Wolstenholmeov teorem

Jović, Lucija

SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Lucija Jović

WOLSTENHOLMEOV TEOREM

Diplomski rad

Voditelj rada:
doc. dr. sc. Tomislav Pejković

Zagreb, studeni 2019.

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 ukazanom povjerenju i pruženoj pomoći tijekom izrade diplomskog rada.
Od srca se zahvaljujem svojoj obitelji, dečku i prijateljima na neizmjernoj podršci.
Ovaj rad posvećujem svojim roditeljima.

Sadržaj

Uvod

Teorija brojeva spada među najstarije grane matematike. Prvi tragovi teorije brojeva mogu se pronaći kod Babilonaca iz polovice trećeg tisućljeća prije Krista. Tada su nađeni popisi brojeva koje nazivamo Pitagorine trojke. Ova grana matematike proučava svojstva skupova prirodnih, cijelih i racionalnih brojeva. Jedan od najvažnijih pojmova u teoriji brojeva je pojam djeljivosti kojim su se bavili mnogi poznati matematičari. Jedan od njih je i Joseph Wolstenholme.

Joseph Wolstenholme

Joseph Wolstenholme engleski je matematičar rođen 1829. godine u Ecclesu. Diplomirao je na St John Collegeu Sveučilišta u Cambridgeu 1850. godine kao treće rangirani student matematike te je nastavio raditi na istom sveučilištu. Godine 1871. postao je profesorom matematike na *Royal Indian Engineering Collegeu*. Autor je niza matematičkih radova u kojima se bavio pitanjima analitičke geometrije, a obilježila ih je osebujna analitička vještina i domišljatost. U suradnji s engleskim matematičarom Percivalom Frostom izdao je 1863. knjigu *Treatise on Solid Geometry*. Njegova zbirka matematičkih problema u kojoj se nalazi oko tri tisuće zadataka dala je značajan doprinos matematičkom obrazovanju kao pomoć i poticaj mnogim studentima.

Wolstenholme je među ostalim proučavao ostatke dijeljenja s prostim brojevima. Ovaj diplomski rad posvećen je Wolstenholmeovom teoremu, interesantnom rezultatu iz teorije

brojeva, za kojeg danas postoje brojne varijacije i generalizacije. Teorem je iskazao i dokazao 1862. godine u svom članku *On certain properties of prime numbers* koji je objavljen u časopisu *The Quarterly Journal of Pure and Applied Mathematics*.

U prvom poglavlju ovog rada iskazani su pojmovi i tvrdnje koje će olakšati daljnje razumijevanje. U drugom poglavlju iskazan je i dokazan Wolstenholmeov teorem, a zatim je navedena i tvrdnja ekvivalentna teoremu. U sljedećem poglavlju dano je nekoliko varijacija i generalizacija teorema, a u zadnjem poglavlju provjerava se vrijedi li i kada obrat Wolstenholmeovog teorema.

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

Na početku rada definirat ćemo osnovne pojmove vezane uz djeljivost i kongruencije i navesti teoreme koje ćemo koristiti u dokazivanju tvrdnji u sljedećim poglavljima.

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

Teorem 1.2 (**Teorem o dijeljenju s ostatkom**). *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je $b = q \cdot a + r$, $0 \leq r < a$.*

Dokaz. Dokaz se nalazi u [4] na stranici 2. □

Definicija 1.3. *Neka su b i c cijeli brojevi. Cijeli broj a zovemo zajednički djelitelj od b i c ako $a \mid b$ i $a \mid c$. Ako je barem jedan od brojeva b i c različit od nule, onda postoji konačno monogo zajedničkih djelitelja od b i c. Najveći među njima zove se najveći zajednički djelitelj od b i c i označava se s (b, c).*

Definicija 1.4. *Prirodan broj $p > 1$ koji je djeljiv samo s 1 i sa samim sobom nazivamo prost broj. Ako prirodan broj $a > 1$ nije prost, onda kažemo da je složen.*

Teorem 1.5. *Ako je p prost i $p \mid ab$, onda $p \mid a$ ili $p \mid b$.*

Dokaz. Dokaz se nalazi u [5] na stranici 7. □

Definicija 1.6. *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 $a \not\equiv b \pmod{m}$.*

Teorem 1.7. *Relacija "biti kongruentan modulo m" je relacija ekvivalencije na skupu $\mathbb{Z}$.*

Dokaz. Dokaz se nalazi u [5] na stranici 12. □

Teorem 1.8. *Neka su a, b, c, d cijeli brojevi.*

(1) Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a+c \equiv b+d \pmod{m}$, $a-c \equiv b-d \pmod{m}$, $ac \equiv bd \pmod{m}$.

(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. Dokaz se nalazi u [5] na stranici 12. □

Definicija 1.9. *Skup $\{x_1, \ldots, x_m\}$ zove se 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.*

Definicija 1.10. *Reducirani sustav ostataka modulo m je skup cijelih brojeva r_i sa svojstvom da je $(r_i, m) = 1, r_i \not\equiv r_j \pmod{m}$ za $i \neq j$, te da za svaki cijeli broj x takav da je $(x, m) = 1$ postoji r_i takav da je $x \equiv r_i \pmod{m}$. Jedan reducirani sustav ostataka modulo m je skup svih brojeva $a \in \{1, 2, \ldots, m\}$ takvih da je $(a, m) = 1$. Svi reducirani sustavi ostataka modulo m imaju isti broj elemenata. Taj broj označavamo sa $\varphi(m)$, a funkciju $\varphi(m)$ zovemo Eulerova funkcija.*

Teorem 1.11. *Neka je $\{x_1, \ldots, x_m\}$ reducirani sustav ostataka modulo m te neka je $(a, m) = 1$. Tada je $\{ax_1, \ldots, ax_m\}$ također reducirani sustav ostataka modulo m.*

Dokaz. Dokaz se nalazi u [5] na stranici 17. □

Teorem 1.12 (**Kineski teorem o ostatcima**). *Neka su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, a_2, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1},\ x \equiv a_2 \pmod{m_2}, \ldots,\ x \equiv a_r \pmod{m_r} \tag{1.1}$$

ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja od (1.1) dana sa $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

Dokaz. Dokaz se nalazi u [5] na stranici 15. □

Teorem 1.13 (**Mali Fermatov teorem**). *Neka je p prost broj. Ako $p \nmid a$, onda je $a^{p-1} \equiv 1 \pmod{p}$. Za svaki cijeli broj a vrijedi $a^p \equiv a \pmod{p}$.*

Dokaz. Dokaz se nalazi u [5] na stranici 18. □

Teorem 1.14 (**Wilsonov teorem**). *Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.*

Dokaz. Za $p = 2$ i $p = 3$ kongruencija očito vrijedi. Pretpostavimo da je $p \geq 5$.Grupirajmo članove skupa $\{2, 3, \ldots, p-2\}$ u parove (i, j) sa svojstvom $i \cdot j \equiv 1 \pmod{p}$. Vrijedi da je $i \neq j$ jer bi inače broj $(i-1)(i+1)$ bio djeljiv sa p, što je nemoguće zbog $0 < i-1 < i+1 < p$. Time dobivamo $\frac{p-3}{2}$ parova i množenjem tih $\frac{p-3}{2}$ kongruencija dobivamo

$$2 \cdot 3 \cdots (p-2) \equiv 1 \pmod{p},$$

pa je

$$(p-1)! \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}.$$ □

Teorem 1.15 (**Lagrangeov teorem).** *Neka je $f(x)$ polinom s cjelobrojnim koeficijentima stupnja n. Pretpostavimo da je p prost broj te da vodeći koeficijent od f nije djeljiv s p. Tada kongruencija $f(x) \equiv 0 \pmod{p}$ ima najviše n rješenja modulo p.*

Dokaz. Dokaz se nalazi u [5] na stranici 21. □

Definicija 1.16. *Neka je $(a, m) = 1$. Ako kongruencija $x^2 \equiv a \pmod{m}$ ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U protivnom kažemo da je a kvadratni neostatak modulo m. Ako je m prost broj, onda postoji točno $\frac{m-1}{2}$ nekongruentnih kvadratnih ostataka modulo m i $\frac{m-1}{2}$ kvadratnih neostataka modulo m.*

Teorem 1.17 (**Prikaz broja u bazi).** *Neka je $b \geq 2$ zadani prirodan broj. Za svaki prirodan broj n postoji jedinstven niz znamenaka $(x_k, \ldots, x_1, x_0)$, $x_i \in \{0, 1, \ldots, b-1\}$ za $i \in \{0, 1, \ldots, n\}$, $x_k \neq 0$, takav da je*

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

Ovaj zapis nazivamo zapis broja n u bazi b.

Dokaz. Prvo dokazujemo egzistenciju, a zatim jedinstvenost prikaza broja n u bazi b.

Označimo $n_0 = n$. Podijelimo taj broj sa b i prema Teoremu 1.2 postoje n_1 i x_0 takvi da je

$$n_0 = n_1 \cdot b + x_0.$$

Zatim podijelimo n_1 s b i dobivamo

$$n_1 = n_2 \cdot b + x_1.$$

Postupak analogno nastavljamo dok kvocijent ne bude 0. Dobivamo

$$n_2 = n_3 \cdot b + x_2,$$

$$n_3 = n_4 \cdot b + x_3,$$

$$\vdots$$

$$n_k = 0 \cdot b + x_k.$$

Svi daljnji kvocijenti i ostaci bili bi jednaki 0. Jasno je da cjelobrojnim dijeljenjem s $b \geq 2$ postupak staje nakon konačno mnogo koraka jer imamo $n_0 > n_1 > n_2 > n_3 \ldots$ Za sve x_i takve da je $0 \leq i \leq k$ vrijedi $0 \leq x_i \leq b - 1$. Pretpostavimo da smo nakon k koraka dobili kvocijent $n_{k+1} = 0$. Tada je $n_k = n_{k+1} \cdot b + x_k = x_k$ i supstitucijom u prethodne korake dobivamo

$$n_{k-1} = x_k b + x_{k-1},$$
$$n_{k-2} = x_k b^2 + x_{k-1} b + x_{k-2},$$
$$\vdots$$
$$n_1 = x_k b^{k-1} + \cdots + x_1,$$
$$n_0 = x_k b^k + \cdots + x_1 b + x_0.$$

Dakle,

$$n = n_0 = x_k b^k + \cdots + x_1 b + x_0, \tag{1.2}$$

čime smo dokazali egzistenciju. Sada još treba dokazati jedinstvenost tog prikaza. Pretpostavimo da n ima još jedan prikaz u bazi b

$$n = y_l b^l + \cdots + y_1 b + y_0.$$

Tada je

$$n_0 = x_k b^k + \cdots + x_1 b + x_0 = y_l b^l + \cdots + y_1 b + y_0.$$

Sada iz $x_0 \equiv y_0 \pmod{b}$ te zbog $x_0, y_0 \in \{0, 1, \ldots, b-1\}$ vrijedi $x_0 = y_0$. Stoga je

$$n_1 = \frac{n - x_0}{b} = x_k b^k + \cdots + x_1 = y_l b^l + \cdots + y_1.$$

Analogno nastavimo postupak i dobivamo $x_i = y_i$ za svaki $i = 0, 1, 2, \ldots$ te $k = l$, čime smo dokazali jedinstvenost. □

Definicija 1.18. *Neka su m i n nenegativni cijeli brojevi. Broj svih n-članih podskupova m-članog skupa označavamo simbolom $\binom{m}{n}$ i nazivamo ga binomni koeficijent. Vrijedi*

$$\binom{m}{n} = \frac{m(m-1)(m-2)\cdots(m-n+1)}{n(n-1)\cdots 1},$$

odnosno za $m \geq n$

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

Ako je $m < n$, onda je $\binom{m}{n} = 0$.

Teorem 1.19 (**Binomni teorem**). *Za svaki nenegativni cijeli broj m i realne brojeve x i y vrijedi*

$$(x+y)^m = x^m + \binom{m}{1}x^{m-1}y + \cdots + \binom{m}{n}x^{m-n}y^n + \cdots + \binom{m}{m-1}xy^{m-1} + y^m = \sum_{n=0}^{m}\binom{m}{n}x^{m-n}y^n.$$

Dokaz. Dokaz se nalazi u [15] na stranicama 78-79. □

Teorem 1.20 (**Lucasov teorem**). *Neka su m i n nenegativni cijeli brojevi, a p prost broj. Ako su*

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

zapisi brojeva m i n u bazi p, onda je

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

Dokaz. Dokaz se nalazi u [6] na stranicama 589-592. □

Poglavlje 2

Wolstenholmeov teorem

Još od 19. stoljeća poznati matematičari proučavali su probleme vezane uz ostatke dijeljenja s potencijama prostih brojeva. Neki od značajnijih bili su Babbage, Cauchy, Cayley, Gauss, Hensel, Hermite, Kummer, Legendre, Lucas, Stickelberg i Wolstenholme.

U ovom poglavlju iskazat ćemo i dokazati Wolstenholmeov teorem te navesti tvrdnje koje direktno slijede iz tog teorema.

Teorem 2.1 (**Wolstenholmeov teorem).** *Ako je $p \geq 5$ prost broj, onda je brojnik racionalnog broja*

$$1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1} \tag{2.1}$$

djeljiv s p^2.

Dokaz. Neka je $p \geq 5$ prost.
Promotrimo polinom

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - (x^{p-1} - 1).$$

Stupanj od f je manji ili jednak $p-2$ pa stoga polinom f možemo zapisati kao

$$f(x) = a_{p-2}x^{p-2} + a_{p-3}x^{p-3} + \cdots + a_1 x + a_0.$$

Prema Malom Fermatovom teoremu vrijedi $x^{p-1} - 1 \equiv 0 \pmod{p}$ za cijeli broj x koji nije djeljiv sa p.

Zato za $x \in \{1, 2, 3, \ldots, p-1\}$ vrijedi $f(x) = 0$ iz čega slijedi da kongruencija $f(x) \equiv 0 \pmod{p}$ ima barem $p-1$ rješenja modulo p. No, stupanj od f je najviše $p-2$, pa po Lagrangeovom teoremu polinom f mora biti nulpolinom modulo p, tj. $a_n \equiv 0 \pmod{p}$ za sve $n \in \{0, 1, \ldots, p-2\}$.

Uvrštavanjem $x = 0$ u polinom f dobivamo

$$f(0) = (-1)^{p-1}(p-1)! + 1 = a_0,$$

tj. $a_0 = (p-1)! + 1$. Budući da je $a_0 \equiv 0 \pmod{p}$, vrijedi $(p-1)! + 1 \equiv 0 \pmod{p}$ tj. $(p-1)! \equiv -1 \pmod{p}$, čime smo dokazali Wilsonov teorem na drugi način. Uvrštavanjem $x = p$ u polinom f imamo

$$f(p) = (p-1)! - p^{p-1} + 1 = a_{p-2}p^{p-2} + a_{p-3}p^{p-3} + \cdots + a_1 p + a_0,$$

a zbog $a_0 = (p-1)! + 1$ slijedi

$$f(p) = (p-1)! - p^{p-1} + 1 = a_{p-2}p^{p-2} + a_{p-3}p^{p-3} + \cdots + a_1 p + (p-1)! + 1.$$

Dakle,

$$p^{p-1} + a_{p-2}p^{p-2} + a_{p-3}p^{p-3} + \cdots + a_1 p = 0.$$

Dijeljenjem jednakosti s p dobivamo

$$p^{p-2} + a_{p-2}p^{p-3} + a_{p-3}p^{p-4} + \cdots + a_2 p + a_1 = 0.$$

Budući da $p^2 \mid (p^{p-2} + a_{p-2}p^{p-3} + \cdots + a_3 p^2)$ i $p \mid a_2$ pa stoga $p^2 \mid a_2 p$, zaključujemo da $p^2 \mid a_1$. Također, $a_1 = f'(0)$. Deriviranjem polinoma f dobivamo

$$f'(x) = \Big((x-1)(x-2)\cdots(x-p+1) - (x^{p-1}-1)\Big)' = \Big((x-1)(x-2)\cdots(x-p+1)\Big)' - (x^{p-1}-1)'.$$

Logaritmiranjem izraza $(x-1)(x-2)\cdots(x-p+1)$ slijedi

$$\ln (x-1)(x-2)\cdots(x-p+1) = \ln(x-1) + \cdots + \ln(x-p+1),$$

a zatim deriviranjem dobivamo

$$\frac{\Big((x-1)(x-2)\cdots(x-p+1)\Big)'}{(x-1)(x-2)\cdots(x-p+1)} = \frac{1}{x-1} + \frac{1}{x-2} + \cdots + \frac{1}{x-p+1} = \sum_{k=1}^{p-1} \frac{1}{x-k}.$$

Dakle,

$$f'(x) = (x-1)(x-2)\cdots(x-p+1)\sum_{k=1}^{p-1}\frac{1}{x-k} - (p-1)x^{p-2}.$$

Uvrštavanjem $x = 0$ slijedi

$$a_1 = f'(0) = (-1)^{p-1}(p-1)!\sum_{k=1}^{p-1}\frac{1}{-k} = -(p-1)!\sum_{k=1}^{p-1}\frac{1}{k}.$$

Kako $p^2 \mid a_1$ i $p \nmid (p-1)!$, slijedi da $p^2 \mid \sum_{k=1}^{p-1}\frac{1}{k}$, tj.

$$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{p-1} \equiv 0 \pmod{p^2}. \tag{2.2}$$

što je upravo tvrdnja Wolstenholmeovog teorema. □

Ilustrirajmo na primjerima ovaj teorem.

Primjer 2.2.

Za $p = 5$ imamo

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} = \left(1 + \frac{1}{4}\right) + \left(\frac{1}{2} + \frac{1}{3}\right) = \frac{5}{4} + \frac{5}{6}$$
$$= 5\left(\frac{1}{4} + \frac{1}{6}\right) = 5 \cdot \frac{10}{4 \cdot 6} = 5 \cdot 5 \cdot \frac{1}{12}.$$

Kako je $(12, 5) = 1$, slijedi da 5^2 dijeli brojnik razlomka.

Za $p = 7$ imamo

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \left(1 + \frac{1}{6}\right) + \left(\frac{1}{2} + \frac{1}{5}\right) + \left(\frac{1}{3} + \frac{1}{4}\right)$$
$$= 7\left(\frac{1}{6} + \frac{1}{10} + \frac{1}{12}\right) = 7\left(\frac{120 + 72 + 60}{6 \cdot 10 \cdot 12}\right)$$
$$= 7\left(\frac{252}{6 \cdot 10 \cdot 12}\right) = 7 \cdot 7 \cdot \left(\frac{36}{6 \cdot 10 \cdot 12}\right).$$

Kako je $(6, 7) = 1, (10, 7) = 1$ i $(12, 7) = 1$, to je i $(6 \cdot 10 \cdot 12, 7) = 1$, pa slijedi da 7^2 dijeli brojnik razlomka.

Za $p = 11$ imamo

$$1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \frac{1}{9} + \frac{1}{10} = \left(1 + \frac{1}{10}\right) + \left(\frac{1}{2} + \frac{1}{9}\right) + \left(\frac{1}{3} + \frac{1}{8}\right) + \left(\frac{1}{4} + \frac{1}{7}\right) + \left(\frac{1}{5} + \frac{1}{6}\right)$$
$$= 11\left(\frac{1}{10} + \frac{1}{18} + \frac{1}{24} + \frac{1}{28} + \frac{1}{30}\right)$$
$$= 11\left(\frac{966240}{10 \cdot 18 \cdot 24 \cdot 28 \cdot 30}\right)$$
$$= 11 \cdot 11 \cdot \left(\frac{87840}{10 \cdot 18 \cdot 24 \cdot 28 \cdot 30}\right).$$

Kako je $(11, 10) = 1, (11, 18) = 1, (11, 24) = 1, (11, 28) = 1$ i $(11, 30) = 1$, to je i $(10 \cdot 18 \cdot 24 \cdot 28 \cdot 30, 11) = 1$, pa slijedi da 11^2 dijeli brojnik razlomka.

Koristeći polinom f definiran u dokazu Wolstenholmeovog teorema možemo dokazati sljedeću tvrdnju.

Teorem 2.3. *Neka je $p \geq 5$ prost broj. Tada vrijedi*

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}. \tag{2.3}$$

Dokaz. Neka je $p \geq 5$ prost i f polinom definiran sa

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - (x^{p-1}-1).$$

Uvrštavanjem $x = 2p$ u polinom f dobivamo

$$f(2p) = (2p-1)(2p-2)\cdots(2p-(p-1)) - \left((2p)^{p-1}-1\right) = a_{p-2}(2p)^{p-2} + \ldots + a_1(2p) + a_0.$$

Budući da je $a_0 = (p-1)! + 1$ imamo

$$\frac{(2p-1)!}{p!} - (2p)^{p-1} + 1 = a_{p-2}(2p)^{p-2} + \cdots + a_1(2p) + (p-1)! + 1,$$

pa je

$$\frac{(2p-1)!}{p!} = (2p)^{p-1} + a_{p-2}(2p)^{p-2} + \cdots + a_1(2p) + (p-1)!.$$

Po definiciji binomnog koeficijenta, izraz $\frac{(2p-1)!}{p!}$ možemo zapisati kao

$$\binom{2p-1}{p-1}(p-1)!,$$

te vrijedi

$$\binom{2p-1}{p-1}(p-1)! = (2p)^{p-1} + a_{p-2}(2p)^{p-2} + \cdots + a_2(2p)^2 + a_1(2p) + (p-1)!.$$

Pokazali smo da $p \mid a_2$ i $p^2 \mid a_1$ pa stoga $p^3 \mid a_2(2p)^2$ i $p^3 \mid a_1(2p)$. Budući da $p^3 \mid (2p)^{p-1} + a_{p-2}(2p)^{p-2} + \cdots + a_3(2p)^3$, slijedi

$$\binom{2p-1}{p-1}(p-1)! \equiv (p-1)! \pmod{p^3}.$$

Zbog $p \nmid (p-1)!$ zaključujemo da vrijedi

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}. \qquad \square$$

Kongruencija (2.3) obično se također naziva Wolstenholmeov teorem. Pokažimo da (2.3) možemo zapisati

$$\binom{2p}{p} \equiv 2 \pmod{p^3}.$$

Po definiciji binomnog koeficijenta vrijedi

$$\binom{2p}{p} = \frac{2p!}{p!p!} = \frac{2p}{p} \cdot \frac{(2p-1)!}{(p-1)!p!} = 2\binom{2p-1}{p-1}.$$

Iz prehodne jednakosti i (2.3) slijedi

$$\binom{2p}{p} \equiv 2 \pmod{p^3}. \tag{2.4}$$

Primijetimo da jednakosti (2.3) i (2.4), ali samo modulo p, možemo dobiti iz Lucasovog teorema 1.20.

Poglavlje 3

Generalizacije Wolstenholmeovog teorema

Wolstenholmeov rezultat utjecao je na pojavu brojnih generalizacija i varijacija. U ovom poglavlju ćemo razraditi varijaciju Wolstenholmeovog teorema koju je dao E. Alkan, a zatim i generalizaciju Wolstenholmeovog teorema koju je izložio M. Bayat.

3.1 Varijacije Wolstenholmeovog teorema

Matematičar E. Alkan dao je 1994. nekoliko varijacija Wolstenholmeovog teorema za kongruenciju modulo p koje su navedene u članku [1]. U ovom potpoglavlju iskazat ćemo i dokazati Alkanove varijacije navedenog teorema.

Teorem 3.1. *Ako je $p \geq 5$ prost broj, brojnik razlomka*

$$\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + \cdots + \frac{1}{(\frac{p-1}{2})(\frac{p+1}{2})}$$

je djeljiv sa p.

Dokaz. Neka je $p \geq 3$ prost broj. Imamo

$$\begin{aligned}
\frac{1}{1} + \frac{1}{p-1} &= \frac{p-1+1}{1(p-1)} = p \cdot \frac{1}{1(p-1)} \\
\frac{1}{2} + \frac{1}{p-2} &= \frac{p-2+2}{2(p-2)} = p \cdot \frac{1}{2(p-2)} \\
&\vdots \\
\frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p+1}{2}} &= \frac{\frac{p+1}{2} + \frac{p-1}{2}}{(\frac{p-1}{2})(\frac{p+1}{2})} = p \cdot \frac{1}{(\frac{p-1}{2})(\frac{p+1}{2})}.
\end{aligned}$$

Zato je

$$p\Big(\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+\cdots+\frac{1}{(\frac{p-1}{2})(\frac{p+1}{2})}\Big)=\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{p-2}+\frac{1}{p-1},$$

pa iz Wolsteholmeovog teorema direktno slijedi tražena tvrdnja. □

Teorem 3.2. *Neka je $p \geq 5$ prost broj. Brojnici racionalnih brojeva*

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(p-1)^2} \quad i \quad \frac{1}{1^2}+\frac{1}{2^2}+\cdots+\frac{1}{(\frac{p-1}{2})^2}$$

su djeljivi sa p.

Dokaz. Za $k \in \{1, 2, \ldots, p-1\}$ vrijedi

$$\begin{aligned} k(p-k) &\equiv -k^2 \pmod{p} \\ \frac{1}{k^2} &\equiv \frac{-1}{k(p-k)} \pmod{p}, \end{aligned}$$

odnosno

$$\begin{aligned} \frac{1}{1^2} &\equiv \frac{-1}{1(p-1)} \pmod{p} \\ \frac{1}{2^2} &\equiv \frac{-1}{2(p-2)} \pmod{p} \\ &\vdots \\ \frac{1}{\left(\frac{p-1}{2}\right)^2} &\equiv \frac{-1}{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)} \pmod{p} \\ \frac{1}{\left(\frac{p+1}{2}\right)^2} &\equiv \frac{-1}{\left(\frac{p+1}{2}\right)\left(\frac{p-1}{2}\right)} \pmod{p} \\ &\vdots \\ \frac{1}{(p-1)^2} &\equiv \frac{-1}{(p-1)\cdot 1} \pmod{p} \end{aligned}$$

Stoga je

$$1+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(p-1)^2} \equiv -2\Big(\frac{1}{1(p-1)}+\frac{1}{2(p-2)}+\cdots+\frac{1}{(\frac{p-1}{2})(\frac{p+1}{2})}\Big) \pmod{p}.$$

Prva tvrdnja teorema sada slijedi iz Teorema 3.1.

Gledamo li nazivnike u izrazu

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2}$$

modulo p, vidimo da se svaki kvadratni ostatak pojavljuje točno dva puta jer je $k^2 \equiv (p-k)^2 \pmod{p}$. Zato je

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(p-1)^2} \equiv 2\Big(\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(\frac{p-1}{2})^2}\Big) \pmod{p},$$

pa slijedi i druga tvrdnja teorema. □

Sada lako dobivamo sljedeći rezultat.

Teorem 3.3. *Neka je $p \geq 5$ prost broj i neka su $a_1, a_2, \ldots, a_{\frac{p-1}{2}}$ različiti kvadratni ostaci modulo p koji su uzeti iz nekog reduciranog sustava ostataka modulo p. Tada je brojnik od*

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{\frac{p-1}{2}}}$$

djeljiv s p.

Dokaz. Iz $x \equiv y \pmod{p}$ slijedi $x^2 \equiv y^2 \pmod{p}$ te stoga $\frac{1}{x^2} \equiv \frac{1}{y^2} \pmod{p}$ ako je $nzd(x, p) = nzd(y, p) = 1$. Zato je dovoljno dokazati teorem za kvadratne ostatke generirane iz jednog reduciranog sustava ostataka modulo p, pa uzmimo upravo $\{-\frac{p-1}{2}, \ldots, -1, 1, \ldots, \frac{p-1}{2}\}$ te dobivamo da su kvadratni ostaci upravo $1^2, 2^2, \ldots, (\frac{p-1}{2})^2$. Sada tvrdnja slijedi iz Teorema 3.2. □

Teorem 3.4. *Neka je $p \geq 5$ prost broj i neka su $b_1, b_2, \ldots, b_{\frac{p-1}{2}}$ različiti kvadratni neostaci modulo p koji su uzeti iz nekog reduciranog sustava ostataka modulo p. Tada je brojnik od*

$$\frac{1}{b_1} + \frac{1}{b_2} + \cdots + \frac{1}{b_{\frac{p-1}{2}}}$$

djeljiv s p.

Dokaz. Reducirani sustav ostataka modulo p može se zapisati kao disjunktna unija skupa kvadratnih ostataka $\{a_1, a_2, \ldots, a_{\frac{p-1}{2}}\}$ i skupa kvadratnih neostataka $\{b_1, b_2, \ldots, b_{\frac{p-1}{2}}\}$. Iz Teorema 3.3 je

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{\frac{p-1}{2}}} \equiv 0 \pmod{p},$$

dok je iz Wolstenholmeovog teorema

$$\frac{1}{a_1} + \frac{1}{a_2} + \cdots + \frac{1}{a_{\frac{p-1}{2}}} + \frac{1}{b_1} + \frac{1}{b_2} + \cdots + \frac{1}{b_{\frac{p-1}{2}}} \equiv 0 \pmod{p}.$$

Oduzimanjem tih izraza slijedi tvrdnja teorema. □

Pokažimo da vrijedi i sljedeća tvrdnja.

Teorem 3.5. *Neka je m prirodan broj, a p neparan prost djelitelj od m. Ako su* $t_1, t_2, \ldots, t_{\varphi(m)}$ *prirodni brojevi manji od m i relativno prosti s m, tada je brojnik od*

$$\frac{1}{t_1} + \frac{1}{t_2} + \cdots + \frac{1}{t_{\varphi(m)}}$$

djeljiv s p.

Dokaz. Neka je m prirodan broj, a p neparan prost djelitelj od m. Neka je $1 \leq t < m$ takav da je $nzd(t, m) = 1$. Tada je $1 \leq m - t < m$ i $nzd(m - t, m) = 1$. Imamo

$$\frac{1}{t} + \frac{1}{m-t} = \frac{m-t+t}{t(m-t)} = \frac{m}{t(m-t)}.$$

Kako $p \mid m$ i $p \nmid t(m-t)$, rasporedimo li brojeve $t_1, t_2, \ldots, t_{\varphi(m)}$ u ovakve parove dobivamo tvrdnju teorema. □

Primijetimo da koristeći ideju Teorema 3.2 možemo dati alternativni dokaz Wolstenholmeovog teorema.

Dokaz. Članove sume

$$\frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$$

grupiramo u parove

$$\left(\frac{1}{1} + \frac{1}{p-1}\right) + \left(\frac{1}{2} + \frac{1}{p-2}\right) + \cdots + \left(\frac{1}{\frac{p-1}{2}} + \frac{1}{\frac{p+1}{2}}\right),$$

pa dobivamo

$$p\left(\frac{1}{1(p-1)} + \frac{1}{2(p-2)} + \cdots + \frac{1}{\left(\frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)}\right).$$

Preostaje pokazati da je izraz u zagradi djeljiv s p. Zbog $\frac{1}{k(p-k)} \equiv -\frac{1}{k^2}$, to je ekvivalentno tvrdnji da je

$$\frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{\left(\frac{p-1}{2}\right)^2} \equiv 0 \pmod{p}.$$

Gledamo li u grupi $(\mathbb{Z}/p\mathbb{Z})^*$ reduciranog sustava ostataka modulo p pridruživanje $i \mapsto \frac{1}{i}$, lako je provjeriti da je to bijekcija skupa kvadratnih ostataka u samog sebe. Naime, kvadratni ostatak se preslikava u kvadratni ostatak, a surjektivnost i injektivnost se trivijalno

pokazuju. Stoga je

$$\frac{1}{1^2}+\frac{1}{2^2}+\frac{1}{3^2}+\cdots+\frac{1}{(\frac{p-1}{2})^2} \equiv 1^2+2^2+\cdots+\Big(\frac{p-1}{2}\Big)^2$$
$$\equiv \frac{\left(\frac{p-1}{2}\right)\left(\frac{p-1}{2}+1\right)\left(2\cdot\frac{p-1}{2}+1\right)}{6} \equiv 0 \pmod{p}$$

za prost $p \geq 5$ pri čemu smo iskoristili formulu za sumu prvih $n = \frac{p-1}{2}$ kvadrata prirodnih brojeva. □

3.2 Generalizacija Wolstenholmeovog teorema

U ovom potpoglavlju ćemo dokazati generalizaciju Wolstenholmeovog teorema koju je dao I.M. Gessel [8] , ispravljajući pogreške iz članka M. Bayata [3].

Teorem 3.6. *Neka je p prost broj i neka je k prirodan broj takav da je $k < p-2$. Tada je brojnik od*

$$\sum_{\substack{1\leq i<p^n\\(i,p)=1}} \frac{1}{i^k}$$

djeljiv sa p^n ako je k paran i sa p^{n+1} ako je k neparan broj.

Neka su m i k prirodni brojevi i neka je

$$S(m,k) = \sum_{i\in R_m} \frac{1}{i^k},$$

gdje je R_m skup cijelih brojeva iz $\{1,2,\ldots,m-1\}$ koji su relativno prosti sa m.

Prvo ćemo dokazati dvije leme. Kao i prije, za racionalne brojeve u i v, $u \equiv v \pmod{m}$ znači da je brojnik skraćenog razlomka za $u-v$ djeljiv s m.

Lema 3.7. *Ako je a cijeli broj relativno prost s m, onda je $(a^k-1)\,S(m,k) \equiv 0 \pmod{m}$.*

Dokaz. Skup R_m je reducirani sustav ostataka modulo m, pa je prema Teoremu 1.11 skup $\{ai : i \in R_m\}$ također reducirani sustav ostataka modulo m. Tada je

$$S(m,k) \equiv \sum_{i\in R_m} \frac{1}{(ai)^k} = \frac{1}{a^k} S(m,k) \pmod{m}.$$

Dakle,

$$a^k S(m,k) \equiv S(m,k) \pmod{m},$$

tj. vrijedi tvrdnja leme. □

Lema 3.8. *Ako je k neparan broj, onda je* $2S(m,k) \equiv -mkS(m,k+1) \pmod{m^2}$.

Dokaz. Imamo

$$2S(m,k) = \sum_{i \in R_m} \left(\frac{1}{i^k} + \frac{1}{(m-i)^k} \right) = \sum_{i \in R_m} \frac{i^k + (m-i)^k}{i^k (m-i)^k}.$$

Za k neparan, primjenom binomnog teorema 1.19 dobivamo

$$i^k + (m-i)^k \equiv i^k + m^k - \binom{k}{1} m^{k-1} i + \cdots + \binom{k}{k-1} m i^{k-1} - i^k \equiv k i^{k-1} m \pmod{m^2}.$$

Također,

$$(m-i)^k \equiv -i^k \pmod{m}.$$

Stoga je

$$2S(m,k) \equiv \sum_{i \in R_m} \frac{k i^{k-1} m}{i^k (-i^k)} \equiv -km \sum_{i \in R_m} \frac{1}{i^{k+1}} \pmod{m^2}. \qquad \square$$

Teorem 3.9. *Neka je k prirodan broj koji nije djeljiv sa $p-1$ niti za jedan prost broj p koji dijeli m. Tada je $S(m,k) \equiv 0 \pmod{m}$.*

Dokaz. Neka je p prost broj koji dijeli m. Kako $p-1$ ne dijeli k, postoji cijeli broj a_p takav da $a_p^k - 1 \not\equiv 0 \pmod{p}$.

Pretpostavimo suprotno te neka je K ostatak pri dijeljenju k sa $p-1$. Tada je zbog malog Fermatovog teorema $x^k \equiv x^K \pmod{p}$ za svaki $x \in \{1, \ldots, p-1\}$, pa bi polinom $x^K - 1$ koji je stupnja strogo manjeg od $p-1$, imao $p-1$ nultočaka modulo p što je u suprotnosti sa Lagrangeovim teoremom 1.15. Koristeći Kineski teorem o ostatcima, dobivamo cijeli broj a takav da je $a \equiv a_p \pmod{p}$ za svaki prost broj p koji dijeli m. Iz Leme 3.7 sada slijedi da je

$$S(m,k) \equiv 0 \pmod{m}. \qquad \square$$

Teorem 3.10. *Neka je k neparan prirodan broj takav da za svaki prosti broj p koji dijeli m imamo $(p-1) \nmid (k+1)$. Tada je $S(m,k) \equiv 0 \pmod{m^2}$.*

Dokaz. Po Teoremu 3.9 je $S(m,k+1) \equiv 0 \pmod{m}$. Prema Lemi 3.8 je

$$2S(m,k) \equiv -mkS(m,k+1) \equiv 0 \pmod{m^2}.$$

Budući da $(2-1) \mid (k+1)$ iz uvjeta teorema dobivamo $2 \nmid m$, pa konačno vrijedi

$$S(m,k) \equiv 0 \pmod{m^2}. \qquad \square$$

Dokaz Teorema 3.6. Ako je $k \leq p-2$ paran, uvrstimo $m = p^n$ u Teorem 3.9. Ako je $k < p-2$ neparan, uvrstimo $m = p^n$ u Teorem 3.10. $\square$

Za $n = 1$ dobivamo iz Teorema 3.6 sljedeći rezultat M. Bayata iz članka [3].

Korolar 3.11. *Neka je p prost broj i neka je k prirodan broj takav da je $2k < p - 1$. Tada je brojnik od*

$$1 + \frac{1}{2^{2k-1}} + \cdots + \frac{1}{(p-1)^{2k-1}}$$

djeljiv sa p^2, a brojnik od

$$1 + \frac{1}{2^{2k}} + \cdots + \frac{1}{(p-1)^{2k}}$$

je djeljiv sa p.

Vidimo da za $k = 1$ prva tvrdnja prethodnog korolara daje upravo Wolstenholmeov teorem.

Iz Teorema 3.10 slijedi odmah i idući Leudesdorfov rezultat.

Korolar 3.12. *Ako je m prirodan broj relativno prost sa 6, onda je*

$$\sum_{\substack{1 \le i < m \\ (i,m)=1}} \frac{1}{i} \equiv 0 \pmod{m^2}.$$

Poglavlje 4

Obrat Wolstenholmeovog teorema

Kako je navedeno u članku [14], J.P. Jones prvi je pretpostavio kako vrijedi obrat Wolstenholmeovog teorema, tj. da prirodan broj p koji zadovoljava kongruenciju $\binom{2p-1}{p-1} \equiv 1 \pmod{p^3}$ nužno mora biti prost. Ta slutnja do danas nije dokazana i smatra se težim problemom u teoriji brojeva. V. Trevisan i K. Weber su 2001. u radu [14] dali djelomične rezultate pokazavši da slutnja vrijedi u određenim beskonačnim skupovima prirodnih brojeva.

Najprije ćemo dokazati neke pomoćne rezultate vezane uz binomne koeficijente.

Lema 4.1. *Neka je n prirodan broj. Tada vrijedi*

$$\binom{2n}{n} = \sum_{j=0}^{n} \binom{n}{j}^2.$$

Dokaz. Raspisom identiteta

$$(1+x)^n(1+x)^n = (1+x)^{2n}$$

dobivamo

$$\left(\sum_{j=0}^{n}\binom{n}{j}x^j\right)\left(\sum_{j=0}^{n}\binom{n}{j}x^j\right) = \sum_{j=0}^{2n}\binom{2n}{j}x^j.$$

Polinomi s lijeve i desne strane se podudaraju pa su koeficijenti uz x^n jednaki. Imamo

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n}\binom{n}{0} = \binom{2n}{n}.$$

Primijenimo li svojstvo simetrije binomnih koeficijenata $\binom{n}{m} = \binom{n}{n-m}$, dobivamo

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}.$$

Dakle,

$$\binom{2n}{n} = \sum_{j=0}^{n} \binom{n}{j}^2. \qquad \square$$

Također, za prirodne brojeve r i s vrijedi jednakost

$$\binom{r}{s} = \frac{r}{s}\binom{r-1}{s-1}. \tag{4.1}$$

To vidimo iz definicije binomnog koeficijenta

$$\binom{r}{s} = \frac{r(r-1)\cdots(r-s+1)}{1\cdot 2\cdots(s-1)s} = \frac{r}{s}\binom{r-1}{s-1}.$$

Koristeći (4.1) i Lemu 4.1 možemo pisati

$$\binom{2n-1}{n-1} = \frac{1}{2}\binom{2n}{n} = \frac{1}{2}\sum_{j=0}^{n}\binom{n}{j}^2. \tag{4.2}$$

Lema 4.2. *Neka je p prost broj. Ako je $n = p^r$ i p^s najveća potencija od p koja dijeli m ($s \leq r$), tada je p^{r-s} najveća potencija od p koja dijeli $\binom{n}{m}$.*

Dokaz. Lako je vidjeti da je najveća potencija prostog broja p koja dijeli $k!$ za prirodan broj k upravo k^t, gdje je

$$t = \left\lfloor \frac{k}{p} \right\rfloor + \left\lfloor \frac{k}{p^2} \right\rfloor + \left\lfloor \frac{k}{p^3} \right\rfloor + \cdots$$

Ovdje smo sa $\lfloor\cdot\rfloor$ označili funkciju najveće cijelo ili pod. Zato je eksponent najveće potencije od p koja dijeli $\binom{n}{m}$ iz izraza leme jednak

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots - \left(\left\lfloor \frac{m}{p} \right\rfloor + \left\lfloor \frac{m}{p^2} \right\rfloor + \left\lfloor \frac{m}{p^3} \right\rfloor + \cdots \right) - \left(\left\lfloor \frac{n-m}{p} \right\rfloor + \left\lfloor \frac{n-m}{p^2} \right\rfloor + \left\lfloor \frac{n-m}{p^3} \right\rfloor + \cdots \right)$$

$$= \left(- \left\lfloor \frac{-m}{p} \right\rfloor - \left\lfloor \frac{m}{p} \right\rfloor \right) + \left(- \left\lfloor \frac{-m}{p^2} \right\rfloor - \left\lfloor \frac{m}{p^2} \right\rfloor \right) + \cdots + \left(- \left\lfloor \frac{-m}{p^s} \right\rfloor - \left\lfloor \frac{m}{p^s} \right\rfloor \right).$$

Lako je provjeriti da za prirodan broj $t \in \{1, \ldots, s\}$ vrijedi

$$- \left\lfloor \frac{-m}{p^t} \right\rfloor - \left\lfloor \frac{m}{p^t} \right\rfloor = \begin{cases} 0 & , \text{ako } p^t \mid m \\ 1 & , \text{ako } p^t \nmid m. \end{cases}$$

Odavde direktno slijedi tvrdnja leme. $\square$

Da bismo za složeni broj n pokazali kako vrijedi $\binom{2n-1}{n-1} \not\equiv 1 \pmod{n^3}$, dovoljno je pokazati da $\binom{2n-1}{n-1} \not\equiv 1 \pmod{R}$, gdje je $R > 1$ bilo koji djelitelj od n. Koristeći ovu ideju, provjerit ćemo vrijedi li obrat Wolstenholmeovog teorema za potencije prostih brojeva tako da odredimo vrijednost binomnih koeficijenata modulo p^3, p^4 i p^5.

Teorem 4.3. *Ako je n paran prirodan broj, tada*

$$\binom{2n-1}{n-1} \not\equiv 1 \pmod{n^3}. \tag{4.3}$$

Drugim riječima, obrat Wolstenholmeovog teorema vrijedi za parne brojeve.

Da bismo dokazali teorem, pokažimo prvo sljedeću tvrdnju.

Lema 4.4. *Binomni koeficijent $\binom{2n-1}{n-1}$ je neparan ako i samo ako je n potencija broja 2.*

Dokaz. Primijenit ćemo Lucasov teorem za brojeve $2n-1$ i $n-1$ prikazane u bazi 2. Ako je

$$n - 1 = a_k 2^k + \cdots + a_1 \cdot 2 + a_0,$$

binarni zapis od $n-1$, onda je

$$2n - 1 = 2(n-1) + 1 = a_k 2^{k+1} + \cdots + a_1 \cdot 2^2 + a_0 \cdot 2 + 1$$

binarni zapis od 2n-1, pa iz Lucasovog teorema 1.20 dobivamo

$$\binom{2n-1}{n-1} \equiv \binom{a_k}{0}\binom{a_{k-1}}{a_k} \cdots \binom{a_0}{a_1}\binom{1}{a_0} \pmod{2}.$$

Vidimo da je $\binom{2n-1}{n-1}$ neparan ako i samo ako se ne pojavljuje u gornjem umnošku faktor oblika $\binom{0}{1}$, tj. ako je $(a_i, a_{i-1}) \neq (1,0)$ za svaki $i \in \{1, \ldots, k\}$. Budući da je $a_k = 1$, to je ekvivalentno sa $a_k = a_{k-1} = \ldots = a_1 = a_0 = 1$, odnosno

$$n - 1 = 2^k + \cdots + 2 + 1 = 2^{k+1} - 1$$

iz čega slijedi tvrdnja leme. □

Prema Teoremu 1.2 postoje jedinstveni cijeli brojevi q i r takvi da

$$\binom{2n-1}{n-1} = qn^3 + r \tag{4.4}$$

gdje je $0 \leq r < n^3$ ostatak, to jest

$$r \equiv \binom{2n-1}{n-1} \pmod{n^3}.$$

Za paran broj n koji nije potencija broja 2, primjenom Leme 4.4 vidimo da je lijeva strana jednakosti (4.4) također parna pa slijedi da i r mora biti paran broj. Tada vrijedi obrat Wolstenholmeovog teorema. Još nam preostaje dokazati slučaj kad je n potencija broja 2.

Lema 4.5. *Ako je $n = 2^l, l \geq 1$, tada je*

$$\binom{2n-1}{n-1} \equiv 3 \pmod{2^4}.$$

Dokaz. Neka je $l \geq 2$. Primjenom jednakosti (4.2) imamo

$$\begin{aligned}\binom{2n-1}{n-1} &= \frac{1}{2}\sum_{j=0}^{n}\binom{n}{j}^2 \\ &= \frac{1}{2}\left(\binom{2^l}{0}^2 + \binom{2^l}{1}^2 + \cdots + \binom{2^l}{2^l-1}^2 + \binom{2^l}{2^l}^2\right) \\ &= \frac{1}{2}\left(1^2 + \binom{2^l}{1}^2 + \cdots + \binom{2^l}{2^l-1}^2 + 1^2\right) \\ &= 1 + \frac{1}{2}\left(\binom{2^l}{1}^2 + \cdots + \binom{2^l}{2^l-1}^2\right).\end{aligned}$$

Iskoristimo li svojstvo simetrije binomnih koeficijenata $\binom{n}{m} = \binom{n}{n-m}$, dobivamo

$$\begin{aligned}\binom{2n-1}{n-1} &= 1 + \frac{1}{2}\left(2\cdot\left(\binom{2^l}{1}^2 + \binom{2^l}{2}^2 + \cdots + \binom{2^l}{2^{l-1}-1}^2\right) + \binom{2^l}{2^{l-1}}^2\right) \\ &= 1 + \sum_{j=1}^{2^{l-1}-1}\binom{2^l}{j}^2 + \frac{1}{2}\binom{2^l}{2^{l-1}}^2.\end{aligned}$$

Preostaje nam pokazati da je $A = \sum_{j=1}^{2^{l-1}-1}\binom{2^l}{j}^2 + \frac{1}{2}\binom{2^l}{2^{l-1}}^2 \equiv 2 \pmod{2^4}$. Primijenimo li Lemu 4.2 dobivamo da 4 dijeli $\binom{2^l}{j}$ za svaki $j \in \{1, \ldots, 2^{l-1}-1\}$ pa stoga 16 dijeli $\binom{2^l}{j}^2$ za svaki $j \in \{1, \ldots, 2^{l-1}-1\}$. Iz toga slijedi da je $A \equiv \frac{1}{2}\binom{2^l}{2^{l-1}}^2 \pmod{2^4}$. Prema Lemi 4.2 također vrijedi da je 2^1 najveća potencija broja 2 koja dijeli $\binom{2^l}{2^{l-1}}$. Tada je $\binom{2^l}{2^{l-1}} = 2k$, gdje je k neparan broj. Slijedi

$$\frac{1}{2}\binom{2^l}{2^{l-1}}^2 = \frac{1}{2}(2k)^2 = 2k^2.$$

Kako je k neparan, vrijedi $k \equiv 1 \pmod 2$ iz čega slijedi $k \equiv \pm 1 \pmod 8$ ili $k \equiv \pm 3 \pmod 8$. U oba slučaja vrijedi $k^2 \equiv 1 \pmod 8$. Zato je

$$\frac{1}{2}\binom{2^l}{2^{l-1}}^2 = 2k^2 \equiv 2 \pmod{2^4},$$

to jest

$$A \equiv 2 \pmod{2^4},$$

čime smo dokazali tvrdnju leme. □

Sada ćemo dokazati da obrat Wolstenholmeovog teorema vrijedi za potencije prostih brojeva $p^l, l \geq 2$, za $p < 2.5 \cdot 10^8$ kako je napravljeno u članku [14]. Za početak ćemo pokazati da obrat navedenog teorema vrijedi za potencije broja 3 .

Teorem 4.6. *Ako je $n = 3^l, l \geq 1$, onda vrijedi obrat Wolstenholmeovog teorema.*

Dokaz. Neka je $n = 3^l, l \geq 1$. Želimo pokazati da je

$$\binom{2n-1}{n-1} \equiv 10 \pmod{3^3}.$$

Za $l = 1$ tvrdnja očito vrijedi. Za $l \geq 2$ primjenom jednakosti (4.2) imamo

$$\begin{aligned}
\binom{2n-1}{n-1} &= \frac{1}{2}\sum_{j=0}^{n}\binom{n}{j}^2 \\
&= \frac{1}{2}\left(\binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n-1}^2 + \binom{n}{n}^2\right) \\
&= \frac{1}{2}\left(2 + 2\cdot\sum_{j=1}^{\frac{n-1}{2}}\binom{n}{j}^2\right) \\
&= 1 + \sum_{j=1}^{\frac{n-1}{2}}\binom{n}{j}^2.
\end{aligned}$$

Primijenimo li Lemu 4.2 dobivamo da $3^2 = 9$ dijeli $\binom{3^l}{j}$ za svaki $j \in \{1, \ldots, 3^{l-1} - 1, 3^{l-1} + 1, \ldots, \frac{3^l-1}{2}\}$ pa stoga 3^4 dijeli $\binom{3^l}{j}^2$ za svaki j iz tog skupa. Za $j = 3^{l-1}$ dobivamo da je 3^1 najveća potencija koja dijeli $\binom{3^l}{j}$. Stoga je

$$\sum_{j=1}^{\frac{n-1}{2}}\binom{n}{j}^2 \equiv \binom{3^l}{3^{l-1}}^2 \pmod{3^4}.$$

Kako 3 točno dijeli $\binom{3^l}{3^{l-1}}$, vrijedi $\binom{3^l}{3^{l-1}} = 3k$, pri čemu je $(3, k) = 1$. Zato je $k \equiv \pm 1 \pmod 3$ iz čega slijedi $k^2 \equiv 1 \pmod 3$. Množenjem kongruencije sa 9 dobivamo $9k^2 \equiv 9 \pmod{3^3}$. Imamo

$$\sum_{j=1}^{\frac{n-1}{2}}\binom{n}{j}^2 \equiv \binom{3^l}{3^{l-1}}^2 \equiv (3k)^2 \equiv 9 \pmod{3^3}.$$

Dakle,

$$\binom{2n-1}{n-1} \equiv 1 + 9 \equiv 10 \pmod{3^3},$$

pa vrijedi tvrdnja teorema. □

Pokazali smo kako je $\binom{2n-1}{n-1} \not\equiv 1 \pmod{2^4}$ za $n = 2^l$ i $\binom{2n-1}{n-1} \not\equiv 1 \pmod{3^3}$ za $n = 3^l$. Stoga zaključujemo kako obrat Wolstenholmeovog teorema vrijedi za potencije brojeva 2 i 3. Kako bismo proučili vrijedi li obrat i za $n = p^l$, za p prost broj veći od 3, navest ćemo najprije nekoliko pomoćnih tvrdnji.

Lema 4.7. *Neka su m, n i p nenegativni cijeli brojevi. Tada vrijedi*

$$\binom{(m+1)p}{n} = \sum_{j=0}^{n} \binom{mp}{n-j}\binom{p}{j}.$$

Dokaz. Raspisom identiteta

$$(1+x)^{(m+1)p} = (1+x)^{mp}(1+x)^p$$

dobivamo

$$\left(\sum_{j=0}^{(m+1)p} \binom{(m+1)p}{j} x^j\right) = \left(\sum_{j=0}^{mp} \binom{mp}{j} x^j\right)\left(\sum_{j=0}^{p} \binom{p}{j} x^j\right),$$

to jest

$$\left(\sum_{j=0}^{(m+1)p} \binom{(m+1)p}{j} x^j\right) = \left(\binom{mp}{0} + \binom{mp}{1}x + \cdots + \binom{mp}{mp}x^{mp}\right)\left(\binom{p}{0} + \binom{p}{1}x + \cdots + \binom{p}{p}x^p\right).$$

Polinomi s lijeve i desne strane se podudaraju pa su koeficijenti uz x^n jednaki. Imamo

$$\binom{(m+1)p}{n} = \sum_{j=0}^{n} \binom{mp}{n-j}\binom{p}{j}.$$ □

Lema 4.8. *Neka je n nenegativan cijeli broj i $p \geq 5$ prost broj. Tada vrijedi*

$$\binom{np}{p} \equiv n \pmod{p^3}.$$

Dokaz. Dokaz ćemo provesti matematičkom indukcijom po n.

Za $n = 1$ imamo

$$\binom{p}{p} = 1 \equiv 1 \pmod{p^3},$$

pa tvrdnja očito vrijedi. Za $n = 2$ tvrdnja vrijedi prema (2.4).

Pretpostavimo da tvrdnja $\binom{mp}{p} \equiv m \pmod{p^3}$ vrijedi za $m = 1, 2, \ldots, n+1$, gdje je $n \geq 1$. Trebamo provjeriti vrijedi li tvrdnja i za $m = n + 2$. Primjenom Leme 4.7 imamo

$$\begin{aligned}\binom{(n+2)p}{p} &= \binom{((n+1)+1)p}{p} \\ &= \sum_{i=0}^{p} \binom{(n+1)p}{p-i}\binom{p}{i} \\ &= \binom{(n+1)p}{p} + \sum_{i=1}^{p-1} \binom{(n+1)p}{p-i}\binom{p}{i} + 1.\end{aligned}$$

Po pretpostavci indukcije i Lemi 4.7 vrijedi

$$\binom{(n+1)p}{p} + \sum_{i=1}^{p-1} \binom{(n+1)p}{p-i}\binom{p}{i} + 1 \equiv n + 1 + \sum_{i=1}^{p-1} \left(\binom{p}{i} \sum_{j=0}^{p-i} \binom{np}{p-i-j}\binom{p}{j}\right) + 1 \pmod{p^3}.$$

Preostaje pokazati

$$\sum_{i=1}^{p-1} \left(\binom{p}{i} \sum_{j=0}^{p-i} \binom{np}{p-i-j}\binom{p}{j}\right) \equiv 0 \pmod{p^3}.$$

Iz lijeve strane kongruencije izdvojimo članove sume za $j = 0$ i $j = p - i$ te dobivamo

$$\sum_{i=1}^{p-1} \binom{p}{i}\binom{np}{p-i} + \sum_{i=1}^{p-1} \sum_{j=1}^{p-i-1} \binom{p}{i}\binom{np}{p-i-j}\binom{p}{j} + \sum_{i=1}^{p-i} \binom{p}{i}\binom{p}{p-i}. \tag{4.5}$$

Prema Lucasovom teoremu, svaki član srednjeg dijela prethodnog izraza je kongruentan 0 modulo p^3. To vrijedi jer je

$$\binom{np}{p-i-j} \equiv \binom{n}{0}\binom{0}{p-i-j} \equiv 0 \pmod{p}, \quad 0 < p - i - j \leq p - 1,$$

$$\binom{p}{i} \equiv \binom{p}{0}\binom{0}{i} \equiv 0 \pmod{p}, \quad 0 < i \leq p - 1,$$

$$\binom{p}{j} \equiv \binom{p}{0}\binom{0}{j} \equiv 0 \pmod{p}, \quad 0 < j \leq p - 1.$$

Ponovno primjenjujući Lemu 4.7 dobivamo

$$\sum_{i=1}^{p-1}\binom{p}{i}\binom{np}{p-i}+\sum_{i=1}^{p-1}\binom{p}{i}\binom{p}{p-i}=\sum_{i=0}^{p}\binom{p}{i}\binom{np}{p-i}-\binom{np}{p}-1+\sum_{i=0}^{p}\binom{p}{i}\binom{p}{p-i}-1-1$$
$$=\binom{(n+1)p}{p}-\binom{np}{p}+\binom{2p}{p}-3.$$

Po pretpostavci indukcije gornji izraz je kongruentan $(n+1)-n+2-3=0$ modulo p^3. Time smo pokazali da vrijedi

$$\binom{(n+2)p}{p}\equiv n+2 \pmod{p^3}.$$

Po principu matematičke indukcije zaključujemo da tvrdnja vrijedi za sve prirodne brojeve n. □

Teorem 4.9. *Neka su m i n nenegativni cijeli brojevi, a p prost broj, $p \geq 5$. Tada je*

$$\binom{mp}{np}\equiv\binom{m}{n} \pmod{p^3}.$$

Dokaz. Dokaz ćemo provesti matematičkom indukcijom po n.

Za $n = 0$ imamo

$$1 \equiv 1 \pmod{p^3},$$

pa tvrdnja očito vrijedi.

Za $n = 1$ tvrdnja vrijedi prema Lemi 4.8.

Sada fiksiramo neki $n \geq 2$ i pretpostavimo da tvrdnja vrijedi za manje n-ove. Provodimo indukciju po m. Za $m < n$ imamo $\binom{mp}{np} = 0$ i $\binom{m}{n} = 0$ iz čega slijedi $0 \equiv 0 \pmod{p^3}$ pa tvrdnja vrijedi za svaki $m < n$. Za $m = n$ tvrdnja očito vrijedi. Pretpostavimo da tvrdnja vrijedi za neki $m \geq n$. Provjerimo vrijedi li i za $m + 1$. Primjenom Leme 4.7 uz uvođenje

oznake $m = k + 1$ dobivamo

$$\begin{aligned}
\binom{(m+1)p}{np} &= \sum_{i=0}^{np} \binom{mp}{np-i}\binom{p}{i} \\
&= \sum_{i=0}^{p} \binom{mp}{np-i}\binom{p}{i} \\
&= \sum_{i=0}^{p} \binom{(k+1)p}{np-i}\binom{p}{i} \\
&= \sum_{i=0}^{p} \sum_{j=0}^{np-i} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} \\
&= \sum_{i=0}^{p} \sum_{j=0}^{p} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} \\
&= \sum_{j=0}^{p} \binom{kp}{np-j}\binom{p}{j} + \sum_{i=0}^{p-1} \sum_{j=0}^{p} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} + \sum_{j=0}^{p} \binom{kp}{(n-1)p-j}\binom{p}{j}.
\end{aligned}$$

Ponovnom primjernom Leme 4.7 dobivamo da je gornji izraz jednak

$$\binom{(k+1)p}{np} + \sum_{i=0}^{p-1} \sum_{j=0}^{p} \binom{kp}{np-i-j}\binom{p}{j}\binom{p}{i} + \binom{(k+1)p}{(n-1)p}.$$

Kao u dokazu Leme 4.8, korištenjem Lucasovog teorema pokaže se da je svaki pribrojnik u srednjem članu gornjeg izraza kongruentan 0 modulo p^3. Po pretpostavci indukcije imamo

$$\binom{(k+1)p}{np} + \binom{(k+1)p}{(n-1)p} \equiv \binom{k+1}{n} + \binom{k+1}{n-1} \pmod{p^3}.$$

Vrijedi

$$\binom{k+1}{n} + \binom{k+1}{n-1} = \binom{k+2}{n} = \binom{m+1}{n},$$

čime smo pokazali da tvrdnja vrijedi za $m + 1$. Dakle,

$$\binom{(m+1)p}{np} \equiv \binom{m+1}{n} \pmod{p^3}.$$

Po principu matematičke indukcije tvrdnja teorema vrijedi za sve prirodne brojeve m i n. □

Sljedeća lema generalizira prethodni rezultat.

Lema 4.10. *Neka je $p \geq 5$ prost broj, a i b nenegativni cijeli brojevi te k prirodan broj. Tada vrijedi*

$$\binom{p^k a}{p^k b} \equiv \binom{p^{k-1} a}{p^{k-1} b} \pmod{p^{3k}}.$$

Dokaz. Stavimo $c = a - b$ te pretpostavimo da je $c > 0$ jer je u protivnom tvrdnja očito ispunjena. Imamo

$$\binom{p^k a}{p^k b} = \frac{(p^k c + 1)(p^k c + 2) \cdots (p^k c + p^k b)}{1 \cdot 2 \cdots p^k b},$$

$$\begin{aligned}\binom{p^{k-1} a}{p^{k-1} b} &= \frac{(p^{k-1} c + 1)(p^{k-1} c + 2) \cdots (p^{k-1} c + p^{k-1} b)}{1 \cdot 2 \cdots p^{k-1} b} \\ &= \frac{(p^k c + p)(p^k c + 2p) \cdots (p^k c + p^k b)}{p \cdot 2p \cdots p^k b}.\end{aligned}$$

Označimo sa S skup svih prirodnih brojeva manjih od $p^k b$ koji nisu djeljivi sa p. Iz gornjih jednakosti vidimo da vrijedi

$$\begin{aligned}\binom{p^k a}{p^k b} &= \binom{p^{k-1} a}{p^{k-1} b} \prod_{i \in S} \left(1 + \frac{p^k c}{i}\right) \\ &\equiv \binom{p^{k-1} a}{p^{k-1} b} \left(1 + \sum_{i \in S} \frac{p^k c}{i} + \sum_{\substack{i,j \in S \\ i<j}} \frac{p^{2k} c^2}{ij}\right) \pmod{p^{3k}}.\end{aligned}$$

Iz Teorema 3.10 vidimo da je $\sum_{i \in S} \frac{1}{i} \equiv 0 \pmod{p^{2k}}$, a slično koristeći

$$\sum_{\substack{i,j \in S \\ i<j}} \frac{1}{ij} = \frac{1}{2}\left(\left(\sum_{i \in S} \frac{1}{i}\right)^2 - \sum_{i \in S} \frac{1}{i^2}\right)$$

iz Teorema 3.9 dobivamo da je

$$\sum_{\substack{i,j \in S \\ i<j}} \frac{1}{ij} \equiv 0 \pmod{p^k}.$$

Zato je

$$\binom{p^k a}{p^k b} \equiv \binom{p^{k-1} a}{p^{k-1} b} \pmod{p^{3k}}$$

što smo i htjeli dokazati. □

Za dokaz obrata Wolstenholmeovog teorema kad je $n = p^l$ za $p > 3$ prost, trebamo promatrati vrijednost binomnog koeficijenta $\binom{2n-1}{n-1}$ modulo p^m. Sljedeći rezultat pokazuje kako trebamo promatrati potencije s eksponentom $m > 3$.

Teorem 4.11. *Ako je $p \geq 5$ prost broj i $n = p^l$, $l \geq 1$, onda vrijedi*

$$\binom{2n-1}{n-1} \equiv 1 \pmod{p^3}.$$

Dokaz. Primijenimo li l puta Teorem 4.9 dobivamo

$$\binom{2n}{n} \equiv \binom{2p^l}{p^l} \equiv \binom{2p^{l-1}}{p^{l-1}} \equiv \cdots \equiv \binom{2p}{p} \equiv 2 \pmod{p^3}.$$

Iz jednakosti (4.2) slijedi

$$\binom{2n-1}{n-1} = \frac{1}{2}\binom{2n}{n} \equiv \frac{1}{2} \cdot 2 \equiv 1 \pmod{p^3}. \qquad \square$$

Sljedeći teorem dat će nam kriterij za utvrđivanje vrijedi li obrat Wolstenholmeovog teorema za određene potencije prostih brojeva.

Teorem 4.12. *Ako je $p \geq 5$ prost broj, l prirodan broj i $n = p^l$, onda je*

$$\binom{2n-1}{n-1} \equiv \binom{2p-1}{p-1} \pmod{p^4}.$$

Dokaz. Kako je p neparan, dovoljno je pokazati da vrijedi $\binom{2n}{n} \equiv \binom{2p}{p} \pmod{p^4}$. Prema Lemi 4.1 vrijedi

$$\binom{2n}{n} = \sum_{j=0}^{n} \binom{n}{j}^2 = 2 + \sum_{j=1}^{n-1} \binom{n}{j}^2 = 2 + \sum_{j=1}^{p^l-1} \binom{p^l}{j}^2.$$

Ako p^{l-1} ne dijeli j, onda prema Lemi 4.2 znamo da p^2 dijeli $\binom{p^l}{j}$. Tada p^4 dijeli $\binom{p^l}{j}^2$, odnosno $\binom{p^l}{j}^2 \equiv 0 \pmod{p^4}$. Stoga je

$$\binom{2n}{n} = 2 + \sum_{j=1}^{p-1} \binom{p^l}{jp^{l-1}}^2 \pmod{p^4}.$$

Za $l \geq 3$ i $k = 2$ primjenom Leme 4.10 imamo

$$\binom{p^l}{jp^{l-1}} \equiv \binom{p^k p^{l-2}}{p^k jp^{l-3}} \equiv \binom{p^{k-1} p^{l-2}}{p^{k-1} jp^{l-3}} \equiv \binom{p^{l-1}}{jp^{l-2}} \pmod{p^6},$$

Primijenimo li još $l-3$ puta Lemu 4.10 dobivamo

$$\binom{p^l}{jp^{l-1}} \equiv \binom{p^2}{jp} \pmod{p^6},$$

za svaki $0 < j < p$ i $l \geq 2$. Zato je

$$\binom{2n}{n} \equiv 2 + \sum_{j=1}^{p-1} \binom{p^2}{jp}^2 \pmod{p^4}.$$

Preostaje još vidjeti

$$\begin{aligned}
\binom{p^2}{jp} &= \binom{p}{j} \prod_{\substack{1 \leq i < jp \\ p \nmid i}} \frac{p^2 - i}{i} \\
&= \binom{p}{j} (-1)^{jp-j} \prod_{\substack{1 \leq i < jp \\ p \nmid i}} \left(1 - \frac{p^2}{i}\right) \\
&\equiv \binom{p}{j} (-1)^{j(p-1)} \left(1 - p^2 \sum_{\substack{1 \leq i < jp \\ p \nmid i}} \frac{1}{i}\right) \\
&\equiv \binom{p}{j} \pmod{p^4},
\end{aligned}$$

gdje smo u zadnjem koraku primijenili Teorem 3.10 uz $m = jp$ i $k = 1$ u ondje korištenim oznakama. Dakle,

$$\binom{2n}{n} \equiv 2 + \sum_{j=1}^{p-1} \binom{p}{j}^2 \equiv \binom{2p}{p} \pmod{p^4}$$

iz čega slijedi tvrdnja teorema. □

Ovaj rezultat je važan jer možemo izračunati vrijednost od $\binom{2p-1}{p-1} \pmod{p^4}$. Ako je dobivena vrijednost različita od 1, tada obrat Wolstenholmeovog teorema vrijedi za sve potencije danog prostog broja p.

Proste brojeve p za koje vrijedi

$$\binom{2p-1}{p-1} \equiv 1 \pmod{p^4}$$

zovemo Wolstenholmeovi prosti brojevi. Slutnja je da postoji beskonačno mnogo Wolstenholmeovih prostih brojeva, ali su do sada poznata samo dva: 16843 nađen 1964. godine i 2124679 nađen 1993.

Dakle, prethodni teorem kaže da ako prost broj p nije Wolstenholmeov, tada obrat Wolstenholmeovog teorema vrijedi za sve potencije od p. Trevisan i Weber provjerili su vrijednost izraza $\binom{2p-1}{p-1} \pmod{p^4}$ za sve $p < 2.5 \cdot 10^8$ i prema Teoremu 4.12 dokazali kako obrat Wolstenholmeovog teorema vrijedi za sve potencije prostih brojeva u tom intervalu osim eventualno za navedena dva Wolstenholmeova prosta broja. No, može se pokazati da Teorem 4.12 vrijedi i modulo p^5, pa je provjerom $\binom{2p-1}{p-1} \pmod{p^5}$ pokazano da i za potencije navedenih Wolstenholmeovih prostih brojeva vrijedi obrat Wolstenholmeovog teorema.

Bibliografija

[1] E. Alkan, *Variations on Wolstenholme's Theorem*, The American Mathematical Monthly, Vol. 101, No. 10 (1994.), 1001-1004.

[2] D.F. Bailey, *Two p^3 variations of Lucas' theorem*, Journal of Number Theory 35 (1990.), 208-215.

[3] M. Bayat, *A Generalization of Wolstenholme's Theorem*, The American Mathematical Monthly , Vol. 104., No. 6 (1997.), 557-560.

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

[5] A. Dujella, *Uvod u teoriju brojeva*, dostupno na
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf` (srpanj 2019.)

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

[7] I.M. Gessel, *Some Congruences for Generalized Euler Numbers*, Canadian Journal of Mathematics, Vol. 35., No. 4 (1983.), 687-709.

[8] I.M. Gessel, *Wolstenholme Revisited*, The American Mathematical Monthly, Vol. 105., No. 7 (1998.), 657-658.

[9] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Clarendon Press, Oxford 1980.

[10] S. Hussein, *A note on the converse of Wolstenholme's Theorem*, dostupno na
`https://arxiv.org/pdf/1806.05459.pdf` (kolovoz 2019.)

[11] V. Krčadinac, *Osnove algoritama*, dostupno na
`https://web.math.pmf.unizg.hr/nastava/oa/oa-skripta.pdf`

[12] R. Meštrović, *Wolstenholme's theorem: Its Generalizations and Extensions in the last hundred and fifty years (1862-2012)*, dostupno na

`https://arxiv.org/abs/1111.3057` (srpanj 2019.)

[13] J. Stevens, *Olympiad Number Theory Through Challenging Problems*, dostupno na `http://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olympiad-number-theory.pdf` (srpanj 2019.)

[14] V. Trevisan, K. Weber, *Testing the converse of Wolstenholme's theorem*, Mathematica Contemporanea 21 (2001.), 275-286.

[15] D. Veljan, *Kombinatorna i diskretna matematika*, Algoritam, Zagreb 2001.

[16] J. Wolstenholme, *On certain properties of prime numbers*, Quart. J. Pure Appl. Math. 5 (1862), 35-39., dostupno na `http://books.google.com/books?id=vL0KAAAAIAAJ&pg=PA35` (srpanj 2019.)

[17] J. J. O'Connor, E. F. Robertson, *Biography of Joseph Wolstenholme*, dostupno na `http://www-history.mcs.st-and.ac.uk/~history/Biographies/Wolstenholme.html` (srpanj 2019.)

Sažetak

Joseph Wolstenholme engleski je matematičar koji je 1862. godine dokazao da je za prost broj p veći od 3 brojnik racionalnog broja $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ djeljiv s p^2.

Ovaj diplomski rad posvećen je Wolstenholmeovom teoremu i sadrži četiri poglavlja. U prvom poglavlju izlažemo osnovne pojmove i rezultate iz teorije brojeva koji se koriste u nastavku rada. U drugom poglavlju iskazujemo i dokazujemo Wolstenholmeov teorem te navodimo tvrdnju ekvivalentnu navedenom teoremu. Treće poglavlje posvećeno je nekim generalizacijama Wolstenholmeovog teorema. Navedeno je i dokazano nekoliko varijacija, a zatim dokazana i generalizacija. U zadnjem poglavlju ovog rada pokazujemo kako obrat Wolstenholmeovog teorema vrijedi u određenim beskonačnim skupovima prirodnih brojeva.

Summary

Joseph Wolstenholme was an English mathematician who proved in 1862 that for a prime p greater than 3, the numerator of the fraction $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{p-1}$ is divisible by p^2.

This graduate thesis is devoted to the Wolstenohlme's theorem and contains four chapters. In the first chapter, we give some of the fundamental terms and results from the theory of numbers used throughout the rest of the thesis. In the second chapter we state and prove Wolstenholme's theorem and give an equivalent formulation. The third chapter gives some generalizations of Wolstenholme's theorem. Several variations are stated and proved, followed by a generalization. In the last chapter of this graduate thesis, we prove that the converse of Wolstenholme's theorem is true in certain infinite sets of natural numbers.

Životopis

Rođena sam 13.4.1994. u Zadru. Pohađala sam OŠ Jurja Barakovića u Ražancu, nakon čega sam nastavila svoje školovanje u Gimnaziji Jurja Barakovića u Zadru, smjer prirodoslovno-matematički. U srpnju 2013. godine upisala sam Prirodoslovno-matematički fakultet u Zagrebu. Godine 2017. završila sam preddiplomski studij Matematika, smjer nastavnički i iste godine upisala diplomski studij Matematika, smjer nastavnički na istom fakultetu.