^k + a_{k-1}p^{k-1} + \cdots + a_1 p + a_0 - (a_k + a_{k-1} + \cdots + a_0)}{p-1} \\
&= \frac{n - (a_k + a_{k-1} + \cdots + a_0)}{p-1} \\
&= \frac{n - s_p(n)}{p-1}.
\end{aligned}$$

□

Dokaz Kummerovog teorema. Zapišimo prvo brojeve $m+n, m$ i n u bazi p.

$$\begin{aligned} m+n &= a_r p^r + a_{r-1}p^{r-1} + \cdots a_1 p + a_0, \\ m &= b_r p^r + b_{r-1}p^{r-1} + \cdots b_1 p + b_0, \\ n &= c_r p^r + c_{r-1}p^{r-1} + \cdots c_1 p + c_0. \end{aligned}$$

Zapis broja u bazi p uvijek možemo nadopuniti s nulama na vodećim mjestima jer se vrijednost broja neće promijeniti. Zato možemo pretpostaviti da $m+n, m$ i n imaju r znamenaka u bazi p. Definirajmo funkciju prijenosa γ. Najprije, $\gamma_0 = 0$ ako je $b_0 + c_0 < p$, a inače $\gamma_0 = 1$. Za $1 \leqslant i < r$, definiramo

$$\gamma_i = \begin{cases} 1, & b_i + c_i + \gamma_{i-1} \geqslant p \\ 0, & b_i + c_i + \gamma_{i-1} < p. \end{cases}$$

Budući da je a_r vodeći koeficijent broja $m+n$ u bazi p, to je $\gamma_r = 0$ i $a_r = b_r + c_r + \gamma_{r-1}$. Usporedimo li znamenke brojeva $m+n, m$ i n u bazi p, vidimo da vrijedi

$$\begin{aligned} a_0 &= b_0 + c_0 - p\gamma_0, \\ a_i &= b_i + c_i + \gamma_{i-1} - p\gamma_i, \qquad \text{za sve } 1 \leqslant i \leqslant r-1. \end{aligned}$$

Koristeći Legendreovu formulu (Teorem 2.4), dobivamo

$$\begin{aligned} v_p(\binom{m+n}{n}) &= v_p((m+n)! - v_p(m!) - v_p(n!)) \\ &= \frac{m+n-s_p(m+n)}{p-1} - \frac{m-s_p(m)}{p-1} - \frac{n-s_p(n)}{p-1} \\ &= \frac{s_p(m)+s_p(n)-s_p(m+n)}{p-1} \\ &= \frac{(b_0+c_0-a_0)+(b_1+c_1-a_1)+\cdots+(b_r+c_r-a_r)}{p-1} \\ &= \frac{p\gamma_0+(p\gamma_1-\gamma_0)+\cdots+(p\gamma_{r-1}-\gamma_{r-2})-\gamma_{r-1}}{p-1} \\ &= \gamma_0+\gamma_1+\cdots+\gamma_{r-1}. \end{aligned}$$

što smo i htjeli dokazati. □

Primjer 2.1. *Koji je najveći cijeli broj v za koji vrijedi* $5^v \mid \binom{4729}{532}$*?*

Rješenje. Zadatak možemo riješiti koristeći Kummerov teorem za $n = 532$ i $m = 4729 - 532 = 4197$. Brojeve 532 i 4197 zapišemo u bazi 5:

$$4197 = 113242_{(5)},\ 532 = 4112_{(5)}.$$

$$\begin{array}{cccccccc} & & 1 & & 1 & & & \\ & 1 & 1 & 3 & 2 & 4 & 2 \\ + & & & 4 & 1 & 1 & 2 \\ \hline & 1 & 2 & 2 & 4 & 0 & 4 \end{array}$$

Prema Kummerovom teoremu, najveći cijeli broj v za koji vrijedi $5^v \mid \binom{4729}{532}$ je broj prijenosa koji dobijemo zbrajanjem brojeva 532 i 4179 u bazi 5. Dakle, $v = 2$ i najveća potencija broja 5 koja dijeli $\binom{4729}{532}$ je 5^2.

Teorem 2.5 (**Lucasov teorem**)**.** *Neka su m i n nenegativni cijeli brojevi, a p prost broj. Ako su*

$$\begin{aligned} m &= m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0 \quad i \\ n &= n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0 \end{aligned}$$

zapisi brojeva m i n u bazi p, onda je

$$\binom{m}{n} \equiv \binom{m_k}{n_k}\binom{m_{k-1}}{n_{k-1}} \cdots \binom{m_0}{n_0} \pmod{p}.$$

Primijetimo kako u ovoj notaciji tvrdnja Kummerovog teorema kaže da je $v_p(\binom{m}{n})$ jednak broju indeksa i za koje je $m_i < n_i$ [11].

Vidimo da iz Kummerovog teorema tvrdnja Lucasovog teorema odmah slijedi u slučaju kada p dijeli $\binom{m}{n}$. Naime, taj slučaj po Kummeru nastupa samo ako se pojavljuje barem jedan prijenos u zbrajanju $m - n$ i n u bazi p, tj. ako za barem jedan $i \in \{0, 1, \ldots, k\}$ vrijedi $m_i < n_i$, odnosno $\binom{m_i}{n_i} = 0$.

Dokaz. Dokaz donosimo prema [9]. Primjenom binomnog teorema (Teorem 1.9), zapisa

broja m u bazi p, te Propozicije 2.2 dobivamo

$$\begin{aligned}
\sum_{N=0}^{m} \binom{m}{N} x^N &= (1+x)^m \\
&= (1+x)^{m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0} \\
&= \prod_{i=0}^{k} (1+x)^{m_i p^i} \\
&= \prod_{i=0}^{k} \left((1+x)^{p^i}\right)^{m_i} \\
&\equiv \prod_{i=0}^{k} \left(1+x^{p^i}\right)^{m_i} \pmod{p} \\
&= \prod_{i=0}^{k} \left(\sum_{s_i=0}^{m_i} \binom{m_i}{s_i} \left(x^{p^i}\right)^{s_i} \right) \\
&= \prod_{i=0}^{k} \left(\sum_{s_i=0}^{m_i} \binom{m_i}{s_i} x^{s_i p^i} \right). \qquad (2.1)
\end{aligned}$$

Zapišimo jednakost (2.1) tako da grupiramo koeficijente uz pojedinu potenciju od x. Time dobivamo izraz

$$\sum_{N=0}^{m} \left(\sum \prod_{i=0}^{k} \binom{m_i}{s_i} \right) x^N,$$

pri čemu smo unutarnju sumu uzeli po skupovima $(s_0, s_1, \ldots, s_k)$ takvim da je $\sum_{i=0}^{k} s_i p^i = N$. Kako je $0 \leqslant s_i \leqslant m_i \leqslant p-1$, to je $\sum_{i=0}^{k} s_i p^i = N$ prikaz broja N u bazi p, a takav prikaz je prema Teoremu 1.5 jedinstven. Izjednačimo li za $n \leqslant m$ koeficijente uz x^n dobivamo tvrdnju teorema, tj.

$$\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}.$$

Za $n > m$ znamo da vrijedi $\binom{m}{n} = 0$, a za barem jedan i je $n_i > m_i$ jer bi u protivnom bilo $n \leqslant m$ te je $\prod_{i=0}^{k} \binom{m_i}{n_i} = 0$. Zato tvrdnja Lucasovog teorema vrijedi i u tom slučaju. □

Idući primjer nam pokazuje direktnu primjenu Lucasovog teorema kod računanja ostatka pri dijeljenju binomnog koeficijenta s prostim brojem.

Primjer 2.2. *Koji je ostatak pri dijeljenju broja* $\binom{3330}{508}$ *brojem* 7*?*

Rješenje. Najprije brojeve 3330 i 508 zapišemo u bazi 7

$$3330 = 12465_{(7)},\ 508 = 1324_{(7)}.$$

Primjenom Lucasovog teorema dobivamo

$$\begin{aligned}\binom{3330}{508} &\equiv \binom{1}{0}\binom{2}{1}\binom{4}{3}\binom{6}{2}\binom{5}{4}\\ &\equiv 1\cdot 2\cdot 4\cdot 15\cdot 5\\ &\equiv 5 \pmod 7.\end{aligned}$$

Dakle, ostatak pri dijeljenju $\binom{3330}{508}$ sa 7 je 5.

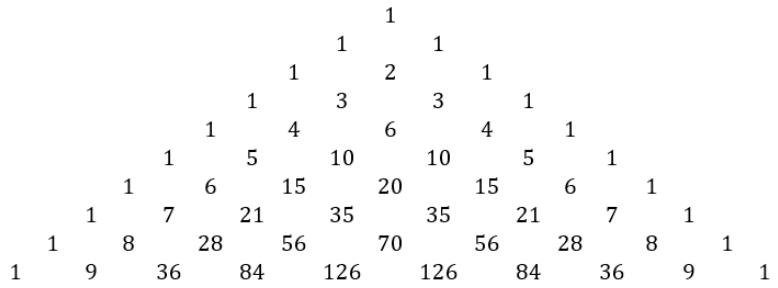
Poglavlje 3

Binomni koeficijenti modulo manji prirodni broj

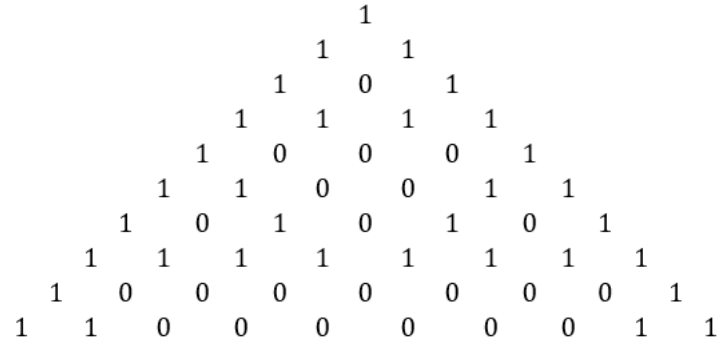
U ovom poglavlju najprije ćemo se baviti rezultatima koji su vezani uz ostatke pri dijeljenju binomnih koeficijenata s manjim prirodnim brojevima te ih interpretirati unutar Pascalovog trokuta.

3.1 Binomni koeficijenti modulo 2

Budući da se Pascalov trokut sastoji od binomnih koeficijenata, možemo promotriti što se događa kada na njega primijenimo modularnu aritmetiku, tj. svaki broj u trokutu zamijenimo brojem koji mu je kongruentan modulo m. Najprije uzimamo $m = 2$. Promotrimo prvih deset redova Pascalovog trokuta (Slika 3.1). Pascalov trokut modulo 2 sastoji se od ostataka pri dijeljenju s dva, tj. od nula i jedinica. Primjerice, na mjestu $\binom{3}{1} = 3$ će biti broj 1 jer je $3 \equiv 1 \pmod 2$. Dakle, na mjestu parnih brojeva bit će broj nula, a na mjestu neparnih broj jedan (Slika 3.2).



Slika 3.1: Prvih deset redova Pascalovog trokuta



Slika 3.2: Prvih deset redova Pascalovog trokuta modulo 2

Sa slike možemo primijetiti da su drugi, četvrti i osmi red Pascalovog trokuta modulo 2 sastavljeni od rubnih jedinica između kojih su sve nule. Iz Propozicije 4.1 koju ćemo kasnije dokazati slijedi idući korolar kao poseban slučaj prema kojemu su svi redovi kojima je redni broj potencija broja dva oblika $100\ldots001$.

Korolar 3.1. *Svaki od brojeva*

$$\binom{2^n}{1}, \binom{2^n}{2}, \ldots, \binom{2^n}{2^n-1}$$

je paran.

S druge strane, n-ti redak Pascalovog trokuta modulo 2, za n oblika $2^m - 1$ sastoji se samo od jedinica i to su svi takvi retci. To je posljedica iduće propozicije.

Propozicija 3.2. *Sljedeće tvrdnje su ekvivalentne.*

(1) *Svi brojevi oblika* $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n-1}, \binom{n}{n}$ *su neparni.*

(2) *Broj* $n+1$ *je potencija broja dva.*

Za provedbu dokaza koristit ćemo Lucasov teorem pomoću kojega se lako može ustanoviti vrijednost binomnog koeficijenta modulo prost broj. Dokaz je preuzet iz [17].

Dokaz. Neka je $n = a_r 2^r + a_{r-1}2^{r-1} + \cdots + a_1 2^1 + a_0$ prikaz broja n u bazi 2, gdje je $r \geqslant 0, a_r \neq 0$. Budući da je $a_r \neq 0$, nužno je $a_r = 1$. Neka je $k \in \{0, 1, \ldots, n\}$. Kako je $k \leqslant n$, možemo k prikazati u bazi 2 u obliku $k = b_r 2^r + b_{r-1}2^{r-1} + ... + b_1 2^1 + b_0$, gdje su $b_0, b_1, ..., b_r \in \{0, 1\}$. Iz Lucasovog teorema slijedi

$$\binom{n}{k} \equiv \binom{a_r}{b_r}\binom{a_{r-1}}{b_{r-1}} \cdots \binom{a_1}{b_1}\binom{a_0}{b_0} \pmod 2.$$

(2) ⇒ (1). Broj $n+1$ je potencija broja dva, pa možemo pisati $n = 2^s - 1$, tj. $n = 1\cdot 2^{s-1} + 1\cdot 2^{s-2} + \cdots + 1\cdot 2^1 + 1$. U ovom slučaju je $r = s-1$ i $a_r = a_{r-1} = \ldots = a_1 = a_0 = 1$. Dakle, svi faktori $\binom{a_i}{b_i}$ jednaki su ili $\binom{1}{0}$ ili $\binom{1}{1}$, pa u svakom slučaju iznose 1. Dobivamo da je $\binom{n}{k} \equiv 1 \pmod 2$ za sve $k \in \{0, 1, \ldots, n\}$, tj. $\binom{n}{k}$ je neparan za sve $k \in \{0, 1, \ldots, n\}$.

(1) ⇒ (2). Pretpostavimo sada da su svi brojevi $\binom{n}{0}$, $\binom{n}{1}$, ..., $\binom{n}{n-1}$, $\binom{n}{n}$ neparni. To znači da za svaki od njih vrijedi $\binom{a_i}{b_i} = 1$ za sve $i = 0, 1, ..., r$. Dakle, $b_i \leqslant a_i$ za $i = 0, 1, ..., r$. Kad bi neki od a_i bio jednak 0, tada bi za $b_i = 1$ imali $\binom{a_i}{b_i} = 0$, što daje

$$\binom{n}{2^i} \equiv 0 \pmod 2.$$

Zaključujemo da je $a_i = 1$ za sve $i \in \{0, 1, \ldots, r\}$. Otuda slijedi $n = 2^r + 2^{r-1} + \cdots + 2^1 + 2^0 = 2^{r+1} - 1$. □

Podsjetimo se da je $v_2(n)$ definiran kao broj k takav da $2^k \mid n$ i $2^{k+1} \nmid n$. Sa $s_2(n)$ označavamo zbroj znamenki u binarnom prikazu prirodnog broja n. Naravno, to je zapravo broj jedinica u binarnom zapisu broja n.

Propozicija 3.3. *Neka su a, b nenegativni cijeli brojevi. Sljedeće tvrdnje su ekvivalentne.*

(a) $\binom{a+b}{a}$ *je neparan broj,*

(b) $v_2((a+b)!) = v_2(a!) + v_2(b!)$,

(c) $s_2(a+b) = s_2(a) + s_2(b)$.

Dokaz. $(a) \Rightarrow (b)$ Pretpostavimo da je $\binom{a+b}{a}$ neparan broj za $a, b \geqslant 0$. To znači da je $v_2(\binom{a+b}{a}) = 0$, odnosno

$$v_2((a+b)!) - v_2(a!) - v_2(b!) = 0$$

iz čega slijedi tvrdnja pod (b).

$(b) \Rightarrow (c)$ Pretpostavimo da vrijedi $v_2((a+b)!) = v_2(a!) + v_2(b!)$ za $a, b \geqslant 0$. Koristeći Legendreovu formulu dobivamo

$$(a+b) - s_2(a+b) = a - s_2(a) + b - s_2(b)$$

iz čega slijedi tvrdnja pod (c).

$(c) \Rightarrow (a)$ Pretpostavimo da je $s_2(a+b) = s_2(a) + s_2(b)$. Pomoću Legendreove formule dobivamo

$$\begin{aligned} v_2(\binom{a+b}{a}) &= v_2((a+b)! - v_2(a!) - v_2(b!) \\ &= (a+b-s_2(a+b)) - (a-s_2(a)) - (b-s_2(b)) \\ &= s_2(a) + s_2(b) - s_2(a+b) \\ &= 0, \end{aligned}$$

pa je $\binom{a+b}{a}$ neparan. □

Možemo se pitati koliko ima neparnih brojeva u n-tom retku Pascalovog trokuta za proizvoljni n. Ekvivalentno pitanje je koliko ima jedinica u n-tom retku Pascalovog trokuta modulo 2. O tome nam govori rezultat engleskog matematičara J. W. L. Glaishera iz 1899. godine. Prema Glaisheru, broj neparnih brojeva u n-tom retku je određena potencija broja dva.

Teorem 3.4 (Glaisher)**.** *Za svaki prirodan broj n, u nizu*

$$\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n-1}, \binom{n}{n}$$

ima točno $2^{s_2(n)}$ *neparnih brojeva.*

Dokaz I. Slijedi iz Teorema 4.5 za $p = 2$. □

Dokaz II. Označimo broj neparnih brojeva u danom nizu sa w_n. Neka je $n = 2^s + m$, gdje je s nenegativni cijeli broj i $0 \leqslant m < 2^s$. Za $0 \leqslant k < 2^s$ primjenjujući Lucasov teorem, dobivamo

$$\binom{2^s+m}{k} \equiv \binom{1}{0}\binom{m}{k} \equiv \binom{m}{k} \pmod 2. \tag{3.1}$$

Međutim, za $2^s \leqslant k \leqslant n$ imamo $k - 2^s \leqslant n - 2^s = m < 2^s$, pa koristeći Lucasov teorem slijedi

$$\binom{2^s+m}{k} = \binom{2^s+m}{2^s+k-2^s} \equiv \binom{1}{1}\binom{m}{k-2^s} \equiv \binom{m}{k-2^s} \pmod 2. \tag{3.2}$$

Stoga je $w_n = 2w_m$. Ponavljajući postupak za broj m, dobivamo $w_m = 2w_{m_1}$ za neki m_1. Nastavimo dalje i konačno dobivamo da je $w_n = 2^s w_0$, gdje je $s = s_2(n)$. Očito je $w_0 = 1$. Dakle, $w_n = 2^{s_2(n)}$.

Tvrdnju (3.1) mogli smo dokazati i bez primjene Lucasovog teorema. Za $0 \leqslant k < 2^s$ imamo

$$\binom{2^s+m}{k} = \frac{(2^s+m)(2^s+m-1)\cdots(2^s+m-k+1)}{k!},$$
$$\binom{m}{k} = \frac{m(m-1)\cdots(m-k+1)}{k!}.$$

Za $i \in \{0,1,\ldots,k-1\}$ vrijedi $v_2(2^s+m-i) = v_2(m-i)$ jer je $|m-i| < 2^s$, pa je $v_2(m-i) < s$. Također znamo da je $v_p(a+b) = v_p(a)$ ako je $v_p(a) < v_p(b)$. Zato je

$$v_2(\binom{2^s+m}{k}) = v_2(\binom{m}{k}),$$

što povlači $\binom{2^s+m}{k} \equiv \binom{m}{k} \pmod 2$.

Slično dobivamo tvrdnju (3.2). Za $k \geqslant 2^s$ primjenom svojstva simetričnosti binomnog koeficijenta imamo

$$\binom{2^s+m}{k} = \binom{2^s+m}{2^s+m-k}.$$

Iz $m < 2^s \leqslant k$ slijedi $2^s+m-k < 2^s$, pa smo u prvom slučaju i vrijedi

$$\binom{2^s+m}{2^s+m-k} \equiv \binom{m}{2^s+m-k} = \binom{m}{k-2^s} \pmod 2.$$

Dokaz je preuzet iz [17]. □

Idući teorem nam daje postupak za određivanje parnosti binomnih koeficijenata.

Teorem 3.5. *Broj $\binom{n}{k}$ je neparan ako i samo ako u binarnom zapisu nijedna znamenka od k nije veća od odgovarajuće znamenke od n.*

Dokaz. Neka su zapisi od n i k u bazi 2

$$n = n_m \cdot 2^m + n_{m-1} \cdot 2^{m-1} + \cdots + n_1 \cdot 2 + n_0,$$
$$k = k_m \cdot 2^m + k_{m-1} \cdot 2^{m-1} + \cdots + k_1 \cdot 2 + k_0.$$

Pretpostavimo da je $\binom{n}{k}$ neparan. Kad bi barem jedna znamenka k_i bila veća od odgovarajuće znamenke n_i, za $0 \leqslant i \leqslant m$, slijedilo bi

$$\binom{n_i}{k_i} \equiv 0 \pmod 2. \tag{3.3}$$

Tada bismo iz (3.3) i Lucasovog teorema 2.5 imali

$$\binom{n}{k} \equiv \prod_{j=0}^{m} \binom{n_j}{k_j} \equiv 0 \pmod 2.$$

To je u kontradikciji s pretpostavkom da je $\binom{n}{k}$ neparan. Dakle, svaka znamenka od k mora biti manja ili jednaka odgovarajućoj znamenci od n.

Pretpostavimo sada da je broj $\binom{n}{k}$ takav da u binarnom zapisu nijedna znamenka od k nije veća od odgovarajuće znamenke od n. Svi koeficijenti n_i, k_i, za $0 \leqslant i \leqslant m$, u binarnom zapisu su iz skupa $\{0, 1\}$. Postoje dva slučaja.

1° Ako je $n_i = 0$ za neki $0 \leqslant i \leqslant m$, prema pretpostavci k_i može biti jedino jednak nuli. Slijedi $\binom{n_i}{k_i} = \binom{0}{0} = 1$.

2° Ako je $n_i = 1$ za neki $0 \leqslant i \leqslant m$, prema pretpostavci k_i je iz skupa $\{0, 1\}$. Slijedi, $\binom{n_i}{k_i} = \binom{1}{0} = \binom{1}{1} = 1$.

U oba slučaja će prema Lucasovom teoremu vrijediti

$$\binom{n}{k} \equiv \prod_{j=0}^{m} \binom{n_j}{k_j} \equiv 1 \pmod 2.$$

Dakle, broj $\binom{n}{k}$ je neparan. □

Primjer 3.1. *(a) Broj* $\binom{27}{9}$ *je neparan jer u binarnom zapisu nijedna znamenka broja* 9 *nije veća od odgovarajuće znamenke broja* 27. *To lako vidimo napišemo li brojeve jedan ispod drugog.*

$$27 = 11011_{(2)},\ 9 = 1001_{(2)}$$

$$\begin{array}{ccccc} 1 & 1 & 0 & 1 & 1 \\ & 1 & 0 & 0 & 1 \end{array}$$

(b) Broj $\binom{19}{11}$ *je paran jer je u binarnom zapisu znamenka uz* 2^3 *broja* 11 *veća od odgovarajuće znamenke broja* 19.

$$19 = 10011_{(2)},\ 11 = 1011_{(2)}$$

$$\begin{array}{ccccc} 1 & 0 & 0 & 1 & 1 \\ & 1 & 0 & 1 & 1 \end{array}$$

Posljedica iduće propozicije je da ni u jednom parnom redu Pascalovog trokuta modulo 2 nema bloka 11, tj. nema dviju uzastopnih jedinica.

Propozicija 3.6. *Ako je k neparan broj, onda je $\binom{2n}{k}$ paran broj.*

Dokaz. Tvrdnja slijedi iz Teorema 3.5 budući da je u binarnom zapisu zadnja znamenka od $2n$ jednaka 0, a od k je 1. □

Propozicija 3.7. *Ako za prirodan broj n vrijedi da je broj $\binom{2n-1}{n}$ neparan, onda je $n = 2^s$ za neki $s \in \mathbb{N}_0$.*

Dokaz. Lako se provjeri da je $s_2(2n-1) = s_2(n-1) + 1$. Prema Propoziciji 3.3 je $\binom{2n-1}{n}$ neparan broj ako i samo ako je $s_2(2n-1) = s_2(n) + s_2(n-1)$, tj. ako i samo ako je $s_2(n) = 1$, a to upravo znači da je $n = 2^s$ za neki $s \in \mathbb{N}_0$. □

Označimo sa $a(n)$ i $b(n)$ broj nula, odnosno broj jedinica u n-tom retku Pascalovog trokuta modulo 2. Znamo već da je $b(n) = 2^{s_2(n)}$, gdje je $s_2(n)$ broj jedinica u binarnom prikazu broja n (Teorem 3.4), pa je $a(n) = n + 1 - b(n) = n + 1 - 2^{s_2(n)}$.

Propozicija 3.8. (1) *Za svaki n su brojevi $a(n)$ i $b(n)$ različiti. Drugim riječima, u Pascalovom trokutu modulo 2 nema retka u kojem je broj jedinica jednak broju nula.*

(2) $a(n) = b(n) + 1 \iff n = 4$.

(3) $a(n) = b(n) - 1 \iff n = 2^k - 2$, *gdje je k prirodni broj.*

Dokaz. (1) Za $a(n) = b(n)$ je

$$a(n) = b(n) = \frac{n+1}{2} = 2^{s_2(n)} \Rightarrow n = 2^{s_2(n)+1} - 1. \tag{3.4}$$

Binarni zapis broja $n = 2^k - 1$ sastoji se od k jedinica. Zato je $s_2(2^k - 1) = k$ za svaki nenegativni cijeli broj k. Iz ove činjenice te (3.4) slijedi

$$s_2(n) = s_2(2^{s_2(n)+1} - 1) = s_2(n) + 1,$$

čime je dobivena kontradikcija.

(2) Za $a(n) = b(n) + 1$ je

$$b(n) = \frac{n}{2} = 2^{s_2(n)} \iff n = 2^{s_2(n)+1}. \tag{3.5}$$

Binarni zapis broja $n = 2^k$ je oblika $10\ldots0$, gdje je točno k nula. Zato je $s_2(2^k) = 1$ za svaki nenegativni cijeli broj k. Iz toga te iz (3.5) slijedi

$$s_2(n) = s_2(2^{s_2(n)+1}) = 1 \Rightarrow n = 2^{1+1} = 4.$$

(3) Za $a(n) = b(n) - 1$ je

$$\begin{aligned} a(n) = \frac{n}{2} &= n + 1 - 2^{s_2(n)} \\ n &= 2n + 2 - 2^{s_2(n)+1} \\ n &= 2^{s_2(n)+1} - 2, \end{aligned}$$

odnosno, n je oblika $2^k - 2$ za prirodan broj k. □

Neka je $c(n)$ ukupan broj jedinica do n-tog retka Pascalovog trokuta modulo 2, tj.

$$c(n) = \sum_{i=0}^{n} b(i).$$

Propozicija 3.9. *Za prirodni broj s vrijedi*

$$c(2^s - 1) = 3^s.$$

Dokaz. Binomni koeficijenti koji doprinose zbroju $c(2^s - 1)$ su oblika $\binom{n}{k}$, gdje je

$$\begin{aligned} n &= a_s 2^{s-1} + a_{s-1} 2^{s-2} + \ldots + a_1 2^1 + a_0 \\ k &= b_s 2^{s-1} + b_{s-1} 2^{s-2} + \ldots + b_1 2^1 + b_0. \end{aligned}$$

Prema Teoremu 3.5 mogući parovi koeficijenata su $(a_i, b_i) \in \{(0,0), (1,0), (1,1)\}$. Takvih parova (n, k) prema principu produkta ima $\underbrace{3 \cdot 3 \cdots 3}_{s \text{ puta}} = 3^s$. □

Iznad n-tog retka Pascalovog trokuta ima $1 + 2 + \cdots + n = \binom{n+1}{2}$ elemenata.

Propozicija 3.10.

$$\lim_{n\to\infty} \frac{c(n)}{\binom{n+1}{2}} = \lim_{n\to\infty} \frac{c(n)}{n^2} = 0.$$

Dokaz. Za prirodan broj n neka je s prirodan broj takav da je $2^s - 1 \leqslant n < 2^{s+1} - 1$. Tada je

$$c(2^s - 1) \leqslant c(n) \leqslant c(2^{s+1} - 1),$$

odnosno, zbog prethodne propozicije $3^s \leqslant c(n) \leqslant 3^{s+1}$. Dalje slijedi

$$\frac{3^s}{(2^{s+1} - 1)^2} \leqslant \frac{c(n)}{n^2} \leqslant \frac{3^{s+1}}{(2^s - 1)^2}$$

Kad $n \to \infty$, onda i $s \to \infty$ te vrijedi $\lim_{s\to\infty} \frac{3^s}{(2^{s+1}-1)^2} = \lim_{s\to\infty} \frac{3^{s+1}}{(2^s-1)^2} = 0$. Iz teorema o sendviču dobivamo

$$\lim_{n\to\infty} \frac{c(n)}{n^2} = 0.$$

Pomnožimo sa $\lim_{n\to\infty} \frac{n^2}{\binom{n+1}{2}} = 2$ i dobivamo

$$\lim_{n\to\infty} \frac{c(n)}{\binom{n+1}{2}} = 0. \qquad \square$$

Propozicija 3.11. *Niti u jednom retku Pascalovog trokuta modulo 2 nema blokova oblika* 1101 *i* 1011.

Dokaz. Blokovi $1, 0, a, b$ i $b, a, 0, 1$ pojavit će se u retku Pascalovog trokuta modulo 2 ako i samo ako je $ab \equiv 0 \pmod 2$. Neka su zapisi od n i r u bazi 2

$$n = \sum_{i=0}^{m} n_i 2^i, \; r = \sum_{i=0}^{m} r_i 2^i.$$

Označimo sa r, s, t, u redom brojeve $r, r+1, r+2, r+3$. Označimo sa $seg(n, r)$ niz binomnih koeficijenata $\binom{n}{r}, \binom{n}{s}, \binom{n}{t}, \binom{n}{u}$. Pretpostavimo da je $1, 0, a, b \equiv seg(n, r) \pmod 2$ za $a \not\equiv 0 \pmod 2$. Zbog $\binom{n}{t} \equiv 1 \pmod 2$, $\binom{n}{r} \equiv 1 \pmod 2$ i Teorema 3.5 uz prirodne oznake imamo $r_0 \leqslant n_0$ i $t_0 \leqslant n_0$, pri čemu je ili $r_0 = 0, s_0 = 1, t_0 = 0$ ili $r_0 = 1, s_0 = 0, t_0 = 1$. No druga mogućnost bi davala $n_0 = 1$ i onda $\binom{n}{s} \equiv 1 \pmod 2$. Zato je $t_0 = r_0 = 0$ i $n_0 < s_0 = 1$, tj. $n_0 = 0$.

Neka je

$$R = \sum_{i=1}^{m} r_i 2^{i-1}, \; N = \sum_{i=1}^{m} n_i 2^{i-1}, \; K = \binom{N}{R+1}.$$

Primjenjujući Lucasov teorem imamo

$$a \equiv \binom{n}{t} \equiv K\binom{0}{0} \equiv K \pmod 2,$$
$$b \equiv \binom{n}{u} \equiv K\binom{0}{1} \equiv 0 \pmod 2,$$

tj. $ab \equiv 0 \pmod 2$. Iz simetričnosti svakog reda u Pascalovom trokutu slijedi tvrdnja za blok $b, a, 0, 1$. Blokovi 1101 i 1011 neće se pojaviti u Pascalovom trokutu modulo 2 jer je $1 \cdot 1 \not\equiv 0 \pmod 2$. Dokaz je preuzet iz [8]. $\square$

Teorem 3.12 (Roberts)**.** *Neka je n prirodan broj i neka je*

$$n = n_d 2^d + \cdots + n_1 2^1 + n_0$$

njegov prikaz u bazi 2*. Označimo sa z_n broj koji je dobiven čitanjem n-tog retka Pascalovog trokuta modulo 2 slijeva nadesno. Ako je $S_n = \{i : n_i = 1\}$, tada vrijedi jednakost*

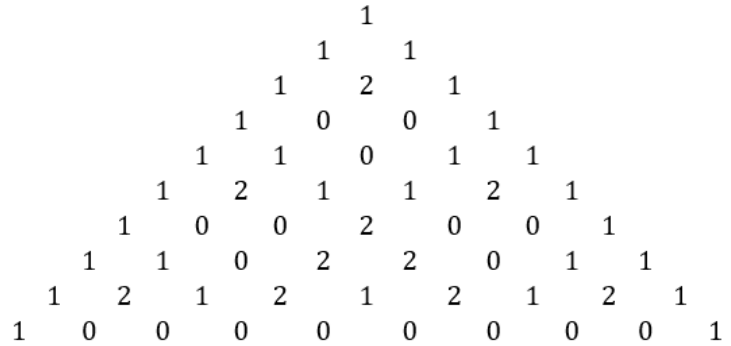
$$z_n = \prod_{i \in S_n} F_i,$$

gdje $F_i = 2^{2^i} + 1$ označava i-ti Fermatov broj.

Dokaz nećemo provoditi, ali se zasniva na činjenici da je red $k = 2^s + m$ u Pascalovom trokutu modulo 2 za $m \in \{0, 1, \ldots, 2^s - 1\}$ zapravo dvije kopije reda m razdvojene sa $2^s - m - 1$ nula. Ova se činjenica dokazuje slično kao drugi dokaz Teorema 3.4.

3.2 Binomni koeficijenti modulo 3

Pogledajmo prvih deset redova Pascalovog trokuta modulo 3 (Slika 3.3). Svaki broj Pascalovog trokuta (Slika 3.1) zamijenili smo ostatkom pri dijeljenju tog broja brojem tri. Primjerice, na mjestu $\binom{8}{3} = 56$ je broj 2 jer je $56 \equiv 2 \pmod 3$. Pascalov trokut modulo 3 se zato sastoji od nula, jedinica i dvojki.



Slika 3.3: Prvih deset redova Pascalovog trokuta modulo 3

Slično kao prije, prema Propoziciji 4.1 vrijedi idući korolar iz kojeg slijedi da su svi redovi kojima je broj potencija broja tri oblika $100\ldots001$.

Korolar 3.13. *Svaki od brojeva*

$$\binom{3^n}{1}, \binom{3^n}{2}, \ldots, \binom{3^n}{3^n-1}$$

je djeljiv s 3.

Propozicija 3.14. *U svakom redu Pascalovog trokuta modulo* 3 *broj jedinica je veći od broja dvojki.*

Dokaz. Polinom s cjelobrojnim koeficijentima zvat ćemo *s-polinomom* ako je broj njegovih koeficijenata koji daju ostatak 1 pri dijeljenju s 3 veći od broja koeficijenata koji daju ostatak 2 pri dijeljenju s 3. Moramo pokazati da je $(1+x)^n$ s-polinom. Neka je

$$n = n_k 3^k + n_{k-1}3^{k-1} + \cdots + n_1 3 + n_0$$

prikaz broja n u bazi 3, gdje su $n_0, n_1, \ldots, n_k \in \{0,1,2\}$. Tada koristeći Propoziciju 2.2 imamo

$$\begin{aligned}(1+x)^n &= (1+x)^{n_k 3^k}(1+x)^{n_{k-1}3^{k-1}}\cdots(1+x)^{n_1 3}(1+x)^{n_0}\\ &\equiv (1+x^{3^k})^{n_k}(1+x^{3^{k-1}})^{n_{k-1}}\cdots(1+x^3)^{n_1}(1+x)^{n_0} \pmod 3.\end{aligned}$$

Za $i \in \{0,1,\ldots,k\}$ neka je

$$F_i = (1+x^{3^i})^{n_i}(1+x^{3^{i-1}})^{n_{i-1}}\cdots(1+x^3)^{n_1}(1+x)^{n_0}.$$

Treba dokazati da je F_k s-polinom. Matematičkom indukcijom dokazat ćemo da su svi polinomi F_i s-polinomi.

Za $i = 0$ tvrdnja je očita jer je $(1+x)^0 = 1$, $(1+x)^1 = 1+x$, $(1+x)^2 = 1+2x+x^2$. Pretpostavimo da je F_i s-polinom za neki $i < k$. Neka je a broj njegovih koeficijenata koji su kongruentni 1 modulo 3, a b broj koeficijenata koji su kongruentni 2 modulo 3. Po definiciji *s*-polinoma vrijedi $a > b$. Promotrimo polinom F_{i+1}. Uočimo najprije da vrijedi

$$F_{i+1} = (1+x^{3^{i+1}})^{n_{i+1}}F_i.$$

Ako je $n_{i+1} = 0$, onda je $F_{i+1} = F_i$, pa je u tom slučaju F_{i+1} s-polinom.

Ako je $n_{i+1} = 1$, tada je $F_{i+1} = (1+x^{3^{i+1}})F_i$. Budući da je stupanj od F_i manji ili jednak $2\cdot 3^i + 2\cdot 3^{i-1} + \cdots + 2\cdot 3 + 2 < 3^{i+1}$, vidimo da je u F_{i+1} broj promatranih koeficijenata jednak $2a$ i $2b$. Znamo da je $a > b$, iz čega slijedi $2a > 2b$, što znači da je i u ovom slučaju F_{i+1} s-polinom.

Ako je $n_{i+1} = 2$, tada je $F_{i+1} = (1+2x^{3^{i+1}} + x^{2\cdot 3^{i+1}})F_i$. Ovoga puta broj koeficijenata koji pri dijeljenju s 3 daju ostatak 1, odnosno ostatak 2 jednak je redom $2a+b$ i $2b+a$. Iz $a > b$ slijedi $2a+b > 2b+a$, tj. F_{i+1} je s-polinom. Dokaz je preuzet iz [17]. □

Označimo s a_n i b_n broj jedinica, odnosno broj dvojki u n-tom redu Pascalovog trokuta modulo 3. Zbog prethodne propozicije znamo da će razlika $a_n - b_n$ uvijek biti pozitivan broj, a može se reći i nešto više.

Propozicija 3.15. *Za svaki prirodan broj n, razlika $a_n - b_n$ je potencija broja dva.*

Zbroj $a_n + b_n$ je broj svih brojeva u n-tom redu Pascalovog trokuta koji nisu djeljivi s 3.

Propozicija 3.16. *Za svaki prirodan broj n, broj $a_n + b_n$ jednak je $2^p 3^q$, gdje su sa p i q označeni broj jedinica, odnosno dvojki u prikazu broja n u bazi* 3.

Dokaz. Koristit ćemo ideju dokaza Propozicije 3.14. Ako je f polinom s cjelobrojnim koeficijentima, označimo s $w(f)$ broj koeficijenata polinoma f koji nisu djeljivi s 3. Neka je

$$n = n_k 3^k + n_{k-1} 3^{k-1} + \cdots + n_1 3 + n_0$$

prikaz broja n u bazi 3, gdje su $n_0, n_1, \ldots, n_k \in \{0, 1, 2\}$. Moramo pokazati da je $w((1+x)^n) = 2^p 3^q$, gdje su brojevi p i q kao u tvrdnji propozicije. Znamo otprije da vrijedi

$$\begin{aligned}(1+x)^n &= (1+x)^{n_k 3^k}(1+x)^{n_{k-1}3^{k-1}} \cdots (1+x)^{n_1 3}(1+x)^{n_0} \\ &\equiv (1+x^{3^k})^{n_k}(1+x^{3^{k-1}})^{n_{k-1}} \cdots (1+x^3)^{n_1}(1+x)^{n_0} \pmod 3.\end{aligned}$$

Za $i \in \{0, 1, \ldots, k\}$, neka je kao prije

$$F_i = (1+x^{3^i})^{n_i}(1+x^{3^{i-1}})^{n_{i-1}} \cdots (1+x^3)^{n_1}(1+x)^{n_0}.$$

Dovoljno je dokazati da je $w(F_k) = 2^p 3^q$. Za $k = 0$ je to očito. Pretpostavimo da tvrdnja vrijedi za F_i, gdje je $i < k$. Neka je a broj koeficijenata u F_i koji su kongruentni 1 modulo 3, a b broj koeficijenata koji su kongruentni 2 modulo 3. Naravno, imamo $w(F_i) = a + b$. Promotrimo polinom F_{i+1}. Prisjetimo se da je

$$F_{i+1} = (1 + x^{3^{i+1}})^{n_{i+1}} F_i$$

te da je stupanj polinoma F_i najviše $3^{i+1} - 1$. Ako je $n_{i+1} = 0$, onda je $F_{i+1} = F_i$ i tvrdnja vrijedi.

Ako je $n_{i+1} = 1$, tada je $F_{i+1} = (1 + x^{3^{i+1}})F_i$. Sada je broj promatranih koeficijenata jednak $2a$ i $2b$. Stoga je

$$w(F_{i+1}) = 2a + 2b = 2(a + b) = 2w(F_i).$$

Ako je $n_{i+1} = 2$, tada je $F_{i+1} = (1 + 2x^{3^{i+1}} + x^{2 \cdot 3^{i+1}})F_i$. Ovoga puta broj promatranih koeficijenata jednak je $2a + b$ i $2b + a$. U ovom slučaju imamo

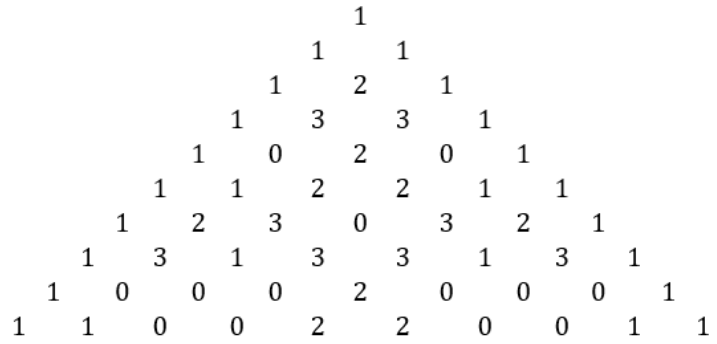
$$w(F_{i+1}) = (2a + b) + (2b + a) = 3(a + b) = 3w(F_i).$$

Iz navedenog proizlazi da je $w(F_k) = 2^u 3^v$, gdje su u i v broj jedinica, odnosno dvojki među brojevima $n_0, n_1, \ldots, n_k$. Očito je $u = p$ i $v = q$. Dokaz je preuzet iz [17]. □

3.3 Binomni koeficijenti modulo 4, 5, 8 i 16

U nastavku ćemo prikazati neke rezultate vezane za pravilnosti u strukturi Pascalovog trokuta modulo m za neke $m \geqslant 4$.

Broj 4 nije prost broj, ali je potencija broja 2. Na Slici 3.4 prikazano je prvih deset redova Pascalovog trokuta modulo 4. Sastoji se od brojeva koji su mogući ostatci pri dijeljenju s 4, a to su $0, 1, 2$ i 3.



Slika 3.4: Prvih deset redova Pascalovog trokuta modulo 4

Označimo s $a_0(n), a_1(n), a_2(n)$ i $a_3(n)$ redom broj nula, jedinica, dvojki i trojki u n-tom redu Pascalovog trokuta modulo 4. Primjerice, $a_1(6) = a_2(6) = a_3(6) = 2$, tj. u šestom redu je broj jedinica, dvojki i trojki jednak i iznosi 2. To nije jedini red u kojem se pojavljuje jednak broj jedinica, dvojki i trojki. Vrijedi još primjerice

$$a_1(11) = a_2(11) = a_3(11) = 4,$$
$$a_1(23) = a_2(23) = a_3(23) = 8,$$
$$a_1(47) = a_2(47) = a_3(47) = 16,$$
$$a_1(95) = a_2(95) = a_3(95) = 32.$$

Možemo primijetiti da se pojavljuju potencije broja dva. Iduća propozicija daje uvjet za pojavljivanje jednakog broja jedinica i trojki u redu.

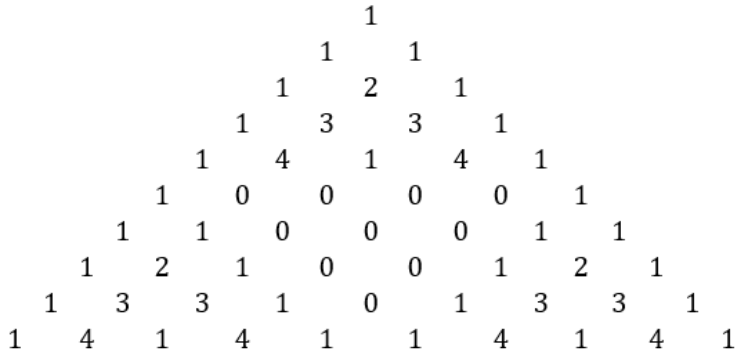
Propozicija 3.17. (1) *Brojevi $a_1(n)$ i $a_3(n)$ jednaki su ako i samo ako se u binarnom zapisu broja n pojavljuje blok* 11*, tj. dvije uzastopne znamenke su jednake* 1.

(2) *Ako je $a_1(n) \neq a_3(n)$, onda je $a_3(n) = 0$.*

(3) *Svaki od brojeva $a_1(n)$ i $a_3(n)$ je ili nula ili potencija broja dva.*

Dokaze ovih tvrdnji dali su Davis i Webb u [4].

Iduća propozicija daje formulu za broj svih brojeva koji nisu nula u pojedinom redu Pascalovog trokuta modulo 5 (Slika 3.5).



Slika 3.5: Prvih deset redova Pascalovog trokuta modulo 5

Propozicija 3.18. *Za svaki prirodan broj n, broj svih brojeva koji nisu djeljivi s* 5 *u n-tom redu Pascalovog trokuta jednak je*

$$2^{a_1}3^{a_2}4^{a_3}5^{a_4},$$

gdje s a_1, a_2, a_3 *i* a_4 *označavamo redom broj jedinica, dvojki, trojki i četvorki u prikazu broja n u bazi* 5*.*

Dokaz. Tvrdnja slijedi uvrštavanjem $p = 5$ u korolar 4.6 kojeg ćemo kasnije iskazati. □

Primjer 3.2. *Broj svih brojeva koji nisu nula u* 7079*. redu Pascalovog trokuta modulo* 5 *je*

$$2^2 \cdot 3^1 \cdot 4^1 \cdot 5^1 = 240$$

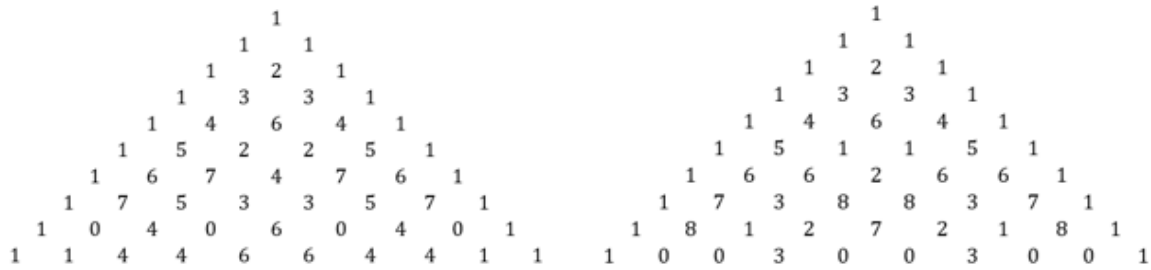
jer je prikaz broja 7079 *u bazi* 5

$$211304_{(5)},$$

tj. $a_1 = 2, a_2 = 1, a_3 = 1$ *i* $a_4 = 1$.

Na Slici 3.6 i Slici 3.7 prikazano je prvih deset redova Pascalovog trokuta modulo 6, 7, 8 i 9.

Slika 3.6: Prvih deset redova Pascalovog trokuta modulo 6 i 7



Slika 3.7: Prvih deset redova Pascalovog trokuta modulo 8 i 9

Označimo s $b_0(n), b_1(n), \ldots, b_7(n)$ redom broj nula, jedinica, ..., sedmica u n-tom redu Pascalovog trokuta modulo 8.

Propozicija 3.19. (1) *Svaki od brojeva* $b_0(n), b_1(n), \ldots, b_7(n)$ *jednak je ili nuli ili potenciji broja dva.*

(2) *Ako u prikazu broja* n *u bazi* 2 *nema blokova* 11 *i* 101*, onda vrijedi* $b_3(n) = b_5(n) = b_7(n) = 0$*.*

(3) *Ako u prikazu broja* n *u bazi* 2 *nema bloka* 11*, ali ima blok* 101*, onda vrijedi* $b_1(n) = b_6(n)$*.*

Vrijedi još primjerice

$$b_1(27) = b_2(27) = b_3(27) = b_4(27) = b_5(27) = b_6(27) = b_7(27) = 4,$$
$$b_1(55) = b_2(55) = b_3(55) = b_4(55) = b_5(55) = b_6(55) = b_7(55) = 8,$$
$$b_1(111) = b_2(111) = b_3(111) = b_4(111) = b_5(111) = b_6(111) = b_7(111) = 16.$$

Za prirodan broj n i $r \in \{0, 1, \ldots, 15\}$, označimo s $c_r(n)$ broj brojeva u n-tom redu Pascalovog trokuta koji su kongruentni r modulo 16.

Propozicija 3.20. (1) *Svaki od brojeva* $c_{2^{s-1}}(n)$*, gdje je* $s \in \{1, 2, 3, 4, 5, 6, 7, 8\}$*, jednak je ili nuli ili potenciji broja dva.*

(2) *Ako je* $n = 111$ *ili* $n = 126$*, tada je* $c_1(n) = c_2(n) = \cdots = c_{15}(n) = 8$*. U binarnom prikazu brojeva* 111 *i* 126 *pojavljuje se* 6 *jedinica i nule čine jedan blok.*

(3) *Ako je n jedan od brojeva* $239, 247, 253, 254$*, tada je* $c_1(n) = c_2(n) = \cdots = c_{15}(n) = 16$*. U binarnom zapisu ovih brojeva pojavljuje se* 7 *jedinica i nule čine jedan blok znamenaka.*

Propozicija 3.19 i Propozicija 3.20 preuzete su iz [17].

Poglavlje 4

Binomni koeficijenti modulo prost broj

Mnogi matematičari su proučavanjem ostataka pri dijeljenju binomnih koeficijenata s potencijama prostih brojeva otkrili pravilnosti. Te se pravilnosti očituju u fraktalnoj strukturi Pascalovog trokuta o kojoj ćemo više u idućem poglavlju. U nastavku ćemo iskazati i dokazati neke rezultate vezane uz primjenu modularne aritmetike na binomne koeficijente te ih povezati s grafičkim prikazom Pascalovog trokuta.

Propozicija 4.1. *Za prirodan broj n, svi brojevi oblika*

$$\binom{p^n}{1}, \binom{p^n}{2}, \ ..., \ \binom{p^n}{p^n - 1}$$

djeljivi su s p.

Dokaz. Neka je $k \in \{1, ..., p^n - 1\}$. Tada imamo

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

iz čega slijedi da je $k\binom{p^n}{k}$ djeljivo s p^n. Budući da je $k < p^n$, znamo da ne može biti djeljiv s p^n. Zaključujemo da $p \mid \binom{p^n}{k}$. □

Propozicija 4.1 nam zapravo govori da su svi redovi Pascalovog trokuta modulo p koji su potencija broja p oblika $10 \ldots 01$.

Propozicija 4.2. *Ako $p \nmid k$, onda je $\binom{pn}{k}$ djeljivo s p.*

Dokaz. Vrijedi jednakost

$$k\binom{pn}{k} = pn\binom{pn - 1}{k - 1}.$$

Iz jednakosti slijedi da je $k\binom{pn}{k}$ djeljivo s p. Znamo da $p \nmid k$, pa zaključujemo da $p \mid \binom{pn}{k}$. □

Ukoliko n-ti red Pascalovog trokuta modulo p ne sadrži niti jednu nulu, onda je n oblika $ap^s - 1$. To je tvrdnja idućeg teorema preuzetog iz [17].

Teorem 4.3. *Neka je p prost broj i n prirodan broj. Sljedeće tvrdnje su ekvivalentne.*

(1) *Niti jedan od brojeva*

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

nije djeljiv s p.

(2) $n = ap^s - 1$, *gdje je* $0 < a \leqslant p$, $s \geqslant 0$.

Dokaz. Za $n < p$ je očito da brojevi $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ nisu djeljivi s p. Zato pretpostavimo da je $n \geqslant p$.

(2) $\Rightarrow$ (1). Pretpostavimo da je $n = ap^s - 1$, gdje je s prirodan broj i $0 < a < p$. Tada je

$$n = (a-1)p^s + (p-1)p^{s-1} + \cdots + (p-1)p^1 + (p-1)$$

prikaz broja n u bazi p. Za svaki $k \in \{0, 1, \ldots, n\}$ prikaz u bazi p je oblika

$$k = b_s p^s + b_{s-1} p^{s-1} + \cdots + b_1 p^1 + b_0,$$

gdje je $b_s \leqslant (a-1)$, $b_0, \ldots, b_s \in \{0, 1, \ldots, p-1\}$. Primjenjujući Lucasov teorem dobivamo

$$\binom{n}{k} \equiv \binom{a-1}{b_s}\binom{p-1}{b_{s-1}} \cdots \binom{p-1}{b_1}\binom{p-1}{b_0} \not\equiv 0 \pmod{p}.$$

Dakle, niti jedan od brojeva $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ nije djeljiv s p.

(1) $\Rightarrow$ (2). Pretpostavimo sada da niti jedan od brojeva $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ nije djeljiv s p. Neka je

$$n = a_r p^r + \cdots + a_1 p + a_0$$

prikaz broja n u bazi p, pri čemu je r prirodan broj i $a_r \neq 0$. Pretpostavimo da je $a_i < p - 1$ za neki $i \in \{0, 1, \ldots, r-1\}$. Iz Lucasovog teorema proizlazi da je tada

$$\binom{n}{(p-1)p^i} \equiv \binom{a_i}{p-1} \equiv 0 \pmod{p},$$

tj. broj $\binom{n}{(p-1)p^i}$ je djeljiv s p, što je suprotno početnoj pretpostavci. Stoga je $a_0 = a_1 = \ldots = a_{r-1} = p-1$ i prema tome $n = a_r p^r + (p-1)p^{r-1} + \cdots + (p-1)p + (p-1) = (a_r+1)p^r - 1$. □

Teorem koji slijedi daje jednostavan algoritam za određivanje djeljivosti binomnog koeficijenta prostim brojem.

Teorem 4.4. *Neka je p prost te m i n nenegativni cijeli brojevi čiji su prikazi u bazi p oblika*

$$m = m_k p^k + m_{k-1} p^{k-1} + \cdots + m_1 p + m_0 \quad i$$
$$n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0.$$

Binomni koeficijent $\binom{m}{n}$ djeljiv je s p ako i samo ako za barem jedan par znamenaka n_i i m_i, $0 \leqslant i \leqslant k$, vrijedi $n_i > m_i$.

Dokaz. Pretpostavimo da je binomni koeficijent $\binom{m}{n}$ djeljiv s p, odnosno

$$\binom{m}{n} \equiv 0 \pmod{p}.$$

Prema Lucasovom teoremu imamo

$$\binom{m}{n} \equiv \binom{m_k}{n_k}\binom{m_{k-1}}{n_{k-1}} \cdots \binom{m_0}{n_0} \pmod{p}.$$

Iz navedenih tvrdnji zaključujemo da je onda za barem jedan i

$$\binom{m_i}{n_i} \equiv 0 \pmod{p}.$$

Zbog $n_i \geqslant 0$ i $m_i < p$, za $m_i \geqslant n_i$ je očito da $p \nmid \binom{m_i}{n_i}$. Stoga je nužno $m_i < n_i$.

Pretpostavimo sada da za barem jedan par znamenaka m_i, n_i, $0 \leqslant i \leqslant k$, vrijedi $n_i > m_i$. Tada je $\binom{m_i}{n_i} = 0$, pa prema Lucasovom teoremu slijedi

$$\binom{m}{n} \equiv 0 \pmod{p},$$

odnosno, binomni koeficijent $\binom{m}{n}$ djeljiv je s p. □

Teorem 4.5 (Fine)**.** *Neka je p prost broj, a n nenegativni cijeli broj čiji je prikaz u bazi p oblika*

$$n = a_k p^k + \cdots + a_1 p^1 + a_0.$$

U nizu brojeva $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ točno je

$$T(n) = (a_0 + 1)(a_1 + 1) \cdots (a_k + 1)$$

brojeva koji nisu djeljivi s p.

Dokaz I. Neka je $i \in \{0, \ldots, n\}$ i neka je $i = i_k p^k + \cdots + i_1 p + i_0$ njegov prikaz u bazi p. Iz Lucasovog teorema slijedi

$$\binom{n}{i} \equiv \binom{a_k}{i_k}\binom{a_{k-1}}{i_{k-1}} \cdots \binom{a_1}{i_1}\binom{a_0}{i_0} \pmod{p}.$$

Tražimo broj cijelih brojeva i za koje vrijedi $0 \leqslant i \leqslant n$ i $\binom{n}{i} \not\equiv 0 \pmod{p}$. Tvrdnji $\binom{n}{i} \not\equiv 0 \pmod{p}$ ekvivalentna je tvrdnja

$$\binom{a_j}{i_j} \not\equiv 0 \pmod{p}$$

za sve $j \in \{0, \ldots, k\}$. Kako je $a_j < p$, svaki i_j biramo iz skupa $\{0, 1, \ldots, a_j\}$. Primjenjujući princip produkta, dobivamo tvrdnju teorema

$$T(n) = (a_0 + 1)(a_1 + 1) \cdots (a_k + 1). \qquad \square$$

Dokaz II. Razmotrimo polinom s cjelobrojnim koeficijentima $(x+1)^n$ modulo p. Broj $T(n)$ je u tom slučaju broj nenul monoma tog polinoma. Koristeći Propoziciju 2.2 imamo

$$\begin{aligned}
(x+1)^n &= (x+1)^{a_k p^k + \cdots + a_1 p + a_0} \\
&= (x+1)^{a_k p^k}(x+1)^{a_{k-1} p^{k-1}} \cdots (x+1)^{a_1 p}(x+1)^{a_0} \\
&\equiv (x^{p^k}+1)^{a_k}(x^{p^{k-1}}+1)^{a_{k-1}} \cdots (x^p+1)^{a_1}(x+1)^{a_0} \\
&\equiv \left(\binom{a_k}{a_k}x^{a_k p^k} + \binom{a_k}{a_k-1}x^{(a_k-1)p^k} + \cdots + \binom{a_k}{0}\right)\left(\binom{a_{k-1}}{a_{k-1}}x^{a_{k-1}p^{k-1}} + \binom{a_{k-1}}{a_{k-1}-1}x^{(a_{k-1}-1)p^{k-1}} + \right. \\
&\left. \cdots + \binom{a_{k-1}}{0}\right) \cdots \left(\binom{a_1}{a_1}x^{a_1 p} + \binom{a_1}{a_1-1}x^{(a_1-1)p} + \cdots + \binom{a_1}{0}\right)\left(\binom{a_0}{a_0}x^{a_0} + \binom{a_0}{a_0-1}x^{a_0-1} + \right. \\
&\left. \cdots + \binom{a_0}{0}\right) \pmod{p}.
\end{aligned}$$

Nakon izvođenja svih množenja, dobivamo da je polinom $(x+1)^n$ modulo p zbroj monoma oblika

$$\binom{a_k}{i_k}\binom{a_{k-1}}{i_{k-1}} \cdots \binom{a_1}{i_1}\binom{a_0}{i_0} x^{i_k p^k + i_{k-1} p^{k-1} + \cdots + i_1 p + i_0},$$

gdje je $i_j \leqslant a_j$ za $j \in \{0, 1, \ldots, k\}$. Monoma ovog oblika ima točno $(a_0+1)(a_1+1)\cdots(a_k+1)$. Svi oni su različitog stupnja zbog jedinstvenosti prikaza broja u bazi p. Dokazi su preuzeti iz [17]. $\square$

Time smo dobili formulu za određivanje broja nenul elemenata n-tog reda Pascalovog trokuta modulo p. Idući korolar je drugačija formulacija prethodnog teorema.

Korolar 4.6. *Neka je p prost broj. Za svaki prirodan broj n, u nizu* $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ *je točno*

$$2^{a_1}3^{a_2}4^{a_3}\cdots(p-1)^{a_{p-2}}p^{a_{p-1}}$$

brojeva koji nisu djeljivi s p, gdje je svaki a_k*, za* $k \in \{1, 2, \ldots, p-1\}$*, broj svih znamenki k koje se javljaju u prikazu broja n u bazi p.*

Primjer 4.1. *Koliko nenul elemenata ima deveti red Pascalovog trokuta modulo* 7*?*

Rješenje. Prikaz broja 9 u bazi 7 glasi

$$9 = 1 \cdot 7^1 + 2.$$

Primjenjujući formulu Teorema 4.5 dobivamo

$$T(9) = (2+1)(1+1) = 6.$$

Primjenom formule Korolara 4.6 dobivamo

$$2^1 \cdot 3^1 \cdot 4^0 \cdot 5^0 \cdot 6^0 = 6.$$

Deveti red Pascalovog trokuta modulo 7 zaista ima šest nenul elemenata u što se možemo uvjeriti na Slici 3.6.

Propozicija 4.7. *Neka je p prost broj i n prirodan broj. Nužan i dovoljan uvjet da svi binomni koeficijenti* $\binom{n}{k}$*,* $0 < k < n$*, budu djeljivi s p jest da n bude potencija broja p.*

Dokaz. Za $k = 0$ i $k = n$ je

$$\binom{n}{k} = 1 \not\equiv 0 \pmod{p},$$

pa je $T(n) \geqslant 2$. Tvrdnji propozicije je ekvivalentna tvrdnja $T(n) = 2$. Prema Teoremu 4.5 to vrijedi ako i samo ako je točno jedna od znamenaka u prikazu broja n u bazi p jednaka 1, a sve ostale znamenke su 0, odnosno prikaz broja n u bazi p je oblika $10\ldots0$. Broj n ima navedeni prikaz u bazi p ako i samo ako je n potencija broja p. Dokaz je preuzet iz [9]. □

Tvrdnja iduće propozicije daje postupak pomoću kojeg možemo odrediti sadrži li neki red Pascalovog trokuta modulo p nulu ili se cijeli sastoji od nenul elemenata.

Propozicija 4.8. *Neka je* $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$, *gdje je* $n_k \neq 0$, *prikaz broja* n *u bazi* p *pri čemu je* p *prost broj. Nužan i dovoljan uvjet da niti jedan binomni koeficijent* $\binom{n}{i}$, *gdje je* $0 \leqslant i \leqslant n$, *nije djeljiv s* p *jest da vrijedi* $n_j = p - 1$, *za sve* $0 \leqslant j \leqslant k - 1$.

Dokaz. Neka je $n^* = n - n_k p^k$. Pretpostavimo da vrijedi $T(n) = n + 1$. Primjenom Teorema 4.5 imamo

$$\begin{aligned} n_k p^k + n^* + 1 = n + 1 &= T(n) \\ &= (n_k + 1) T(n^*) \\ &\leqslant (n_k + 1)(n^* + 1) \\ &= n_k (n^* + 1) + n^* + 1 \\ &\leqslant n_k p^k + n^* + 1. \end{aligned}$$

Prva i posljednja vrijednost su jednake, pa prema tome vrijedi $n^* = p^k - 1$.

Pretpostavimo sada da je $n^* = p^k - 1$. Tada imamo

$$\begin{aligned} T(n) &= (n_k + 1) T(n^*) \\ &= (n_k + 1) p^k \\ &= n_k p^k + n^* + 1 \\ &= n + 1, \end{aligned}$$

što smo i htjeli pokazati. Dokaz je preuzet iz [9]. □

Primijetimo da prethodni rezultat slijedi i direktno iz Teorema 4.3.

Teorem 4.9 (Carlitz)**.** *Neka je* p *prost broj i neka je* $n = n_k p^k + n_{k-1} p^{k-1} + \cdots + n_1 p + n_0$, *gdje je* $n_k \neq 0$, *prikaz broja* n *u bazi* p. *U nizu brojeva* $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ *je točno*

$$\sum_{i=0}^{k-1} (n_0 + 1) \cdots (n_{i-1} + 1)\, (p - 1 - n_i)\, n_{i+1}\, (n_{i+2} + 1) \cdots (n_k + 1)$$

brojeva koji su djeljivi s p *i nisu djeljivi s* p^2.

Propozicija 4.10. *Neka je* p *prost broj. U nekom redu Pascalovog trokuta modulo* p *postoji niz* $1, 0, a, b$ *ako i samo ako je*

$$a(2a + b) \equiv 0 \pmod{p}.$$

Dokaz. Dokaz se može pronaći u [8] na stranicama 578 – 579, a sličan je dokazu Propozicije 3.11. □

Idući rezultati preuzeti su iz članka [11]. Neka su $n = n_d p^d + \cdots + n_1 p + n_0$ i $m = m_d p^d + \cdots + m_1 p + m_0$ prikazi brojeva n i m u bazi p. Ako je p^k najveća potencija broja p koja dijeli binomni koeficijent $\binom{n}{m}$, možemo se pitati koja je vrijednost od $\frac{1}{p^k}\binom{n}{m} \pmod p$. Matematičari Anton (1869.), Stickelberger (1890.), Hensel (1902.) i drugi nakon njih pokazali su da vrijedi

$$\frac{1}{p^k}\binom{n}{m} \equiv (-1)^k \left(\frac{n_0!}{m_0! r_0!}\right)\left(\frac{n_1!}{m_1! r_1!}\right)\cdots\left(\frac{n_d!}{m_d! r_d!}\right) \pmod p,$$

gdje je $r = n - m$. Brojni su se autori pitali postoji li analogna formula, modulo p^q, za proizvoljni $q \geqslant 1$. Tako su došli do formule dane u idućem teoremu.

Za dani prirodan broj n, označimo s $(n!)_p$ umnožak svih prirodnih brojeva manjih ili jednakih broju n koji nisu djeljivi s p.

Teorem 4.11. *Neka je p^q potencija prostog broja p. Neka su m, n i r nenegativni brojevi takvi da je $m = n + r$. Neka je $n = n_d p^d + \ldots n_1 p + n_0$ prikaz broja n u bazi p, a N_j najmanji pozitivni ostatak od $\lfloor n/p^j \rfloor \pmod{p^q}$ za svaki $j \geqslant 0$ (tako da je $N_j = n_j + n_{j+1}p + \ldots + n_{j+q-1}p^{q-1}$). Analogno definiramo m_j, M_j, r_j i R_j. Neka je e_j broj indeksa $i \geqslant j$ za koje je $n_i < m_i$. Tada je*

$$\frac{1}{p^{e_0}}\binom{n}{m} \equiv (\pm 1)^{e_{q-1}} \left(\frac{(N_d!)_p}{(M_d!)_p (R_d!)_p}\right)\cdots\left(\frac{(N_1!)_p}{(M_1!)_p (R_1!)_p}\right)\left(\frac{(N_0!)_p}{(M_0!)_p (R_0!)_p}\right) \pmod{p^q},$$

gdje ± 1 iznosi (-1) osim za $p = 2$ i $q \geqslant 3$.

Dokaz nećemo navoditi, no koristi se generalizacija Wilsonovog teorema. Može se pronaći u drugom poglavlju članka [11].

Teorem 4.12 (Wilsonov teorem)**.** *Prirodan broj p veći od 1 je prost ako i samo ako je*

$$(p-1)! \equiv -1 \pmod p.$$

Dokaz. Dokaz se može pronaći u [18] na stranici 549. □

Generalizirana tvrdnja Wilsonovog teorema, dana idućom lemom, dokazuje se izmjenom Gaussovog dokaza Wilsonovog teorema.

Lema 4.13. *Za svaku potenciju p^q prostog broja p vrijedi*

$$(p^q!)_p \equiv \delta \pmod{p^q},$$

gdje je $\delta = \delta(p^q) = -1$ osim za $p = 2$, $q \geqslant 3$ kada je $\delta = 1$.

Poglavlje 5

Fraktalna struktura Pascalovog trokuta modulo prirodan broj

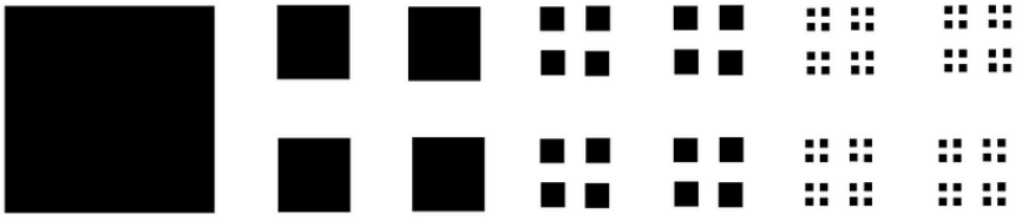
5.1 Fraktali

Najprije ćemo se upoznati s pojmom fraktala. Počeci fraktalne geometrije sežu u 20. stoljeće kada je objavljena knjiga *Fraktalna geometrija prirode* matematičara Benoita Mandelbrota. On je objedinio, proširio i opisao rezultate mnogih matematičara koji su sudjelovali u razvoju fraktalne geometrije, unatoč tome što neki od njihovih rezultata nisu bili dobro prihvaćeni jer su se odvojili od teorija dotadašnje matematike. Naime, do 19. stoljeća euklidska geometrija bila je dovoljna za opisivanje prirode. Za opisivanje su se koristili pojmovi poput točke, pravca, kružnice, kugle, trokuta, stošca itd. No razvojem apstraktnog matematičkog mišljenja, pokazuje se da dotadašnja geometrija ne opisuje u potpunosti oblike poput munja, drveća, pahuljica, planinskih lanaca i slično. Munju ne možemo aproksimirati dužinama, niti je planina stožac. Mandelbrot u svojem djelu opisuje velike mogućnosti novonastale fraktalne geometrije.

Postoji mnogo različitih vrsta fraktala, stoga je nemoguće dati njihovu jedinstvenu definiciju. Možemo reći da su fraktali oblici sa svojstvom da im je svaki dio sličan cjelini. To znači da koliko god uvećamo sliku, vidjet ćemo predmet koji je isti kao neuvećana slika (Slika 5.1) [13].

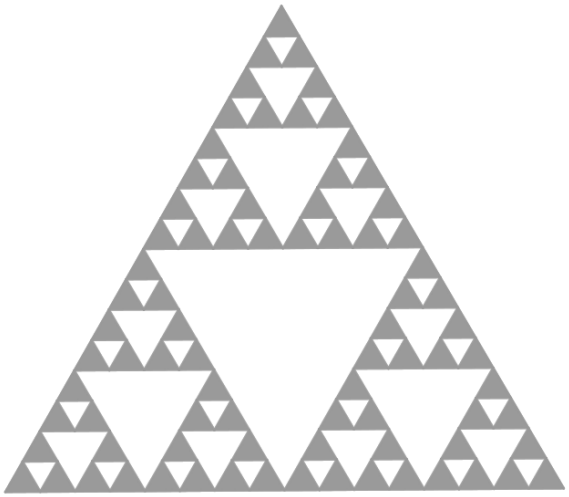
Trokut Sierpinskog

Jedan od najpoznatijih i najjednostavnijih primjera fraktala zove se **trokut (tepih) Sierpinskog**. Dobio je ime prema poljskom matematičaru Waclawu Sierpinskom koji ga je opisao 1915. godine. Trokut Sierpinskog može se konstruirati na različite načine. Najčešće se započne jednakostraničnim trokutom. Spojimo polovišta njegovih stranica čime trokut di-



Slika 5.1: Konstrukcija fraktala zvanog Cantorova prašina

jelimo na četiri sukladna trokuta. Zatim izbacimo središnji trokut. Ponovimo ovaj postupak na tri preostala trokuta i nastavimo ponavljanje beskonačno mnogo puta te dobivamo trokut Sierpinskog (Slika 5.2). Navedeni tijek konstrukcije prikazan je na Slici 5.3 [13, 19].

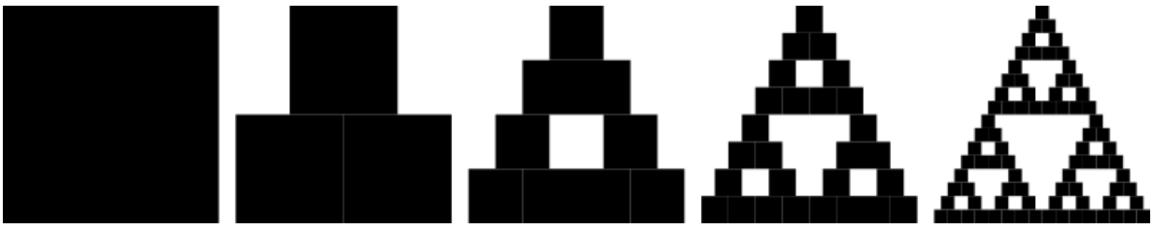


Slika 5.2: Trokut Sierpinskog

Slika 5.3: Konstrukcija trokuta Sierpinskog

Drugi način konstruiranja trokuta Sierpinskog je metodom smanjivanja i umnažanja. Postupak je prikazan na Slici 5.4 za četiri iteracije. Započnemo bilo kakvim zatvorenim

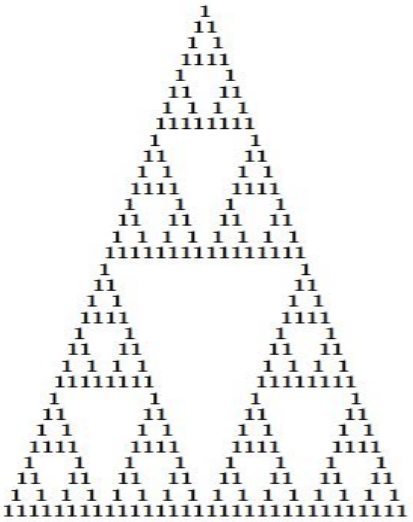
skupom u ravnini, primjerice kvadratom. Dvostruko ga smanjimo, odnosno dvostruko smanjimo njegovu visinu i širinu. Napravimo tri takve kopije te svaku postavimo u jedan vrh "trokuta" na način da se dodiruju. Postupak ponovimo s novodobivenim oblikom. Beskonačnim brojem iteracija dobivamo spomenuti fraktal [1].



Slika 5.4: Konstrukcija trokuta Sierpinskog smanjivanjem i umnažanjem

5.2 Fraktalna struktura Pascalovog trokuta modulo 2

U trećem poglavlju proučili smo pravilnosti koje se javljaju u strukturi Pascalovog trokuta modulo 2. Promotrimo sada prva 32 retka Pascalovog trokuta modulo 2 na način da sve nule obojimo bijelo (Slika 5.5, preuzeta iz [17]). Uočavamo da struktura sliči na spomenuti fraktal – trokut Sierpinskog. U nastavku ćemo dokazati da zaista Pascalov trokut modulo 2 konvergira u trokut Sierpinskog, odnosno da u limesu za beskonačno mnogo redaka Pascalovog trokuta modulo 2 dobivamo trokut Sierpinskog.



Slika 5.5: Pascalov trokut modulo 2

Ideja idućeg dokaza preuzeta je iz [1]. Potrebno je dokazati dvije tvrdnje. Prvo moramo utvrditi da za svaki prirodan broj n, prvih 2^{n+1} redaka Pascalovog trokuta modulo 2 (označimo ih s P_{n+1}) sadrži tri kopije prvih 2^n redaka (označimo ih s P_n) (Slika 5.6). Odnosno, da za sve $0 \leqslant r < 2^n$ i $0 \leqslant c \leqslant r$ vrijedi

$$\binom{r}{c} \equiv \binom{r+2^n}{c} \equiv \binom{r+2^n}{c+2^n} \pmod 2. \tag{5.1}$$

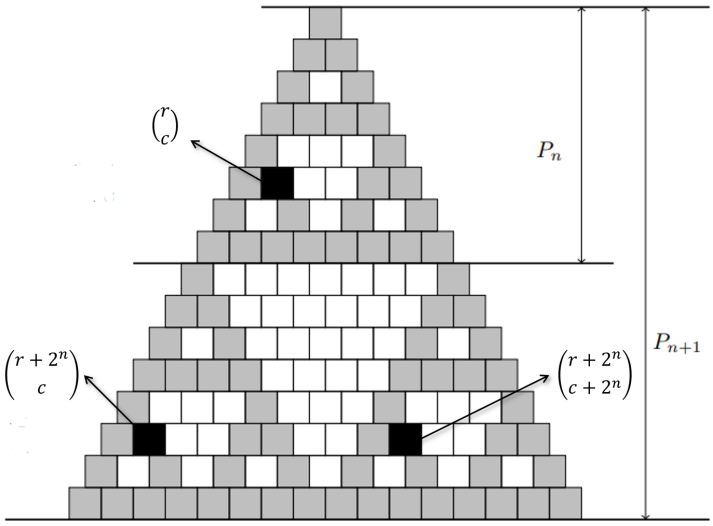
To znači da će se element u retku r i stupcu c kopirati u redak $r + 2^n$ u stupce c i $c + 2^n$. Kongruencija $\binom{r}{c} \equiv \binom{r+2^n}{c} \pmod 2$ slijedi iz (3.1). Primjenom Lucasovog teorema, analogno imamo

$$\binom{r+2^n}{c+2^n} \equiv \binom{1}{1}\binom{r}{c} \equiv \binom{r}{c} \pmod 2,$$

čime je dokazana tvrdnja (5.1). Druga tvrdnja je da prvih 2^{n+1} redaka Pascalovog trokuta modulo 2 sadrži **samo** tri kopije prvih 2^n redaka, tj. da je trokut između tih kopija prazan. To je trokut koji je okrenut jednim vrhom prema dolje. Dovoljno je pokazati da je redak na vrhu tog trokuta oblika $10\ldots01$ jer tada uzastopnom primjenom Pascalovog identiteta slijedi da i ostali retci u tom središnjem trokutu sadrže samo nule. Redak na vrhu je za $r = 2^n$, a već znamo da su krajnji elementi jedinice, odnosno $\binom{r}{0} \equiv \binom{r}{r} \equiv 1 \pmod 2$. Preostaje pokazati da za sve $1 \leqslant c \leqslant 2^n - 1$ vrijedi

$$\binom{2^n}{c} \equiv 0 \pmod 2.$$

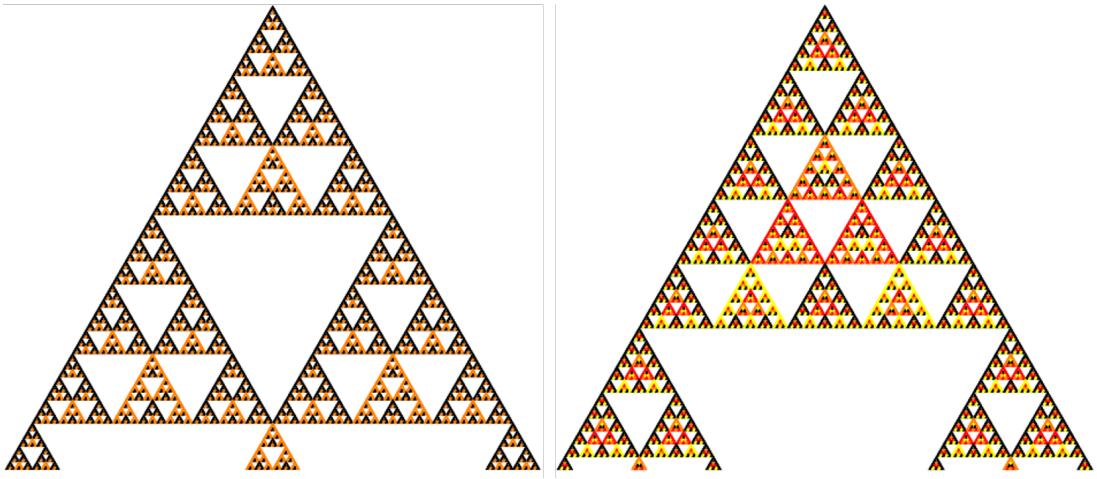
Ova tvrdnja slijedi iz Korolara 3.1.



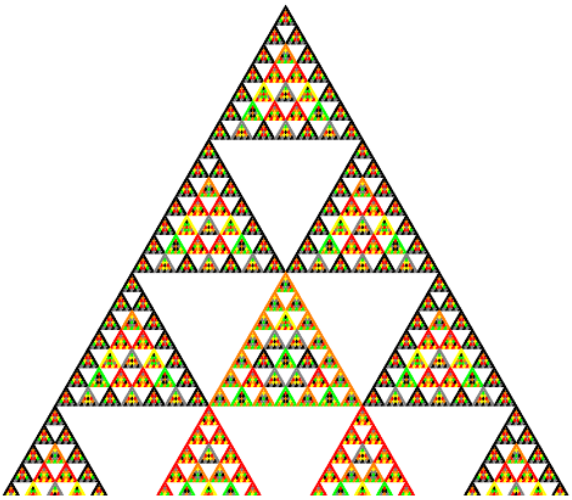
Slika 5.6: Uzorak trokuta Sierpinskog u Pascalovom trokutu modulo 2

5.3 Pascalov trokut modulo prost broj

Za prosti broj p, možemo reći da Pascalov trokut modulo p konvergira u generalizirani oblik trokuta Sierpinskog koji se konstruira metodom smanjivanja i umnažanja. Ta fraktalna struktura može se uočiti na Slikama 5.7 i 5.8 koje redom prikazuju prvih 180 redova Pascalovog trokuta modulo $3, 5$ i 7. Pritom su sve nule obojane bijelo, a ostale vrijednosti drugim bojama.



Slika 5.7: Pascalov trokut modulo 3 (lijevo) i Pascalov trokut modulo 5 (desno)



Slika 5.8: Pascalov trokut modulo 7

Ovog puta umjesto tri kopije imamo $\frac{p(p+1)}{2}$ kopija koje se slažu u veći trokut tako da se vrhovima dodiruju. Za dokaz nam trebaju generalizirane tvrdnje prethodnog potpoglavlja. Najprije treba dokazati da za sve $0 \leqslant l < p$ i $0 \leqslant q \leqslant l$ vrijedi

$$\binom{r}{c} \equiv \binom{r + l \cdot p^n}{c + q \cdot p^n} \pmod{p}.$$

Svaka vrijednost od (l, q) odgovara jednoj od $\frac{p(p+1)}{2}$ kopija. Ova tvrdnja slijedi iz Lucasovog teorema i iz $\binom{l}{q} \not\equiv 0 \pmod{p}$.

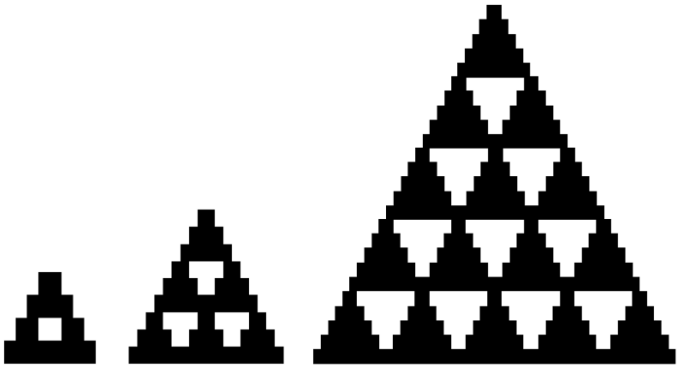
Preostaje pokazati da su svi trokuti okrenuti jednim vrhom prema dolje prazni. Brojevi koji pripadaju tim trokutima odgovaraju binomnim koeficijentima oblika $\binom{r+l\cdot p^m}{c+q\cdot p^m}$, gdje je $r < c < p^m$. Primjenom Lucasovog teorema imamo

$$\binom{r + l \cdot p^m}{c + q \cdot p^m} \equiv \binom{r}{c}\binom{l}{q} \overset{r \leq c}{\equiv} 0 \cdot \binom{l}{q} \equiv 0 \pmod{p}.$$

Time smo dokazali da su svi trokuti okrenuti jednim vrhom prema dolje ispunjeni nulama.

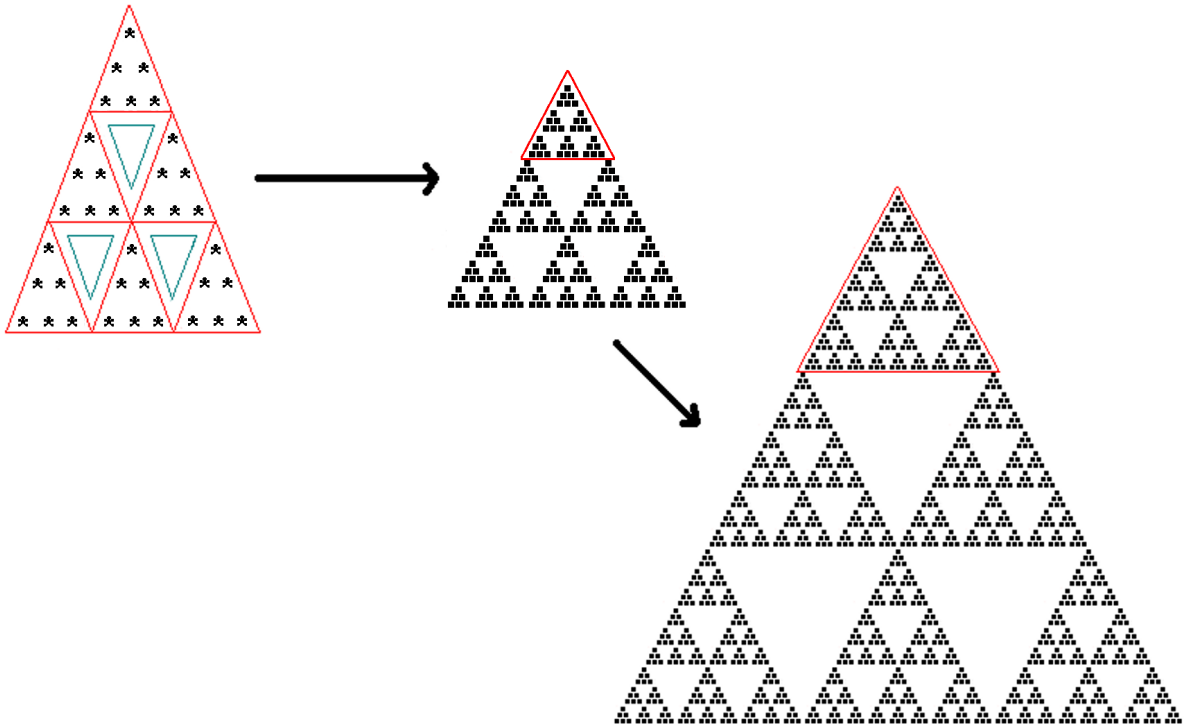
Slaganje spomenutih $\frac{p(p+1)}{2}$ kopija možemo zamisliti kao slaganje blokova prema određenim pravilima. Ponekad ćemo nule ostaviti bijelima, a sve ostale vrijednosti će biti crne. Za prosti broj p, osnovni blok za konstrukciju Pascalovog trokuta modulo p čini prvih p^2 redova, odnosno redovi od 0 do $p^2 - 1$. Za $p = 2$ to su redovi od 0 do 3, za $p = 3$ osnovni blok čine redovi od 0 do 8, a za $p = 5$ redovi od 0 do 24 itd. (Slika 5.9). Svaki osnovni blok sastoji se od $\frac{p(p+1)}{2}$ crnih trokuta.

Bez puno računanja možemo konstruirati velike trokute na način da $\frac{p(p+1)}{2}$ kopija osnovnog bloka posložimo tako da je njihov odnos jednak odnosu crnih trokuta unutar osnovnog



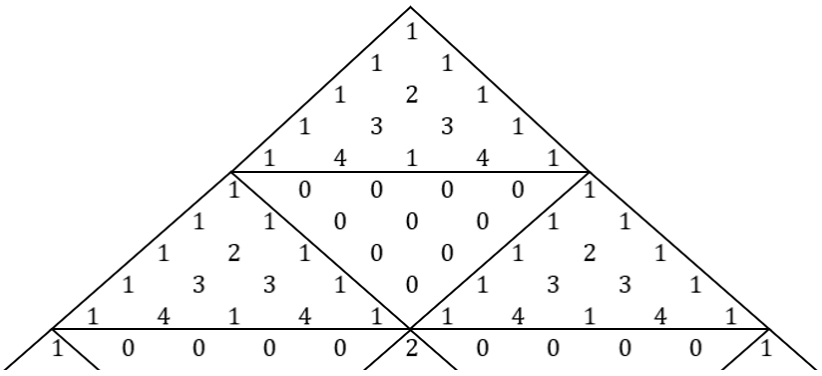
Slika 5.9: Osnovni blok Pascalovog trokuta modulo p za $p \in \{2, 3, 5\}$

bloka. Drugi način kako to možemo vizualizirati je da svaki crni trokut osnovnog bloka zamijenimo kopijom cijelog osnovnog bloka. Taj proces za $p = 3$ prikazan je Slikom 5.10. Preuzeto iz [3].



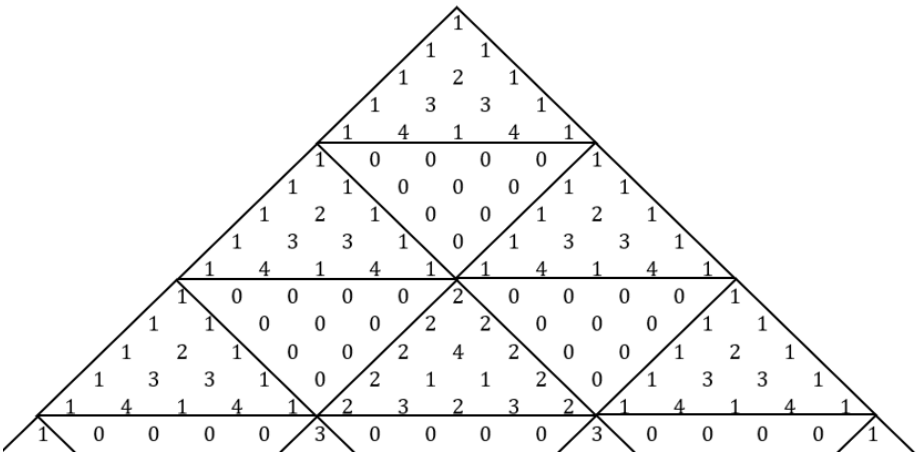
Slika 5.10: Konstrukcija Pascalovog trokuta modulo 3 blokovima

Andrew Granville u članku [11] ima analogni pristup fraktalnoj strukturi Pascalovog trokuta modulo prost broj. Iz Propozicije 4.1 znamo da se p-ti redak Pascalovog trokuta modulo p sastoji od dvije jedinice na svakom kraju i $p-1$ nula između njih. Drugim riječima, p-ti redak je oblika $10\ldots01$. Primjenom Pascalovog identiteta, ispod svake jedinice formira se trokut identičan onome kojeg čini prvih p redova. U $2p$-tom retku tada imamo dvije kopije p-tog retka jedan do drugog, s tim da se u srednjem elementu preklapaju njegovi krajnji elementi. Tako se $2p$-ti redak sastoji od dvije jedinice na svakom kraju, dvojke u sredini, a između njih su nule. Na Slici 5.11 prikazano je prvih 11 redaka Pascalovog trokuta modulo 5.



Slika 5.11: Prvih 11 redova Pascalovog trokuta modulo 5

Ponovno, u $2p$-tom retku ispod svake od jedinica formiramo trokut identičan početnom, odnosno onome kojeg čini prvih p redova, dok ispod dvojke formiramo trokut koji se sastoji od elemenata početnog trokuta pomoženih s brojem 2 (mod p). Tako dobivamo tri nova trokuta. Na sličan način, u $3p$-tom retku se preklapaju tri kopije p-tog retka. To su redom kopije oblika $10\ldots01$, $20\ldots02$ i $10\ldots01$. Tako $3p$-ti redak ima dvije jedinice na svakom kraju, trojke na jednoj i dvije trećine retka te nule na preostalim mjestima. Ispod jedinica formiramo početni trokut, a ispod trojki trokut koji se sastoji od elemenata početnog trokuta pomoženih s brojem 3 (mod p) itd. (Slika 5.12).



Slika 5.12: Prvih 16 redova Pascalovog trokuta modulo 5

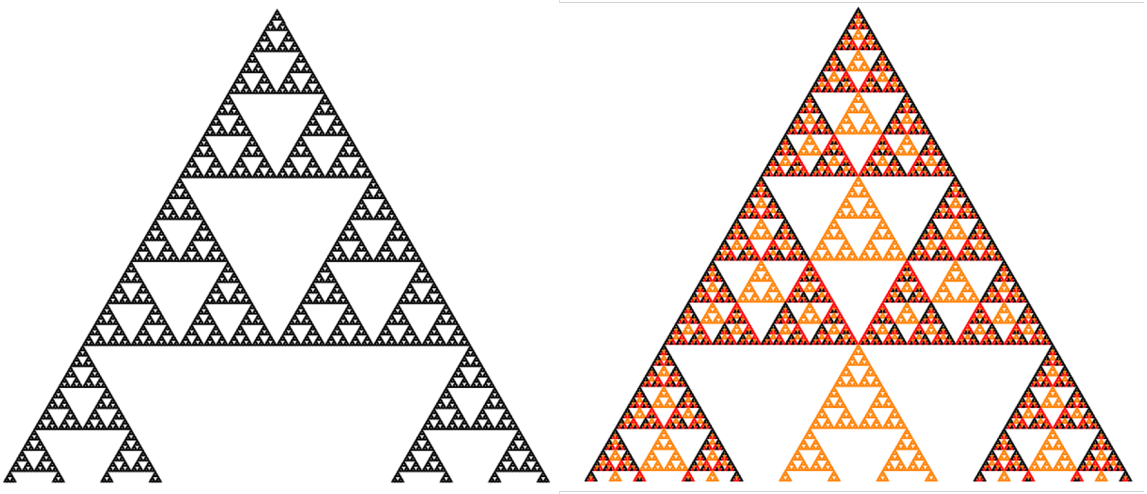
Nastavljanjem ovog postupka uočavamo da je np-ti redak Pascalovog trokuta modulo p kopija n-tog retka s $p-1$ ubačenih nula između uzastopnih elemenata. Idućih $p-1$ redaka dobiveno je formiranjem trokuta ispod svakog nenul elementa np-tog retka takvog da je $\binom{n}{m}$ puta veći od početnog trokuta (mod p) jer je $\binom{np}{mp} \equiv \binom{n}{m} \pmod{p}$. Ovime je zapravo dobiven i rezultat Lucasovog teorema: $\binom{np+k}{mp+j} \equiv \binom{n}{m}\binom{k}{j} \pmod{p}$.

Granville opisuje još jednu zanimljivu posljedicu. Možemo podijeliti Pascalov trokut modulo p na manje trokute. Redovi 0 do $p^k - 1$ tvore prvi takav trokut. Zatim redovi p^k do $2p^k - 1$ su podijeljeni na tri trokuta – dva vanjska i jedan unutarnji okrenut jednim vrhom prema dolje i tako dalje. Bilo koji trokut je tada zbroj dva odgovarajuća trokuta prethodnog reda, tj. trokuta koji imaju s njime jedan zajednički vrh i okrenuti su u istom smjeru. Drugim riječima, trokuti koji tvore Pascalov trokut modulo p podliježu istom pravilu zbrajanja kao i sami elementi Pascalovog trokuta.

5.4 Pascalov trokut modulo potencija prostog broja

Uzorak Pascalovog trokuta postaje kompliciraniji u slučaju s potencijama prostog broja. Na Slici 5.13 možemo usporediti Pascalov trokut modulo 2 i 4. Vidimo da je jedina razlika u njihovim strukturama ta što Pascalov trokut modulo 4 ima dodatne trokute na praznim mjestima Pascalovog trokuta modulo 2.

U članku [1] dokazan je općeniti uzorak Pascalovog trokuta modulo potencija prostog broja. Za prosti broj p, Pascalov trokut modulo p^2 konstruira se na način da se u svakom praznom trokutu Pascalovog trokuta modulo p formira $\frac{p(p-1)}{2}$ kopija Pascalovog trokuta modulo p. Dodavanjem $\frac{p(p-1)}{2}$ kopija Pascalovog trokuta modulo p u svaki prazni trokut



Slika 5.13: Pascalov trokut modulo 2 (lijevo) i Pascalov trokut modulo 4 (desno)

Pascalovog trokuta modulo p^2 dobiva se Pascalov trokut modulo p^3. Iteracijama se može dobiti Pascalov trokut modulo p^k za bilo koji prirodni broj k.

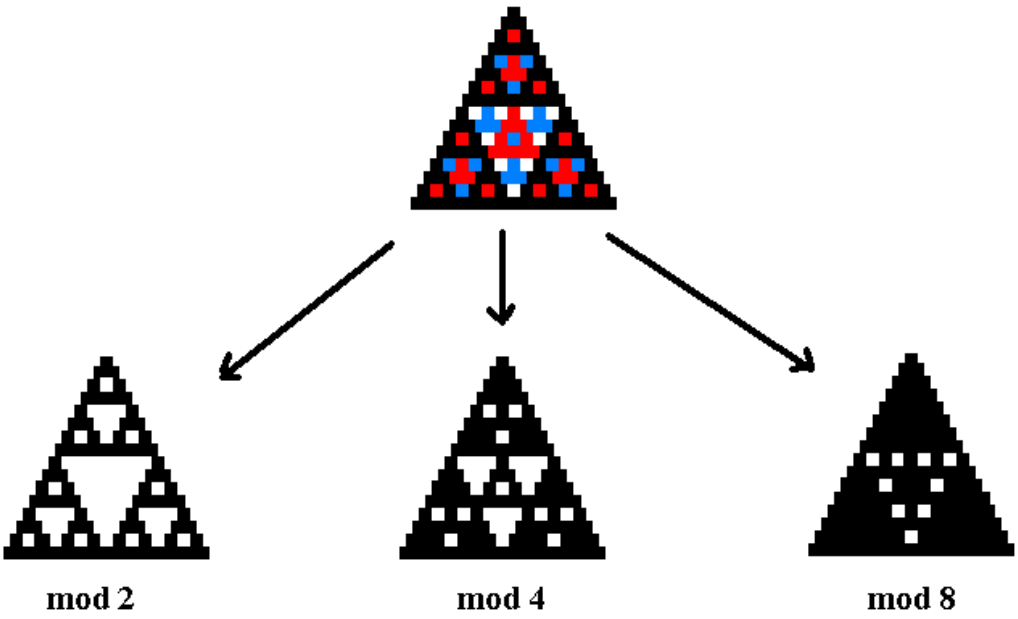
Spomenuto dodavanje kopija možemo predočiti slaganjem blokova prema određenim pravilima. Proučit ćemo najprije konstrukciju blokovima Pascalovog trokuta za manje proste brojeve i njihove potencije, a zatim i za složene brojeve.

Pascalov trokut modulo potencija broja dva

Iduće tvrdnje i slike preuzete su iz [3]. Usporedimo module 2, 4 i 8. Kad je neka pozicija u Pascalovom trokutu modulo 8 obojana bijelo, znači da je binomni koeficijent na tom mjestu djeljiv s 8. Ako je prirodni broj djeljiv s 8, djeljiv je i s 4 i s 2. Zato će ta ista pozicija biti obojana bijelo i u oba Pascalova trokuta modulo 4 i 2. Slično, ako je pozicija u Pascalovom trokutu modulo 2 obojana crno, znači da binomni koeficijent na tom mjestu nije djeljiv s 2. Ako prirodni broj nije djeljiv s 2, neće biti djeljiv niti s 4 niti s 8. Štoviše, neće biti djeljiv niti s jednim parnim brojem. Zato će ta ista pozicija biti crna i u oba Pascalova trokuta modulo 4 i 8.

Uspoređujući navedene trokute zaključujemo da kako modul raste, to crni kvadratići ostaju crni, a neki od bijelih postanu crni. Na Slici 5.14 prikazan je proces prelaska iz Pascalovog trokuta modulo 2 u Pascalov trokut modulo 4 i 8. Tako su u Pascalovom trokutu modulo 2 crvenom bojom prikazani kvadratići koji postanu crni za modulo 4, a plavi kvadratići postanu crni za modulo 8.

Kako bismo utvrdili pravilo prelaska na više potencije prostog broja, vratit ćemo se na Pascalov trokut modulo 2. Možemo ga gledati kao skup bijelih trokuta raznih veličina na

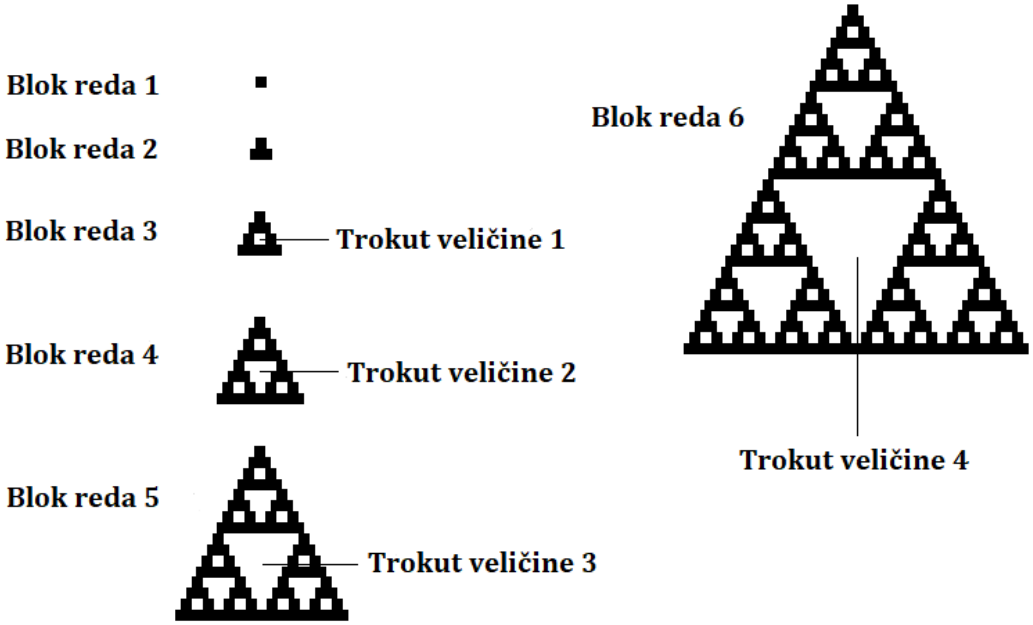


Slika 5.14: Usporedba Pascalovog trokuta modulo 2, 4 i 8

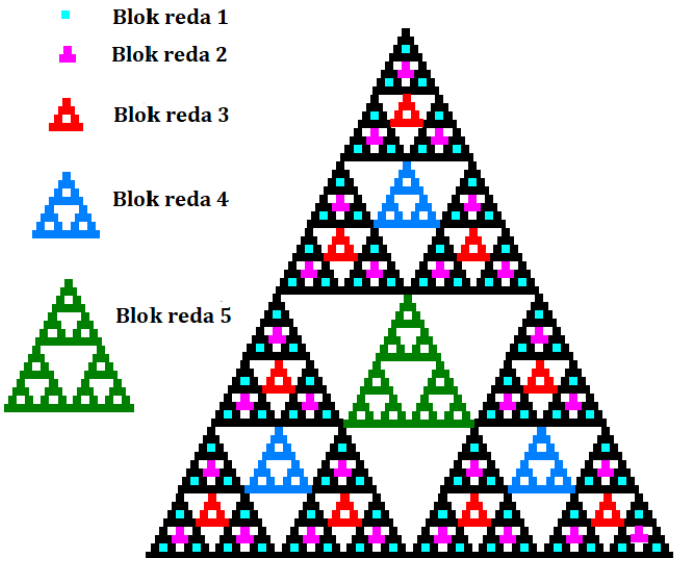
crnoj pozadini. Jedan bijeli kvadratić smatrat ćemo isto trokutom.

Odredimo veličine tih trokuta. Najmanji trokut, veličine 1, bit će jedan bijeli kvadrat koji se nalazi u središtu osnovnog bloka (Slika 5.9). Trokut veličine 2 je onaj koji se nalazi u središtu posložena tri osnovna bloka zajedno. Kako bismo opisali veličine ostalih trokuta, moramo uvesti nove termine. Tako ćemo jedan crni kvadrat smatrati blokom reda 1. Trokut kojeg čini tri crna kvadrata bit će blok reda 2. Trokut kojeg čine tri bloka reda 2 je blok reda 3 (to je ujedno i osnovni blok Pascalovog trokuta modulo 2). Općenito, **blok reda** $n+1$ je trokut kojeg čine tri bloka reda n. Trokut veličine 2 se nalazi u središtu bloka reda 4. Općenito, **trokut veličine** k nalazi se u središtu bloka reda $k+2$ (Slika 5.15).

Opišimo pravilo navedenog prelaska. Svaki bijeli trokut veličine barem dva podijelimo na četiri sukladna trokuta. U sredini će biti trokut jednim vrhom okrenut prema gore, a na njegovim stranicama preostala tri trokuta okrenuta jednim vrhom prema dolje. U trokutu veličine n zamijenit ćemo središnji trokut blokom reda n. Pravilo nije potrebno mijenjati radi trokuta veličine 1. Jednostavno svaki trokut veličine 1 popunimo blokom reda 1. Slika 5.16 prikazuje Pascalov trokut modulo 4 nakon popunjavanja svih odgovarajućih trokuta.



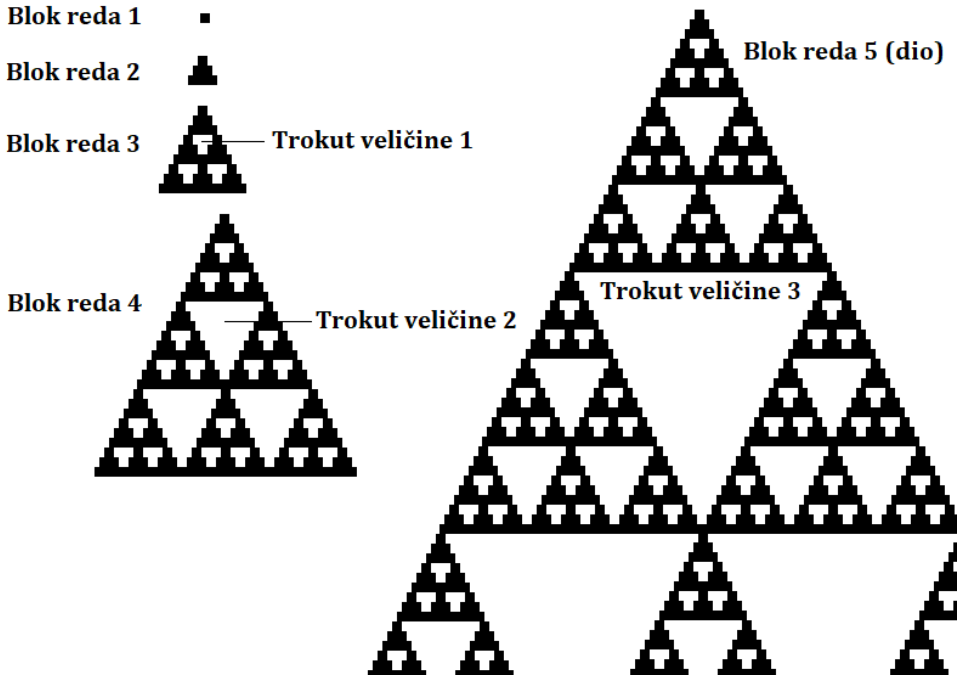
Slika 5.15: Blokovi i trokuti u Pascalovom trokutu modulo 2



Slika 5.16: Pascalov trokut modulo 4 dobiven iz Pascalovog trokuta modulo 2

Pascalov trokut modulo potencija broja tri

Proučimo sada proces prelaska iz Pascalovog trokuta modulo 3 u onaj modulo 9. U osnovnom bloku Pascalovog trokuta modulo 3 nalaze se tri bijela trokuta, za razliku od modulo 2 gdje je bio jedan takav trokut. Njih ćemo zvati trokutima veličine 1. Slaganjem šest osnovnih blokova tako da se odnose kao crni trokuti u osnovnom bloku, dobivamo novi veći blok koji sadrži tri bijela trokuta veličine 2. Blok reda $n+1$ dobivamo slaganjem šest blokova reda n. Blok reda k sadrži tri bijela trokuta veličine $k-2$ (Slika 5.17).

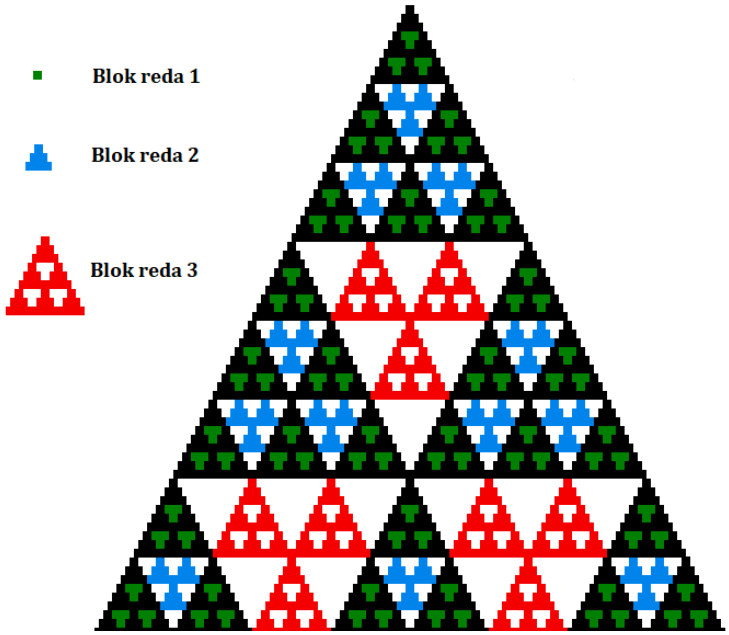


Slika 5.17: Blokovi i trokuti u Pascalovom trokutu modulo 3

Pascalov trokut modulo 9 dobivamo popunjavanjem bijelih trokuta Pascalovog trokuta modulo 3. Opišimo pravilo tog popunjavanja. Ovog puta ćemo bijele trokute podijeliti na devet sukladnih trokuta te popuniti sve one koji su jednim vrhom okrenuti prema gore. Bit će tri takva trokuta. Zato pravilo ostaje isto, trokut veličine n popunjavamo blokovima reda n.

Trokute veličine 1 ne možemo podijeliti na 9 sukladnih trokuta. Zato ćemo kao i prije popuniti te trokute s tri bloka reda 1. Na Slici 5.18 prikazan je Pascalov trokut modulo 9 nakon popunjavanja svih odgovarajućih trokuta.

Analogno, Pascalov trokut modulo 25 dobivamo tako da u Pascalovom trokutu modulo 5 bijele trokute dijelimo na 25 sukladnih trokuta te popunjavamo one koji su jednim vrhom



Slika 5.18: Pascalov trokut modulo 9 dobiven iz Pascalovog trokuta modulo 3

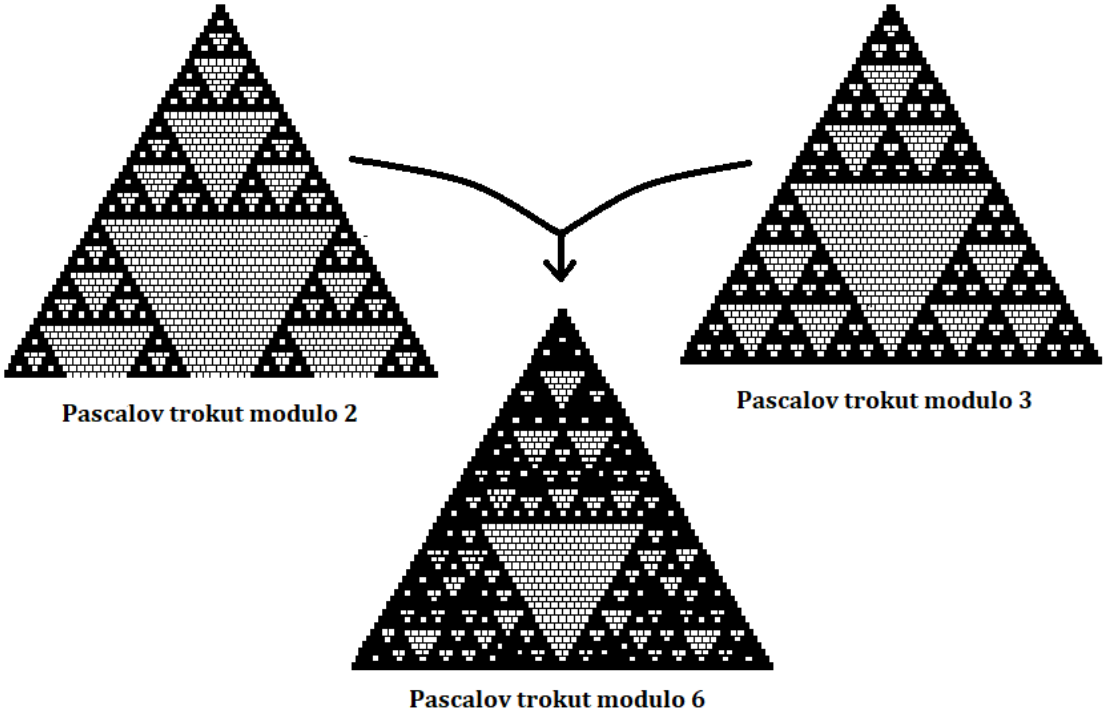
okrenuti prema gore. Općenito, bijele trokute u Pascalovom trokutu modulo p dijelimo na $\underbrace{1+3+5+\ldots+(2p-1)}_{p \text{ članova}} = \frac{p}{2}(1+2p-1) = p^2$ trokuta te popunjavamo $\frac{p(p-1)}{2}$ trokuta okrenuta jednim vrhom prema gore tako da trokute veličine n popunjavamo blokovima reda n.

5.5 Pascalov trokut modulo općeniti složen broj

Prema Osnovnom teoremu aritmetike svaki prirodni broj možemo do na poredak faktora jedinstveno napisati kao umnožak prostih brojeva. Proučimo module koji su složeni brojevi i to takvi da su djeljivi s barem dva različita prosta broja.

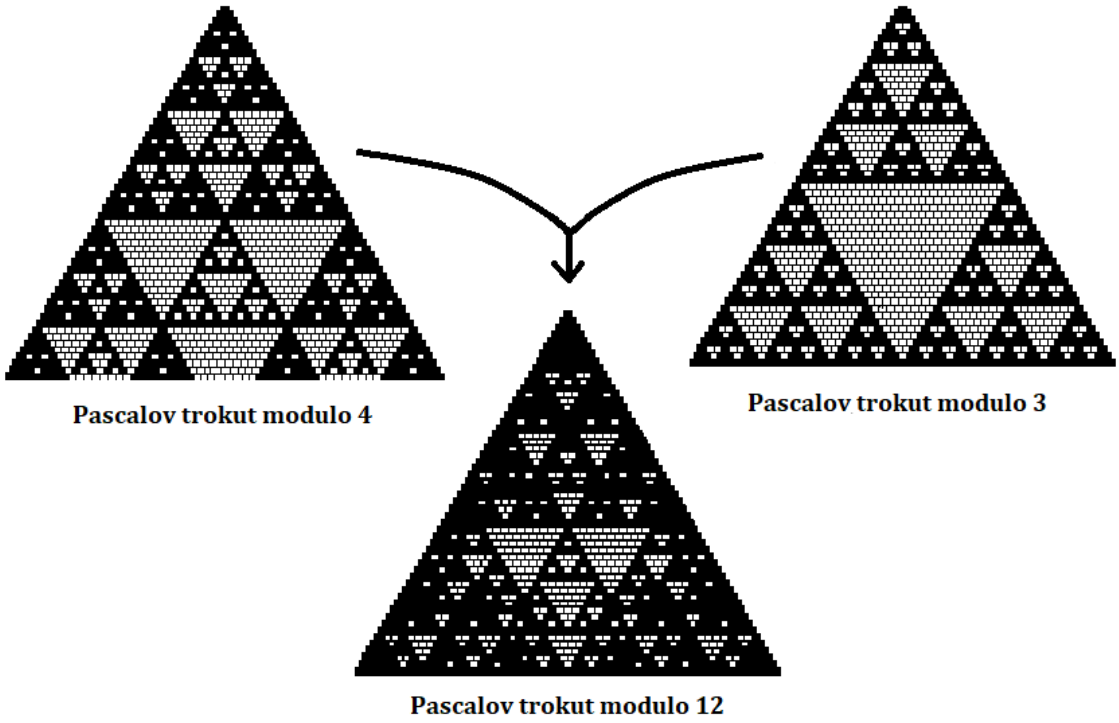
Započnimo s najjednostavnijim primjerom. Ako je neka pozicija u Pascalovom trokutu modulo 6 obojana bijelo, tj. binomni koeficijent na tom mjestu je djeljiv sa 6, onda je ta ista pozicija bijela u oba Pascalova trokuta modulo 2 i 3. Ako je pozicija u nekom od "manjih" trokuta crna, onda će ta ista pozicija biti crna u Pascalovom trokutu modulo 6.

Zaključujemo da kad bismo preklopili Pascalov trokut modulo 2 i 3, jedini bijeli kvadratići koji se pojavljuju odgovaraju onim binomnim koeficijentima koji su djeljivi i s 2 i s 3, a time i sa 6. Zato preklapanjem Pascalovog trokuta modulo 2 i 3 dobivamo Pascalov trokut modulo 6 (Slika 5.19).



Slika 5.19: Pascalov trokut modulo 6 dobiven iz Pascalovog trokuta modulo 2 i 3

Veće module najprije faktoriziramo, odnosno prikažemo ih kao umnožak potencija prostih brojeva. Recimo, $180 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 4 \cdot 9 \cdot 5$. Zatim za svaku potenciju prostog broja slažemo odgovarajuće Pascalove trokute jedan na drugi. Tako bi Pascalov trokut modulo 180 dobili preklapanjem Pascalovog trokuta modulo 4, 9 i 5. Pascalov trokut modulo 12 dobivamo iz Pascalovog trokuta modulo 3 i 4, jer je $12 = 3 \cdot 4$ (Slika 5.20).



Slika 5.20: Pascalov trokut modulo 12 dobiven iz Pascalovog trokuta modulo 3 i 4

Bibliografija

[1] T. Bannink, H. Buhrman, *Quantum Pascal's Triangle and Sierpinski's carpet*, arXiv: 1708.07429, 2017.

[2] H.V. Bigović, *Pascalov trokut*, Matka: časopis za mlade matematičare, Vol. 24, Br. 95 (2013.), 164-167.

[3] B. Cherowitzo, *Pascal's Triangle using Clock Arithmetic-Part I*, dostupno na `http://www-math.ucdenver.edu/~wcherowi/jcorn5.html` (travanj 2021.)

[4] K.S. Davis, W.A. Webb, *Pascal's triangle modulo 4*, Fibonacci Quarterly, Vol. 29 (1991.), 79-83.

[5] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[6] A. Dujella, *Uvod u teoriju brojeva*, dostupno na `http://e.math.hr/zeta/utblink.pdf` (veljača 2021.)

[7] T. Edgar, *Binomial Coefficients Modulo Primes*, Mathematics Magazine, Vol. 93, No. 2 (2020.), 148-149.

[8] *Elementary Problems*, The American Mathematical Monthly, Vol. 87, No. 7 (1980.), 577-581.

[9] N. J. Fine, *Binomial Coefficients Modulo a Prime*, The American Mathematical Monthly, Vol. 54, No. 10, Part 1 (1947.), 589-592.

[10] K. Ge, *Two Theorems on Binomial Coefficients*, dostupno na `http://www.aquatutoring.org/KummerTheoremLucasTheorem.pdf` (veljača 2021.)

[11] A. Granville, *Arithmetic properties of binomial coefficients. I. Binomial coefficients modulo prime powers*. Organic mathematics (Burnaby, BC, 1995), 253–276, CMS Conf. Proc., 20, Amer. Math. Soc., Providence 1997.

[12] W. L. Hosch, *Pascal's triangle*, Encyclopedia Britannica (2013.), dostupno na `https://www.britannica.com/science/Pascals-triangle` (siječanj 2021.)

[13] I. Ivančić, *Fraktalna geometrija i teorija dimenzije*, Odjel za matematiku, Sveučilište u Osijeku, Diplomski rad, Osijek, 2019.

[14] A. Karttunen, *On Pascal's triangle modulo 2 in Fibonacci representation*, The Fibonacci Quarterly, Vol. 42 (2004.), 38-46.

[15] V. Krčadinac, *Osnove algoritama*, dostupno na `https://web.math.pmf.unizg.hr/~krcko/nastava/oa/oa-skripta.pdf` (prosinac 2020.)

[16] M. Mesarić, *Pascalov trokut*, Matka: časopis za mlade matematičare, Vol. 21, No. 83 (2013.), 154-157.

[17] A. Nowicki, *Podróże po Imperium Liczb, Silnie i Symbole Newtona* (poglavlje 6, Symbole Newtona i podzielność; poglavlje 8, Trójkat Pascala modulo m), Olsztyn, Toruń 2011.

[18] B. Pavković, D. Veljan, *Elementarna matematika II*, Školska knjiga, Zagreb 1995.

[19] J. Šikić, *Trokut Sierpinskog*, Matka: časopis za mlade matematičare, Vol. 23, No. 89 (2014.), 13-15.

[20] D. Veljan, *Kombinatorna i diskretna matemtika*, Algoritam, Zagreb 2001.

Sažetak

Primjena modularne aritmetike na binomne koeficijente interesirala je mnoge matematičare 19. stoljeća, ali i matematičare novijeg razdoblja. U radu su izloženi rezultati vezani uz ostatke pri dijeljenju binomnih koeficijenata s potencijama prostih brojeva te njihovi prikazi preko Pascalovog trokuta.

U prvom poglavlju dani su osnovni pojmovi i tvrdnje potrebne za razumijevanje daljnjeg rada. U drugom poglavlju navedene su i dokazane tvrdnje matematičara Lucasa, Legendrea i Kummera. Tako su uključeni rezultati poput Lucasovog teorema koji daje jednostavnu metodu izračunavanja vrijednosti binomnog koeficijenta $\binom{m}{n}$ modulo prost broj p pomoću znamenaka zapisa brojeva m i n u bazi p.

U iduća dva poglavlja su iskazani i dokazani rezultati vezani uz spomenuti problem kongruencija za binomne koeficijente. U trećem poglavlju navedeni su rezultati koji se odnose na konkretne module, manje prirodne brojeve, a u četvrtom poglavlju rezultati vezani uz općenite module koji su prosti brojevi. Posljednje poglavlje posvećeno je fraktalnoj strukturi Pascalovog trokuta promatranog modulo zadani broj.

Summary

Numerous mathematicians of the nineteenth century considered problems involving binomial coefficients in terms of modular arithmetic. In this master thesis results related to binomial coefficients modulo a prime power as well as their representation on Pascal's triangle are given.

Collected in the first chapter are basic notions and statements necessary to understand the rest of the thesis. In the second chapter are stated and proved Lucas', Legendre's and Kummer's theorem. Lucas' theorem gives a simple method of computing binominal coefficient $\binom{m}{n}$ modulo a prime number p using the digits of base p representations of integers m and n.

In the next two chapters results related to congruences for binomial coefficients are stated and proved. In the third chapter results considering specific, smaller natural numbers as moduli are presented, while in the fourth chapter results valid for general prime moduli are given. The last chapter is devoted to the fractal structure of Pascal's triangle modulo a fixed integer.

Životopis

Rođena sam 22. veljače 1997. godine u Karlovcu. Započela sam školovanje 2003. godine u Osnovnoj školi Banija. Nakon osnovne škole sam 2011. godine upisala opći smjer Gimnazije Karlovac koju sam završila 2015. godine s odličnim uspjehom. U gimnaziji sam pohađala DSD-program te stekla Njemačku jezičnu diplomu. Nastavila sam svoje obrazovanje 2015. godine upisom preddiplomskog studija Matematike, nastavnički smjer na Prirodoslovno-matematičkom fakultetu u Zagrebu. Godine 2018. postala sam sveučilišna prvostupnica edukacije matematike i te sam godine upisala diplomski studij Matematike, nastavnički smjer na istom fakultetu.