»Mladi za napredek Maribora 2015«

32. srečanje

Kongruence

Matematika

Raziskovalna naloga

Avtor: MELANI POTRČ

Mentor: LILIJANA PETEK

Šola: PRVA GIMNAZIJA MARIBOR

Maribor, februar 2015

»Mladi za napredek Maribora 2015«

32. srečanje

Kongruence

Matematika

Raziskovalna naloga

Maribor, februar 2015

KAZALO

POVZETEK

V raziskovalni nalogi sem raziskovala deljivost celih števil, kjer sem si pomagala z znanjem kongruenc. V teoretičnem delu naloge sem na podlagi učbenika za prvi letnik srednje šole obnovila in poglobila svoje znanje o deljivosti celih števil. Ponovila sem pomen praštevil, sestavljenih števil, načine iskanja skupnih deliteljev in večkratnikov dveh celih števil, Evklidov algoritem, Eratostenovo sito, osnovni izrek aritmetike, osnovni izrek o deljenju, relacijo deljivosti in kriterije deljivosti. Na kratko sem se srečala tudi z zgodovinskim ozadjem deljivosti celih števil, kjer sem s pomočjo literature poiskala nekaj dejstev o slavnih matematikih, ki so se ukvarjali z deljivostjo in kongruencami. Že v teoretičnem delu sem se srečala z dopolnjevanjem matematičnih dokazov, saj so v literaturi dokazi vselej zapisani brez vseh korakov. Ta metoda dela se je izkazala za pomembno tudi v raziskovalnem delu. V raziskovalnem delu sem proučevala kongruence in njihove lastnosti. Ugotovila sem, da nam kongruence olajšajo računsko operacijo deljenje in nam hkrati omogočajo računanje z večjimi števili brez uporabe tehnologije. Proučevala sem računske operacije s kongruencami in se nazadnje srečala s pomembnimi izreki, kot so Eulerjev, Fermatov in Willsonov izrek. Ugotovila sem, da nam praštevila omogočajo več možnih poti reševanja matematičnih problemov in uporabe kongruenc kot pa sestavljena števila. V zadnjem in najpomembnejšem delu raziskovalne naloge sem teoretično znanje kongruenc preizkusila na konkretnih primerih. V literaturi sem našla naloge, ki pa niso imele zapisanega postopka reševanja, tako sem jih razmislila sama. Nazadnje sem se preizkusila še v samostojnem konstruiranju primerov, kako s kongruencami rešiti naloge o deljivosti. Pri konstruiranju sem si pomagala s teoretičnim znanjem o kongruencah, ki sem ga pridobila tekom raziskovanja. Nekaj primerov uporabe kongruenc sem natančno predstavila v raziskovalni nalogi in jih razložila svojim vrstnikom na dodatnem pouku iz matematike. Pri izdelavi raziskovalne naloge sem ugotovila, kako pomembno je teoretično znanje pri reševanju konkretnih matematičnih nalog, kar je pomembno pri samem pouku matematike. Veliko teoretičnih pojmov sem si razjasnila prav pri dopolnjevanju matematičnih dokazov, kar se je izkazalo za pomemben del moje raziskovalne naloge.

ABSTRACT

This research paper is intended to explore the divisibility of whole numbers (integers) by drawing upon my personal knowledge of congruence. In the theoretical part of the assignment, I refreshed and increased my knowledge of the divisibility of integers on the basis of a textbook for the first year of secondary school. I revised the following areas: the meaning of prime and composite numbers, ways of looking for common divisors and multiples of two integers, the Euclidean Algorithm, the Sieve of Eratosthenes, the Fundamental Theorem of Arithmetic, the Fundamental Theorem of Divisibility, relation of divisibility and divisibility criteria. I also got familiarised with the historical background of divisibility of integers in brief by using relevant literature where I found some facts about famous mathematicians who have dealt with divisibility and congruence. In the theoretical part, I already encountered the problem of complementing mathematical proofs, as the literature always provides evidence without any steps written. This working method has proven to be important for the research part of this work as well. In the research part, I studied the congruences and their properties. I found out that the congruences facilitate the operation of calculating divisibility and allowing us to calculate with larger numbers without the use of technology at the same time. I studied arithmetic operations with congruences and finally met with important theorems, such as Euler's, Fermat's and Willson's theorems. I found out that the primes provide for more possible paths for solving mathematical problems and using congruences than composite numbers. In the last and the most important part of the research paper, I examined the theoretical knowledge of congruence in specific cases. I found exercises in the literature which did not have a written procedure for solving them, so I thought of it myself. Finally, I tried to set up my own examples of how to solve the divisibility exercises by using congruences. When designing the examples, I used my theoretical knowledge of congruence that I gained during the research. Some examples showing the use of congruence were presented in the research project in detail and I explained them to my peers during the supplementary lessons in mathematics. When drawing up the research paper, I became aware of the importance of theoretical knowledge in solving specific mathematical exercises, which is very important in maths lessons. Many theoretical concepts became clear to me by complementing mathematical proofs, which proved to be an important part of my research work.

Zahvala

Iskreno se zahvaljujem svoji mentorici za vodenje, ideje in motivacijo, ki sem je bila deležna pri pripravi svoje raziskovalne naloge. Brez njene pomoči in nasvetov gotovo ne bi nastala takšna raziskovalna naloga, kot je.

Zahvaljujem se tudi profesorici angleščine, ki je strokovno pregledala moj povzetek in profesorici slovenščine, ki je moje delo lektorirala.

Posebno zahvalo pa poklanjam svoji družini, ki mi je ves čas stala ob strani in me pri mojem delu spodbujala.

1. UVOD

V svoji raziskovalni nalogi sem se ukvarjala z deljivostjo števil in kongruencami. Proučila sem njihove lastnosti in pravila, ki jih je potrebno poznati za računanje z njimi. Izpeljala sem tudi dokaze za izreke o kongruencah. Nazadnje sem pridobljeno znanje preverila še na praktičnih primerih.

1.1 NAMEN RAZISKOVALNE NALOGE

Namen moje raziskovalne naloge je bil poglobiti svoje znanje o deljivosti in ga razširiti na kongruence. Z njimi si namreč olajšamo računsko operacijo deljenje. Želela sem se seznaniti z lastnostmi kongruenc in pravili za računanje s kongruencami. Da bi le-te bolje razumela, sem večino pravil skušala tudi sama dokazati ali dokaze dopolniti. Teoretično znanje, ki sem ga dobila tekom raziskovanja, sem želela uporabiti tudi na konkretnih primerih. Tako sem preverila svoje razumevanje in tudi nekatere primere sama konstruirala.

1.2 CILJI RAZISKOVALNE NALOGE

V raziskovalni nalogi sem želela slediti predvsem naslednjim zastavljenim ciljem:

- Ali nam znanje kongruenc olajša raziskovanje deljivosti v množici celih števil?
- Ali je pri ugotavljanju deljivosti celih števil pomembno dejstvo, da je število praštevilo ali sestavljeno število?
- Ali lahko ugotavljamo deljivost velikih celih števil brez uporabe tehnologije?

1.3 HIPOTEZE RAZISKOVALNE NALOGE

V raziskovalni nalogi sem si postavila naslednje hipoteze:

- Znanje kongruenc nam olajša raziskovanje deljivosti v množici celih števil.

- Če je število praštevilo, imamo več načinov ugotavljanja deljivosti s tem številom, kot če je število sestavljeno.
- Deljivost velikih celih števil lahko ugotavljamo brez uporabe tehnologije s pomočjo teoretične podlage.

1.4 METODE DELA

Tema moje raziskovalne naloge sloni na deljivosti celih števil, kar smo pri pouku matematike obravnavali v prvem letniku srednje šole. Tako sem v svoji raziskovalni nalogi poglobila svoje znanje o deljivosti celih števil. Obnovila sem pojme, kot so praštevila in sestavljena števila, Evklidov algoritem, Eratostenovo rešeto, kriterije deljivosti, osnovni izrek aritmetike in osnovni izrek o deljenju, pri čemer sem si pomagala z učbenikom za matematiko za prvi letnik. Svoje raziskovanje sem nadaljevala s pomočjo različne literature, kjer sem spoznala pojem kongruenca, računanje s kongruencami, Eulerjev, Fermatov in Willsonov izrek. To znanje kongruenc sem povezala z znanjem o deljivosti.

Vendar pa sem kmalu naletela na težave, saj v literaturi nisem našla natančnih dokazov za izpeljavo izrekov. Nekatere podrobnosti dokazov preprosto niso bile tako natančno razložene ali pa so jih avtorji smatrali za samoumevne in so jih izpustili. Na tem je torej temeljil večji del mojega raziskovanja. Izpeljevala in dopolnjevala sem dokaze za pravila in izreke, ki jih uporabljamo pri ugotavljanju deljivosti celih števil in računanju s kongruencami.

Nazadnje sem na novo pridobljeno znanje preverila na konkretnih primerih. Nekatere primere sem rešila kot naloge iz matematičnih učbenikov, kjer sem lahko preverila rešitve. Za konec pa sem s pomočjo poznavanja teorije in izrekov poskusila konstruirati lastne primere. Na teh primerih sem torej uporabila vse tisto, kar sem se tekom raziskovanja naučila.

2. TEORETIČNI DEL

2.1 DELJIVOST CELIH ŠTEVIL

Deljenje je že od nekdaj veljalo za četrto računsko operacijo in za najzahtevnejšo od vseh. Prve prave metode deljenja so najbrž odkrili arabski matematiki, ob prelomu tisočletja pa so se razširile v Evropo. Pri deljenju si velikokrat pomagamo s kongruencami, ki nam olajšajo raziskovanje lastnosti deljenja in nam pomagajo pri deljenju večjih števil.

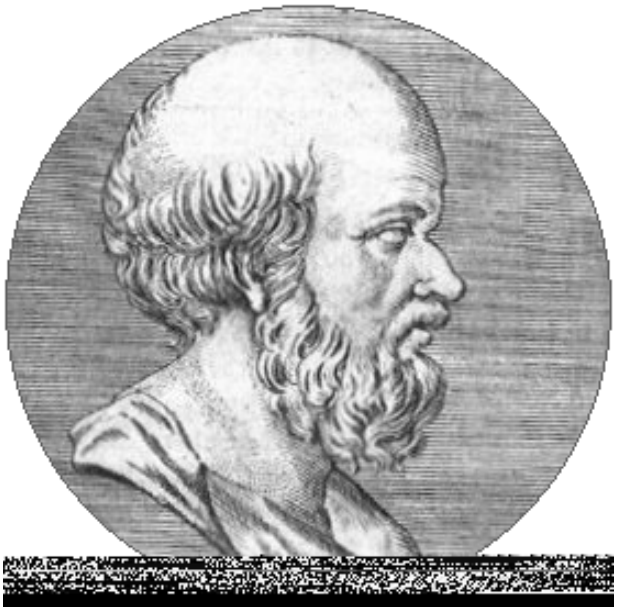
2.2 PRAŠTEVILA, SESTAVLJENA ŠTEVILA IN OSNOVNI IZREK ARITMETIKE

Praštevila so števila, ki imajo natanko dva delitelja: število 1 in samega sebe. Najmanjše praštevilo je število 2, ki je tudi edino sodo praštevilo. Praštevila je raziskoval že Evklid leta 300 pr. Kr. Prihajal je iz Aleksandrije v Egiptu, kjer so še posebej cenili matematično znanje. Njegovo najslavnejše delo so Elementi. To je bilo trinajst dolgih zvitkov papirusa, kjer je bila zbirka do tedaj najpomembnejših matematičnih rezultatov grške tradicije. Napisani so zelo sistematično, zasnovano na podlagi aksiomov, izrekov in dokazov, s čemer je Evklid opisal ravninsko geometrijo. Še veliko stoletij po njegovi smrti, so se študentje matematike zgledovali po njem in uvedli celo obred imenovan Evklidov pogreb. Izvod Evklidovega dela so preluknjali, nato pa je sledil pogrebni sprevod, molitve, nazadnje pa še sežig knjige. S tem so proslavljali zaključke svojih matematičnih študij. Tudi učenci Pitagorove filozofske šole so še posebej cenili praštevila. Danes se praštevila pogosto uporabljajo pri kriptografiji in šifriranju tajnih sporočil. Največje znano praštevilo je $2^{43112609}$ in ima 12978609 mest. (Berlinghoff, 2008, str. 25).

Slika 1: Evklid.

Z iskanjem praštevil se je ukvarjal že starogrški matematik Eratosten. Eratosten je prihajal iz Aleksandrije, kjer je vodil veliko knjižnico. Tukaj je bilo na zvitkih papirusov shranjeno skoraj vse dotedanje znanje. Prav to je pripomoglo k temu, da je postal odličen pisec in učitelj. Tako je nekega dne po naključju prebral zgodbo o mestu Siene, kjer žarek sonca posveti naravnost v vodnjak in doseže vodno gladino na dnu, ta pa se potem odbije kot ogledalo nazaj na površje. Iz tega je sklepal, da mora sonce biti v tistem trenutku natanko nad vodnjakom, to pa njegovim žarkom omogoči, da ne dajejo nobene sence. A ko je sam opravil preizkus v Aleksandriji, mu to ni uspelo. Žarki so na tla pod majhnim kotom metali kratko senco. Eratosten je ta kot izračunal in ugotovil, da znaša natančno eno petdesetino kroga, kar je $7{,}2^{\circ}$. Ta podatek mu je koristil, da je lahko izračunal velikost našega planeta. Razdaljo od Aleksandrije do Siene je pomnožil s petdeset in dobil rezultat, da je obseg zemlje 40.000 km, kar je bil za tiste čase zelo natančen izračun. Na podlagi tega je Eratosten narisal tudi nov zemljevid sveta, kjer si je pomagal z namišljenimi črtami - poldnevniki in vzporedniki. Verjel je, da so nekje na svetu še neodkrite celine in oceani. Bil je eden najboljših geografov in matematikov, vendar za časa svojega življenja ni bil cenjen. Umrl je v starosti 80-ih let, slep in obubožan. Iznašel je poseben postopek, kako najti praštevila do poljubnega, ne

prevelikega naravnega števila, ki ga po njem imenujemo Eratostenovo sito ali rešeto. (Ball, 2010, str. 29).



Slika 2: Eratosten.

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

Slika 3: Eratostenovo sito.

Najprej zapišemo vsa števila do n^2 in med njimi prečrtamo večkratnike števila dva, ki so večji od 2. Pogledamo, katero izmed števil je ostalo ne prečrtano. V našem primeru je to število 3, zato ponovno prečrtamo vse večkratnike števila 3, ki so večji od 3. Tokrat ostane prvo ne prečrtano število 5. Postopek ponovimo, vedno pa je prvo ne prečrtano število praštevilo. Postopek je sicer zamuden, vendar je zelo preprost in nam

pomaga pri iskanju novih praštevil. Za vsako sestavljeno število, ki smo ga pri postopku prečrtali, vidimo, koliko različnih praštevil se nahaja v njegovi razcepitvi. Teh je točno toliko, kolikokrat smo število prečrtali.

Sestavljena števila so števila, ki imajo več kot dva delitelja. Izjema je število 1, ki ima samo enega delitelja.

Vsako naravno število *n* lahko na en sam način zapišemo kot produkt potenc s praštevilskimi osnovami, kar imenujemo **osnovni izrek aritmetike**:

$$\boldsymbol{n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_k^{m_k}}$$
$$\boldsymbol{p_1 \ldots p_k \in P, m_1 \ldots m_k \in N}$$

2.3 KRITERIJI DELJIVOSTI

Ko se srečujemo s pojmom deljivosti, hitro nastanejo težave pri deljenju večjih števil. Če je število preveliko, si ne moremo pomagati z navadnim računalom. Do rešitve pa lahko pridemo brez večjega napora, če poznamo pravila oziroma kriterije za deljenje. Pravila so preprosta in si jih zlahka zapomnimo, zraven tega pa nam olajšajo računanje brez računala.

1) Deljivost z 2, 5, 10, 100 in 1000:

- Število je deljivo z 2, ko je zadnja števka števila deljiva z 2.
- Število je deljivo s 5, ko je zadnja števka enaka 0 ali 5.
- Število je deljivo s potenco števila 10, ko na koncu števila nastopa toliko ničel, kolikšen je eksponent potence števila 10.

Ta pravila lahko dokažemo na preprost način:

$$n = a_n \ldots a_2 a_1 a_0$$
$$n = a_0 + a_1 \cdot 10 + a_2 \cdot 10^2 + \ldots + a_n \cdot 10^n$$
$$n = a_0 + 10 \cdot \left(a_1 + a_2 \cdot 10 + \ldots + a_n \cdot 10^{n-1}\right)$$
$$n = a_0 + 2 \cdot \left(5 \cdot \left(a_1 + a_2 \cdot 10 + \ldots + a_n \cdot 10^{n-1}\right)\right)$$

2) Deljivost s številom 3 in 9:

- Število je deljivo s 3 oziroma z 9, če je vsota njegovih števk deljiva s 3 oziroma z 9.

Dokaza za kriterij deljivosti s številoma 3 in 9 sta bolj zapletena:

$$n = a_n \cdot 10^n + \ldots + a_4 \cdot 10^4 + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

$$n = a_n \cdot \left(\underbrace{99...9}_{n-krat} + 1 \right) + \ldots + a_4 \cdot (9999 + 1) + a_3 \cdot (999 + 1) + a_2 \cdot (99 + 1) + a_1 \cdot (9 + 1) + a_0$$

$$n = \underbrace{99\ldots9}_{n-krat} a_n + a_n + \ldots + 9999a_4 + a_4 + 999a_3 + a_3 + 99a_2 + a_2 + 9a_1 + a_1 + a_0$$

$$n = \left(\underbrace{99...9}_{n-krat} a_n + ... + 9999a_4 + 999a_3 + 99a_2 + 9a_1 \right) + a_n + ... + a_4 + a_3 + a_2 + a_1 + a_0$$

$$n = 9 \cdot \left(\underbrace{11\ldots1}_{n-krat} a_n + \ldots + 1111a_4 + 111a_3 + 11a_2 + a_1 \right) + a_n + \ldots + a_4 + a_3 + a_2 + a_0$$

S tem smo dokazali, da je število deljivo z 9, če je vsota njegovih števk deljiva z 9. Iz tega lahko izpeljemo tudi sklep, da je število deljivo s 3 takrat, ko je vsota njegovih števk deljiva s 3, saj je število 9 večkratnik števila 3.

3) Deljivost s številom 6:

- Naravno število je deljivo s 6, če je deljivo z 2 in s 3 hkrati, oziroma če je zadnja števka sodo število in je vsota vseh števk deljiva s 3.

4) Deljivost s številom 4 in 25:

- Število je deljivo s 4 oziroma s 25, ko je njegov dvomestni konec deljiv s 4 oziroma s 25.

Dokažemo podobno, kot deljivost z 2 in s 5.

5) Deljivost s številom 8 in 125:

- Število je deljivo z 8 oziroma s 125, ko je njegov trimestni konec deljiv z 8 oziroma s 125.

Dokažemo podobno, kot deljivost z 2 in s 5.

6) Deljivost s 7 in 11:

- Število n je deljivo s sedem, če enice poljubnega števila n pomnožimo z 2 in dobljeni produkt odštejemo od števila, ki smo ga dobili tako, da številu n odvzamemo enice, pri tem pa dobimo rezultat, ki je deljiv s 7 ali pa je enak nič.

Dokaz za deljivost s številom 7:

Naj bo poljubno naravno število $n = a_n a_{n-1} ... a_2 a_1 a_0$. Označimo enice z $b = a_0$. Če enice odrežemo od števila n, dobimo $a = a_n a_{n-1} ... a_2 a_1$. Potem je $n = 10a + b$.

Naj velja $a - 2b = 7 \cdot k$. S preoblikovanjem te enačbe dobimo:

$$10a - 20b = 70k$$
$$10a - 20b + b = 70k + b$$
$$10a + b = 70k + 21b$$
$$10a + b = 7(10k + 3b)$$
$$n = 7(10k + 3b)$$

Če 7 deli $a - 2b$, potem 7 deli n.

- Število je deljivo z 11, kadar je alternirajoča vsota njegovih števk enaka nič ali pa je deljiva z 11.

Dokaz za deljivost s številom 11:

Pri dokazu uporabimo znanje kongruenc, ki ga opišemo v razdelku 3. 1. Kongruence.

Naj bo naravno število $n = a_m a_{m-1} ... a_3 a_2 a_1 a_0$.

Torej lahko zapišemo $n = a_0 + 10a_1 + 10^2 a_2 + ... + 10^m a_m$.

Po definiciji kongruence velja $10 \equiv -1 (\mathrm{mod} 11)$. Ker lahko kongruence potenciramo, velja $10^k \equiv (-1)^k (\mathrm{mod} 11)$, $k \in N$.

Dobimo naslednji zapis:

$$n \equiv a_0 + (-1)a_1 + (-1)^2 a_2 + \ldots + (-1)^m a_m \,(\mathrm{mod}\, 11)$$
$$n \equiv a_0 - a_1 + a_2 - \ldots + (-1)^m a_m \,(\mathrm{mod}\, 11)$$
$$\Rightarrow 11 \mid (a_0 - a_1 + a_2 - \ldots + (-1)^m a_m \,(\mathrm{mod}\, 11)$$

2.4 RELACIJA DELJIVOSTI

Samo pravilo deljenja je zelo preprosto in sicer ali poljubno naravno število a deli poljubno naravno število b ali ne. S simboli relacijo deljivosti zapišemo takole:

$\boldsymbol{b \mid a}$ če in samo če je $a = k \cdot b$.

V tem primeru je število a deljenec, število b delitelj, k pa je kvocient. Naravno število b je delitelj naravnega števila a samo v primeru, če obstaja naravno število k, da velja $a = k \cdot b$.

Pri deljivosti naravnih števil obstajajo tudi določene posebnosti, ki nam samo računanje olajšajo.

1) 1 je delitelj vsakega naravnega števila.

2) Poljubno število m je delitelj samega sebe in vseh svojih večkratnikov.

3) Če d deli naravni števili n in m, potem deli tudi vsoto in razliko števil n in m.

Trditev lahko dokažemo s preprosto enačbo:

$$\boldsymbol{n = k_1 \cdot d}$$
$$\boldsymbol{m = k_2 \cdot d}$$
$$\boldsymbol{n \pm m = (k_1 \pm k_2) \cdot d = k \cdot d}$$
$$\boldsymbol{d \mid (n \pm m)}$$

Relacija deljivosti ima tri lastnosti, zaradi katerih je delno urejena in delno ureja množico naravnih števil.

1) refleksivnost: $\boldsymbol{a} \mid \boldsymbol{a}$ ker je $a = 1 \cdot a$

Refleksivnost pomeni, da vsako število deli samega sebe.

2) antisimetričnost: če $\boldsymbol{a} \mid \boldsymbol{b}$ in $\boldsymbol{b} \mid \boldsymbol{a}$, potem je $a = b$

Antisimetričnost dokažemo:

$$b = k_1 \cdot a$$
$$a = k_2 \cdot b$$
$$b = (k_1 \cdot k_2) b$$
$$k_1, k_2 \in N \Rightarrow k_1 \cdot k_2 = 1$$
$$\Rightarrow k_1 = k_2 = 1$$

3) tranzitivnost: če $\boldsymbol{a} \mid \boldsymbol{b}$ in $\boldsymbol{b} \mid \boldsymbol{c}$, potem $\boldsymbol{a} \mid \boldsymbol{c}$

Tranzitivnost dokažemo:

$$\boldsymbol{b} = \boldsymbol{k}_1 \cdot \boldsymbol{a}$$
$$\boldsymbol{c} = \boldsymbol{k}_2 \cdot \boldsymbol{b}$$
$$\boldsymbol{c} = (\boldsymbol{k}_1 \cdot \boldsymbol{k}_2)\boldsymbol{a} \Rightarrow \boldsymbol{a} \mid \boldsymbol{c}$$

2.5 OSNOVNI IZREK O DELJENJU

Če dve naravni števili nista v relaciji deljivosti, pri deljenju dobimo ostanek, ki je manjši od delitelja. Deljenje poljubnih dveh naravnih števil a in b zapišemo tako:

$$a = k \cdot b + r$$

Število a predstavlja deljenec, število b delitelj, k je kvocient, r pa ostanek, ki je nenegativen in manjši od delitelja b. To imenujemo osnovni izrek o deljenju naravnih števil.

2.6 NAJVEČJI SKUPNI DELITELJ IN NAJMANJŠI SKUPNI VEČKRATNIK

Dve naravni števili a in b imata določeno število deliteljev, ki jih znamo določiti in razvrstiti po velikosti. Največji skupni delitelj označimo z $D(a,b)$. Število 1 je skupni delitelj poljubnih dveh naravnih števil. Obstaja pa tudi možnost, da je edini skupni delitelj obeh poljubnih števil število 1, s tem pa tudi njun največji skupni delitelj. Takšni števili imenujemo tuji števili. Kar pomeni, da ima vsako praštevilo v razmerju z naravnim številom le dve možnosti: ali praštevilo deli naravno število ali pa mu je tuje.

Težava pa nastane pri iskanju skupnih večkratnikov dveh naravnih števil, teh je namreč neskončno mnogo. Vendar pa jih nekaj vseeno lahko določimo, pri tem pa opazimo, da je eden izmed njih najmanjši. Najmanjši skupni večkratnik poljubnih dveh števil a in b je najmanjše število, ki je deljivo z obema številoma. Označimo ga z $v(a,b)$.

S pomočjo znanja o deliteljih so odkrili tudi tako imenovana popolna števila. To so števila, katerih vsota njihovih pravih deliteljev je enaka prvotnemu številu. Pravi delitelji pa so tisti delitelji, ki so manjši od danega števila. Primer popolnega števila je število 28. Njegovi pravi delitelji so $D=\{1,2,4,7,14\}$. Če te delitelje seštejemo, spet dobimo število 28, kar vidimo v naslednji enačbi: $1+2+4+7+14=28$.

Poznamo pa tudi prijateljska števila. To sta poljubni števili a in b, pri katerih je vsota pravih deliteljev števila a enaka številu b in obratno, pri katerih je vsota pravih deliteljev števila b enaka številu a. Takšnih parov števil so danes našli že več kot 4300. Prijateljski števili sta na primer število 220 in 284. Najprej vsakemu od števil poiščemo prave delitelje.

$$D_{220}=\{1,2,4,5,10,11,20,22,44,55,110\}$$
$$D_{284}=\{1,2,4,71,142\}$$

Če te delitelje seštejemo, dobimo rezultat, ki nam potrdi zgornjo trditev.

$$1+2+4+5+10+11+20+22+44+55+110=284$$
$$1+2+4+71+142=220$$

Pri iskanju največjega skupnega delitelja in najmanjšega skupnega večkratnika poljubnih dveh števil si pomagamo na več načinov. Eden izmed njih je prafaktorizacija števil.

Za poljubni števili napišemo praštevilski razcep. Nato pogledamo, katera praštevila so skupna in kolikokrat se ponovijo. Največji skupni delitelj izračunamo tako, da pomnožimo vse skupne prafaktorje in pri potenci, kjer nastopajo, izberemo manjši eksponent. Najmanjši skupni večkratnik pa je produkt vseh prafaktorjev in pri potenci, kjer nastopajo, izberemo večji eksponent.

Vendar pa to ni edina povezava med največjim skupnim deliteljem in najmanjšim skupnim večkratnikom poljubnih dveh števil a in b. Če ju pomnožimo, dobimo produkt teh dveh števil, kar zapišemo z enačbo:

$$D(a,b)\cdot v(a,b)=a\cdot b$$

2.7 EVKLIDOV ALGORITEM

Evklidov algoritem je poseben postopek, pri katerem lahko s pomočjo enačbe:

$$D(a,b)\cdot v(a,b)=a\cdot b$$

izračunamo največji skupni delitelj in najmanjši skupni večkratnik. Izmed dveh poljubnih števil a in b izberemo večje in ga z manjšim delimo ter ga zapišemo kot vsoto produkta količnika z manjšim številom in ostanka. V naslednjem koraku deljenec postane prejšnji delitelj, delitelj pa prejšnji ostanek. Zadnji neničelni ostanek je največji skupni delitelj. S pomočjo tega podatka in števil a in b, lahko izračunamo najmanjši skupni večkratnik.

$$v(a,b)=\frac{a\cdot b}{D(a,b)}$$

Evklid je že pred več kot 2300 leti dokazal, da je praštevil neskončno mnogo. To naredimo na naslednji način. Izberemo si poljubno praštevilo p_k in si zastavimo vprašanje ali obstaja praštevilo, ki je večje od njega. Novo število, ki ga iščemo, mora

biti produkt vseh znanih po velikosti urejenih praštevil, povečan za 1, kar zapišemo z enačbo:

$$N = 2 \cdot 3 \cdot 5 \cdot \ldots \cdot p_k + 1$$

Sedaj imamo za novo število dve možnosti, ali ga uvrstimo med praštevila ali sestavljena števila. Če je N praštevilo, je s tem izrek že dokazan, saj smo prišli do števila, ki je večje od števila p_k. Če pa je N sestavljeno število, je deljivo z vsaj enim praštevilom p. Število N je za ena povečan produkt vseh znanih praštevil, zato pri deljenju z vsakim izmed njih dobimo ostanek 1. Iz tega lahko izpeljemo sklep da je N od p_k večje praštevilo, kar pa potrjuje izrek, da je praštevil več kot k. Zato v vsakem primeru obstaja praštevilo, ki je večje od p_k, s čemer pa smo dokazali, da je praštevil neskončno mnogo. (Pavlič, 2013, str. 44, 45).

3. RAZISKOVALNI DEL

3.1 KONGURENCE

Kongruence je uvedel Carl Friedrich Gauss, ki je bil slaven matematik, fizik in astronom. Živel je med leti 1777 in 1855. Že kot otrok je znal odlično računati, pri njegovih rosnih sedemnajstih letih pa je imel za seboj že pomembna odkritja. Le ta je zapisoval v svoj matematični dnevnik. Znal je povezovati teorijo s prakso. Njegovo najbolj znano delo so Aritmetične raziskave, ki v izvirniku nosijo naslov Disquisitiones Arithmeticae. V tem delu Gauss natančno opiše cela števila in njihove lastnosti, kjer vpelje tudi kongruence. Kongruence nam omogočajo poenostavljeno računanje s celimi števili, predvsem deljenje s poljubnim naravnim številom m. S kongruencami se je ukvarjal tudi Jože Grasselli v knjigi Elementarna teorija števil, ki je osnova mojemu nadaljnjemu raziskovanju. (Grasselli, 2009, str. 54- 67).

Slika 4: Carl Friedrich Gauss.

3.1.1 Definicija kongruence

Poljubni celi števili a in b sta kongruentni po modulu m, kar skrajšano zapišemo kot:

$$a \equiv b(\mathrm{mod}\, m),$$

kadar pri deljenju z m dasta isti ostanek. Torej je $a = k_1 m + r$ in $b = k_2 m + r$, $0 \le r < m$. Ta definicija je ekvivalentna naslednji: poljubni celi števili a in b sta kongruentni po modulu m, kadar obstaja takšno celo število k, da velja:

$$a - b = k \cdot m.$$

3.1.2 Lastnosti kongruenc

a) Prva lastnost kongruenc je refleksivnost:

$$a \equiv a(\mathrm{mod}\, m)$$

Dokaz:

$$a - a = 0 \cdot m$$

b) Druga lastnost kongruenc je simetričnost. Če je a kongruenten b po modulu m, je tudi b kongruenten a po modulu m:

$$a \equiv b(\mathrm{mod}\, m) \Rightarrow b \equiv a(\mathrm{mod}\, m)$$

Dokaz:

$$\begin{aligned} a - b &= k \cdot m \\ a - b &= -(b - a) \\ -(b - a) &= k \cdot m \\ b - a &= -k \cdot m \end{aligned}$$

c) Tretja lastnost kongruenc je tranzitivnost. Če je a kongruenten b po modulu m in če je b kongruenten c po modulu m, potem je tudi a kongruenten c po modulu m.

$$a \equiv b(\mathrm{mod}\, m) \wedge b \equiv c(\mathrm{mod}\, m) \Rightarrow a \equiv c(\mathrm{mod}\, m)$$

Dokaz:

$$a \equiv b(\mathrm{mod}\, m) \wedge b \equiv c(\mathrm{mod}\, m)$$
$$a - b = h \cdot m \wedge b - c = k \cdot m$$
$$a - c = (h + k) \cdot m \Rightarrow a \equiv c(\mathrm{mod}\, m)$$
$$k, h \in R$$

3.1.3 Pravila za računanje s kongruencami

a) Seštevanje, odštevanje in množenje: kongruenci, ki imata isti modul, smemo členoma seštevati, odštevati ali množiti:

$$a \equiv b(\mathrm{mod}\, m) \wedge c \equiv d(\mathrm{mod}\, m) \Rightarrow ac \equiv bd(\mathrm{mod}\, m)$$
$$a \equiv b(\mathrm{mod}\, m) \wedge c \equiv d(\mathrm{mod}\, m) \Rightarrow a + c \equiv b + d(\mathrm{mod}\, m)$$
$$a \equiv b(\mathrm{mod}\, m) \wedge c \equiv d(\mathrm{mod}\, m) \Rightarrow a - c \equiv b - d(\mathrm{mod}\, m)$$

Dokaz za seštevanje:

$$a - b = h \cdot m$$
$$c - d = k \cdot m$$
$$(a - b) + (c - d) = h \cdot m + k \cdot m$$
$$a - b + c - d = m \cdot (h + k)$$
$$(a + c) - (b + d) = (h + k) \cdot m$$
$$a + c \equiv b + d(\mathrm{mod}\, m)$$

Dokaz za odštevanje:

$$a - b = h \cdot m$$
$$c - d = k \cdot m$$
$$(a - b) - (c - d) = h \cdot m - k \cdot m$$
$$a - c - (b - d) = m \cdot (h - k)$$
$$a - c \equiv b - d(\mathrm{mod}\, m)$$

Dokaz za množenje:

$$a - b = h \cdot m$$
$$c - d = k \cdot m$$
$$a \cdot c = (b + hm) \cdot (d + km)$$
$$a \cdot c = (b \cdot d + bkm + hmd + hkm^2)$$
$$a \cdot c = b \cdot d + m \cdot (b \cdot k + h \cdot d + m \cdot h \cdot k)$$
$$a \cdot c \equiv b \cdot d(\mathrm{mod}\, m)$$

b) Potenciranje kongruenc: kongruence smemo na obeh straneh potencirati z istim številom:

$$a \equiv b(\mathrm{mod}\, m) \Rightarrow a^n \equiv b^n (\mathrm{mod}\, m)$$

Dokaz: Uporabimo pravilo za množenje, kjer množimo kongruenci $a \equiv b(\mathrm{mod}\, m)$ in $a \equiv b(\mathrm{mod}\, m)$. Torej dobimo $a \cdot a \equiv b \cdot b(\mathrm{mod}\, m) \Rightarrow a^2 \equiv b^2 (\mathrm{mod}\, m)$. Če postopek ponovimo n- krat, dobimo želeni rezultat.

c) Množenje s celim številom: kongruenco smemo na obeh straneh pomnožiti z istim celim številom:

$$a \equiv b(\mathrm{mod}\, m) \wedge c \in Z \Rightarrow ac \equiv bc(\mathrm{mod}\, m)$$

Dokaz:

$$\begin{aligned} &a \equiv b(\mathrm{mod}\, m) \\ &a - b = hm / \cdot c \\ &ac - bc = hcm \\ &ac = bc(\mathrm{mod}\, m) \end{aligned}$$

d) Deljenje: kongruenco lahko delimo s poljubnim številom c samo takrat, ko je c tuj modulu m.

Dokaz: Naj velja nasprotno $D(c,m) = d, d > 1$. Kar pomeni $c = u \cdot d, m = v \cdot d$ in števili u in v sta tuji števili.

$$\begin{aligned} &a \cdot c \equiv b \cdot c(\mathrm{mod}\, m) \\ &a \cdot c - b \cdot c = k \cdot m \\ &(a-b) \cdot c = k \cdot m \\ &(a-b) \cdot (u \cdot d) = k \cdot (v \cdot d) \\ &(a-b) \cdot u = k \cdot v \Rightarrow u / k \\ &(a-b) = h \cdot v \\ &a \equiv b(\mathrm{mod}\, v) \\ &m = v \cdot d \Rightarrow v = \frac{m}{d} \Rightarrow d = 1 \end{aligned}$$

Dobili smo protislovje, kar pomeni da sta c in modul m tuji števili.

3.1.4 Primeri uporabe pravil za računanje s kongruencami

a) seštevanje: $12 \equiv 5(\mathrm{mod}\,7) + (-15 \equiv 6(\mathrm{mod}\,7)) \Rightarrow -3 \equiv 11(\mathrm{mod}\,7)$

b) odštevanje: $12 \equiv 5(\mathrm{mod}\,7) - (-15 \equiv 6(\mathrm{mod}\,7)) \Rightarrow 27 \equiv -1(\mathrm{mod}\,7)$

c) množenje: $12 \equiv 5(\mathrm{mod}\,7) \cdot (-15 \equiv 6(\mathrm{mod}\,7)) \Rightarrow -180 \equiv 30(\mathrm{mod}\,7)$

d) potenciranje: $19 \equiv 3(\mathrm{mod}\,8) \Rightarrow 19^5 \equiv 3^5(\mathrm{mod}\,8)$

e) deljenje: $63 \equiv 7(\mathrm{mod}\,8) \Rightarrow 9 \equiv 1(\mathrm{mod}\,8)$

3.2 KONGRUENČNI RAZREDI IN SESTAVI OSTANKOV

Vsa števila dajo pri deljenju s poljubnim številom m enega izmed ostankov $0, 1, 2, \ldots, m-1$. Glede na to jih lahko razdelimo v kongruenčne razrede. Poljubni dve števili iz istega kongruenčnega razreda dasta enak ostanek pri deljenju s številom m. Potem je tudi njuna razlika deljiva s tem številom, kar pomeni da sta števili kongruentni po modulu m. Dobimo natanko $m-1$ kongruenčnih razredov, ki jih zapišemo:

$$Z(0) = \{k \cdot m; k, m \in Z\}$$
$$Z(1) = \{k \cdot m + 1; k, m \in Z\}$$
$$\ldots$$
$$Z(m-1) = \{k \cdot m + (m-1); k, m \in Z\}$$

Množice, ki nastanejo, so torej $Z(0), Z(1), \ldots, Z(m-1)$. Vsako celo število je tako vsebovano natanko v enem kongruenčnem razredu.

Če iz vsakega kongruenčnega razreda po modulu m vzamemo natančno eno število, dobimo množico števil, ki jo imenujemo popolni sestav ostankov po modulu m.

Izberemo poljubni števili a in b ter popoln sestav ostankov po modulu m, ki ga zapišemo takole: $a_1, a_2, \ldots, a_m$. Veljati mora, da sta števili a in m tuji. Če poljubno

število a pomnožimo z $a_1, a_2, ..., a_m$ in prištejemo poljubno število b, dobimo m števil. Vsa ta števila pa so paroma nekongruentna po modulu m. Če ne bi bila, bi zapisali $a \cdot a_i + b \equiv a \cdot a_k + b (\mathrm{mod}\, m)$. Ker je a tuj m, velja zveza $a_i \equiv a_k (\mathrm{mod}\, m)$. a_1 in a_2 sta različni števili iz popolnega sestava ostankov ter gotovo nekongruentni po modulu m. Dobili smo $aa_1 + b, aa_2 + b..., aa_m + b$ nov popoln sestav ostankov po modulu m.

Popolni sestav ostankov po modulu m vsebuje m števil. Če izvzamemo le tista števila, ki so tuja modulu m, dobimo reducirani sestav ostankov po modulu m. Ta sestav vsebuje $\varphi(m)$ števil. $\varphi(m)$ je Eulerjeva funkcija, ki vsakemu naravnemu številu m poišče število njemu tujih ostankov.

3.3 EULERJEV IN FERMATOV IZREK

Pri računanju s kongruencami si lahko pomagamo z Eulerjevim in Fermatov izrekom.

Eulerjev izrek pravi, da celo število a, ki je tuje številu m, ustreza kongruenci $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$.

ZGLED: Velja: $D(5,12) = 1$. Potem je $\varphi(12) = 4$, saj obstajajo štirje ostanki pri deljenju s številom 12, ki so tuji s številom 12, to so 1, 5, 7 in 11. Eulerjev izrek nam pove, da je $5^4 \equiv 1 (\mathrm{mod}\, 12)$.

Dokaz Eulerjevega izreka:

Vsako število iz reduciranega sestava ostankov $a_1, a_2, ..., a_{\varphi(m)}$ je kongruentno po modulu m natančno enemu številu iz množice $aa_1, aa_2 ..., aa_{\varphi(m)}$, kjer je število a tuje številu m. Ker lahko kongruence množimo, lahko napišemo v obliki:

$$a^{\varphi(m)} \cdot a_1 \cdot a_2 ... a_{\varphi(m)} \equiv a_1 \cdot a_2 ... a_{\varphi(m)} (\mathrm{mod}\, m)$$

Ker lahko kongruence delimo, dobimo $a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$, saj so števila a_i tuja z m.

Če je modul praštevilo p, velja $\varphi(p) = p-1$. Če je celo število a tuje praštevilu p, potem velja kongruenca $a^{p-1} \equiv 1 (\text{mod } p)$. To imenujemo **Fermatov izrek**.

Če $a^{p-1} \equiv 1 (\text{mod } p)$ množimo z a, dobimo $a^p \equiv a (\text{mod } p)$. Praštevilo p tako deli razliko $a^p - a$ za vsako število a, ki je tuje s številom p. Praštevilo p deli to razliko tudi takrat, kadar a ni tuj p. Poljubno lahko izberemo, da je $a = 2$, tako da velja $p \mid (2^p - 2)$. Vsako sestavljeno naravno število n, za katerega velja $n \mid 2^n - 2$, imenujemo psevdopraštevilo.

V množici psevdopraštevil velja:

Če je n liho psevdopraštevilo, je tudi $2^n - 1$ psevdopraštevilo.

Psevdopraštevil je neskončno mnogo.

3.4 WILSONOV IZREK

Čeprav izrek nosi ime po angleškem matematiku Wilsonu iz 18. stoletja, bi ga naj že odkril indijski matematik Bhaskara v sedmem stoletju.

Wilsonov izrek se glasi: Od ena večje naravno število p je praštevilo natanko tedaj, ko je:

$$(p-1)! \equiv -1 (\text{mod } p)$$

Dokaz Wilsonovega izreka:

Naj velja $(p-1)! \equiv -1 (\text{mod } p)$. Denimo, da p ni praštevilo. Potem obstaja delitelj števila p vsebovan v produktu $(p-1)!$ različen od p in od 1. Kar pomeni protislovje z začetno predpostavko.

Naj bo p praštevilo večje od 3. Vsako naravno število a, ki je manjše od p, je tuje številu p, saj je p praštevilo.

Število b je inverz števila a po modulu p, če je $a \cdot b \equiv 1 (\text{mod } p)$. Število a ima enolično določen inverz $b < p$. Inverz a po modulu p obstaja natanko takrat, ko sta si števili a

in p tuji. Če je $b = a$, velja $(a-1)(a+1) \equiv 0 (\text{mod } p)$. Ker je p praštevilo, velja $a = 1$ oziroma $a = p-1$. Če je torej $1 < a < p-1$, obstaja natanko določeno od a različno število b, za katero velja $1 < b < p-1 \text{in } a \cdot b \equiv 1 (\text{mod } p)$. Števila $2,3,4,..., p-2$ uredimo v pare, kjer bo v vsakem paru števil njun produkt enak 1 po modulu p. Zato velja:

$$2 \cdot 3 \cdot 4 \cdot ... \cdot (p-2) \equiv 1 (\text{mod } p)$$
$$1 \cdot 2 \cdot 3 \cdot 4 \cdot ... \cdot (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 (\text{mod } p)$$
$$(p-1)! \equiv -1 (\text{mod } p)$$

Zgled Wilsonovega izreka:

$$p = 13,$$
$$12! = 479001600 \equiv -1 (\text{mod} 13)$$

3.5 PRIMERI UPORABE KONGRUENC

1. primer: uporaba Fermatovega izreka

Naloga: Kolikšen je ostanek pri deljenju števila 2^{100} s številom 17?

Števili 2 in 17 sta si tuji, kar pomeni, da je njun največji skupni delitelj 1 ($D(2,17) = 1$). Število 17 uvrščamo k praštevilom, zato lahko uporabimo Fermatov izrek:

$$2^{17-1} \equiv 1 (\text{mod} 17)$$
$$2^{16} \equiv 1 (\text{mod} 17)$$

Število 100 lahko zapišemo v obliki izreka za deljenje in sicer takole: $100 = 6 \cdot 16 + 4$. Iz pravila o potenciranju kongruenc vemo, da lahko kongruence na obeh staneh potenciramo z istim številom:

$$(2^{16})^6 \equiv 1^6 (\text{mod} 17)$$
$$2^{96} \equiv 1 (\text{mod} 17)$$

Kongruence lahko tudi členoma množimo, pod pogojem da imata enak modul. To v naslednjem koraku tudi storimo:

$$2^4 \cdot 2^{96} \equiv 2^4 \cdot 1 (\mathrm{mod}\, 17)$$
$$2^{100} \equiv 16 (\mathrm{mod}\, 17)$$

Pri deljenju števila 2^{100} s številom 17 dobimo ostanek 16.

2. primer

Naloga: Kolikšen je ostanek pri deljenju števila 317^{259} s številom 15?

Tokrat si pri deljenju ne moremo pomagati s Fermatovim izrekom, saj je število 15 sestavljeno število. Število 317 lahko zapišemo v obliki kongruence, in sicer:

$$317 \equiv 92 (\mathrm{mod}\, 15),$$

saj velja $317 \equiv 21 \cdot 15 + 2$. Dobimo $317 \equiv 2 (\mathrm{mod}\, 15)$. Velja kongruenca:

$$2^4 \equiv 1 (\mathrm{mod}\, 15)$$

Tudi tokrat lahko kongruenco potenciramo na obeh staneh:

$$(2^4)^{46} \equiv 1^{46} (\mathrm{mod}\, 15)$$
$$2^{256} \equiv 1 (\mathrm{mod}\, 15)$$

Nato še pomnožimo in dobimo rezultat:

$$2^{256} \cdot 2^3 \equiv 1 \cdot 2^3 (\mathrm{mod}\, 15)$$
$$2^{259} \equiv 8 (\mathrm{mod}\, 15)$$

Pri deljenju števila 317^{259}s številom 15 dobimo ostanek 8.

3. primer

Naloga: Ali število 43 deli $123^{203} - 45^{62}$?

Nalogo začnemo reševati pri številu 123, ki ga zapišemo v obliki kongruence:

$$123 \equiv -6 (\mathrm{mod}\, 43),$$

saj velja $123 = 43 \cdot 3 - 6$. Če upoštevamo pravila za potenciranje kongruenc, dobimo:

$$123^2 \equiv (-6)^2 (\mathrm{mod}\, 43)$$
$$123^2 \equiv 36 (\mathrm{mod}\, 43)$$

Število 36 lahko ponovno zapišemo v obliki: $36 = 1 \cdot 43 - 7$. Če združimo obe kongruenci dobimo:

$$123^2 \equiv -7 (\mathrm{mod}\, 43)$$

To kongruenco pomnožimo s prvo. Nastane produkt:

$$123^3 \equiv 42 (\mathrm{mod}\, 43),$$

kar lahko skrajšano zapišemo:

$$123^3 \equiv -1 (\mathrm{mod}\, 43).$$

Eksponent 203 ponovno lahko zapišemo v obliki izreka za deljenje in sicer $203 = 67 \cdot 3 + 2$. Ponovno uporabimo pravilo za potenciranje in množenje kongruenc:

$$\left(123^3\right)^{67} \equiv (-1)^{67} (\mathrm{mod}\, 43)$$
$$\left(123^3\right)^{67} \equiv -1 (\mathrm{mod}\, 43)$$
$$\left(123^3\right)^{67} \cdot 123^2 \equiv -1 \cdot (-7) (\mathrm{mod}\, 43)$$
$$123^{203} \equiv 7 (\mathrm{mod}\, 43)$$

Sedaj se lotimo drugega dela računa. Tudi število 45 zapišemo v obliki kongruence in sicer:

$$45 \equiv 2 (\mathrm{mod}\, 43).$$

Iz tega sledi:

$$45^7 \equiv 2^7 (\mathrm{mod}\, 43)$$
$$2^7 \equiv -1 (\mathrm{mod}\, 43)$$

Ker lahko število 62 zapišemo v obliki izreka za deljenje $62 = 7 \cdot 8 + 6$. Glede na to prejšnjo kongruenco potenciramo in dobimo:

$$\left(45^7\right)^8 \equiv (-1)^8 \pmod{43}$$
$$(-1)^8 \equiv 1 \pmod{43}$$
$$45^{62} \equiv 45^{56} \cdot 45^6 \pmod{43}$$
$$45^{56} \cdot 45^6 \equiv 1 \cdot 45^6 \pmod{43}$$
$$1 \cdot 45^6 \equiv 2^6 \pmod{43}$$
$$2^6 \equiv 64 \pmod{43}$$
$$64 \equiv 21 \pmod{43}$$

Kongruence med seboj odštejemo po pravilu za odštevanje in dobimo:

$$123^{203} - 45^{62} \equiv 7 - 21 \equiv -14 \pmod{43}$$

Število $123^{203} - 45^{62}$ torej ni deljivo s 43, saj dobimo ostanek -14.

4. primer: uporaba Eulerjevega izreka

Naloga: Kolikšen je ostanek pri deljenju števila 5^{13} s številom 26?

Pri računanju bomo uporabili Eulerjev izrek. Števili 5 in 26 sta tuji, torej je njun največji skupni delitelj 1. Najprej poiščemo vse ostanke, ki jih dobimo pri deljenju s številom 26. To je množica števil: $\{0,1,2,3,4,...25\}$. Izmed vseh števil, ki smo jih dobili, izberemo ostanke, ki so tuji številu 26. To so števila 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25. Teh je 12, kar zapišemo kot $\varphi(26) = 12$. Velja kongruenca:

$$5^{\varphi(26)} \equiv 1 \pmod{26}$$
$$5^{12} \equiv 1 \pmod{26}$$

Uporabimo pravilo za množenje kongruenc in dobimo:

$$5 \cdot 5^{12} \equiv 5 \cdot 1 \pmod{26}$$
$$5^{13} \equiv 5 \pmod{26}$$

Ostanek je torej 5.

5. primer: uporaba Wilsonovega izreka

Naloga: Poišči ostanek pri deljenju števila 37! s številom 41?

Ker je število 41 praštevilo, lahko uporabimo Wilsonov izrek:

$$(p-1)! \equiv -1 (\mathrm{mod}\ p)$$
$$(41-1)! \equiv -1 (\mathrm{mod}\ 41)$$
$$40! \equiv -1 (\mathrm{mod}\ 41)$$
$$(40)\cdot(39)\cdot(38)\cdot(37!) \equiv -1 (\mathrm{mod}\ 41)$$
$$(-1)\cdot(-2)\cdot(-3)\cdot(37!) \equiv -1 (\mathrm{mod}\ 41)$$
$$(-6)\cdot(37!) \equiv -1 (\mathrm{mod}\ 41)$$
$$6\cdot(37!) \equiv 1 (\mathrm{mod}\ 41)$$

Nato moramo zapisati kongruenco, pri kateri bo na eni strani produkt poljubnega naravnega števila in števila 6, na drugi strani pa bo ena, saj moramo dobiti enako kongruenco kot v prejšnjem delu:

$$6\cdot 7 \equiv 1 (\mathrm{mod}\ 41)$$
$$42 \equiv 1 (\mathrm{mod}\ 41)$$

Uporabimo pravilo za množenje kongruenc in dobimo:

$$7\cdot 6\cdot(37!) \equiv 7\cdot 1 (\mathrm{mod}\ 41)$$
$$37! \equiv 7 (\mathrm{mod}\ 41)$$

Ostanek pri deljenju števila 37! s številom 41 je 7.

4. DRUŽBENA ODGOVORNOST

Pri pripravi svoje raziskovalne naloge sem upoštevala pravilno navajanje virov in literature ter poskrbela, da tako ni prišlo do zlorabe podatkov. Temo raziskovalne naloge sem izbrala tako, da sem poglobila in razširila svoje srednješolsko znanje matematike in temo predstavila svojim vrstnikom, da bi se nekaj novega naučili.

5. ZAKLJUČEK

Med raziskovanjem sem ugotovila, da nam poznavanje kongruenc olajša računsko operacijo deljenja celih števil. S kongruencami, pravili za računanje s kongruencami, Eulerjevim, Fermatovim in Willsonovim izrekom lahko računamo z velikimi števili brez uporabe tehnologije. Pri uporabi kongruenc sem ugotovila, da je pomembno dejstvo ali je neko število praštevilo ali sestavljeno število, saj za praštevila obstaja več načinov reševanja matematičnih problemov. Tako sem vse tri hipoteze, ki sem si jih zastavila na začetku raziskave, potrdila. Spoznala sem, kako pomembno je poznavanje teoretičnega ozadja pri reševanju konkretnih matematičnih nalog. Za pomemben vidik matematičnega raziskovanja se je izkazalo dopolnjevanje matematičnih dokazov. Prav pri tem sem lažje razumela same izreke.

Svoje vrstnike sem pri dodatnem pouku matematike seznanila s pojmom kongruence in primeri uporabe kongruenc. Temo raziskovalne naloge sem jim predstavila kot poglobitev srednješolskega znanja matematike in prikazala kongruence kot nadgradnjo znanja o deljivosti celih števil. Osnova mojemu raziskovanju je bila literatura, ki je v primerjavi z matematičnimi učbeniki za srednje šole, zahtevnejša.

Ob koncu raziskave se ponuja še nekaj odprtih vprašanj, ki omogočajo nadaljnje raziskovanje. Znanje kongruenc bi lahko še razširila in nadgradila ter ga uporabila pri reševanju enačb. Lahko bi raziskovala računanje z večjimi števili, kjer bi poskušala najti ustrezno tehnologijo, ki jo morda lahko uporabimo za računanje.

6. VIRI IN LITERATURA

Ball, I. *Matematični čarovniki: Matematiko najdemo povsod*. Murska Sobota: Pomurska založba, 2010. ISBN 978-961-249-063-6.

Berlinghoff, W. P. in Gouvea F. Q. *Matematika skozi stoletja*. Ljubljana: Modrijan, 2008. ISBN 978-961-241-230-2.

Grasselli, J. *Elementarna teorija števil.* Ljubljana: DMFA, 2009. ISBN 978-961-212-217-1.

Kavka, D. et. al. *Linea = Črta: matematika za 1. letnik gimnazij.* Ljubljana: Modrijan, 2002. ISBN 961-6357-54-9.

Miloševič Dragoljub, M. Kriterij deljivosti s 7 in 13. *Presek*, 1981, letnik 9, št. 1: str. 14-15.

Pagon, D. Kongruence in Eulerjev izrek. *Presek*, 1987, letnik 15, št. 4, str. 194-196.

Pavlič, G. et. al. *Linea nova: matematika za gimnazije.* Ljubljana: Modrijan, 2013. ISBN 978-961-241-547-1.

7. VIRI SLIK

Eratosten, slika 2. Wikipedija: prosta enciklopedija [Online]. 13. 6. 2013. [Citirano: 4. 9. 2014; 1. 18]. Dostopno na spletnem naslovu: http://sl.wikipedia.org/wiki/Eratosten

Eratostenovo sito, slika 3. Ceca Barić, Prosti ili prim brojevi [Online]. [Citirano: 4. 9. 2014; 1. 25]. Dostopno na spletnem naslovu: http://www.mathos.unios.hr/~cbaric/wp/index1.html

Evklid, slika 1. Vikipedio: La libera enciklopedio [Online]. 29. 7. 2014. [Citirano: 5. 10. 2014; 0. 31]. Dostopno na spletnem naslovu: http://eo.wikipedia.org/wiki/E%C5%ADklido

Carl Friedrich Gauss, slika 4. Wikipedija: prosta enciklopedija [Online]. 1. 8. 2014. [Citirano: 14. 10. 2014; 0. 08]. Dostopno na spletnem naslovu: http://sl.wikipedia.org/wiki/Carl_Friedrich_Gauss