SVEUČILIŠTE U ZAGREBU

PRIRODOSLOVNO–MATEMATIČKI FAKULTET

MATEMATIČKI ODSJEK

Kristina Logarušić

TEORIJA BROJEVA U ZADATCIMA S NATJECANJA

Diplomski rad

Voditelj rada:
Izv. prof. dr. sc. Zrinka Franušić

Zagreb, srpanj, 2017.

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 mentorici izv. prof. dr. sc. Zrinki Franušić na posvećenom vremenu, strpljenju, pomoći i vodstvu tijekom izrade ovog diplomskog rada.
Posebno se zahvaljujem svojim roditeljima koji su mi omogućili da danas budem tu gdje jesam.
Najveće hvala mom suprugu na neizmjernoj podršci i ljubavi koju mi je pružio u svim dobrim i lošim trenutcima tijekom studiranja. Ljubavi, hvala Ti za sve!

Sadržaj

Uvod

Postavljanje i rješavanje različitih matematičkih problema duboko su ukorijenjeni u ljudsku povijest. No, prva zabilježena matematička natjecanja odvijala su se od kraja 18. stoljeća u Engleskoj (Cambridge), te za srednjoškolce od kraja 19. stoljeća u Mađarskoj.

Godine 1959. u Rumunjskoj je održano prvo međunarodno matematičko natjecanje za učenike srednjih škola na kojem je sudjelovalo sedam država iz Istočne Europe. Natjecanja su se nastavila pod nazivom *Međunarodna matematička olimpijada* (MMO), odnosno *International Mathematical Olympiad* (IMO). Broj država sudionica se postupno stalno povećavao, tako da ih je krajem devedesetih godina prošlog stoljeća bilo preko 80, a danas se natječu učenici iz preko 100 zemalja s 5 kontinenata. Olimpijada se održava redovito svake godine, s izuzetkom 1980. godine kad nije održana, već je umjesto nje organizirano natjecanje za učenike europskih država. Učenici iz Hrvatske su od 1963. do 1991. godine sudjelovali kao članovi jugoslavenske ekipe. Od 1993. Hrvatska sudjeluje na MMO kao samostalna država. Natjecanje se održava svake godine u drugoj državi. Ekipu svake zemlje čini šest učenika te dva voditelja. Jedan od njih je zadužen da sudjeluje u radu međunarodnog žirija kojeg čine po jedan predstavnik iz svake zemlje. Žiri treba odabrati šest zadataka iz skupine od oko pedeset do stotinu prijedloga. Zadatci se rješavaju tijekom dva dana, svaki dan po tri, i to kroz 4.5 sata. Hrvatska je 2012. godine prvi put osvojila zlatnu medalju na MMO, nakon niza srebrnih i brončanih medalja. Pored MMO održavaju se i neka druga međunarodna matematička natjecanja, kao npr. *Austrijsko-poljsko natjecanje*, *Balkanijada*, *Mediteransko matematičko natjecanje* (MYMC), *Srednjoeuropska matematička olimpijada* (MEMO - *The Middle European Mathematical Olympiad*) i dr.

U svijetu se organiziraju mnoga matematička natjecanja. Neka od njih, čiji zadatci će se naći dalje u radu su:
AHSME – *American High School Mathematics Examination*
AIME – *American Invitation Mathematics Examination*
USAMO - *United States of American Mathematical Olympiad*
PUTNAM - *William Lowell Putnam Mathematical Competition*

William Lowell Putnam Mathematical Competition (PUTNAM) je godišnje natjecanje iz matematike za redovne studente visokih učilišta u Sjedinjenim Američkim Državama i Kanadi. Smatra se jednim od najprestižnijih matematičkih natjecanja na sveučilišnoj razini

u svijetu. O težini samog natjecanja govori činjenica da je broj ostvarenih bodova natjecatelja često nula (od mogućih 120) unatoč tome što na njemu sudjeluju studenti specijalizirani za matematiku. Sastoji se od 12 pitanja od kojih svaki nosi po 10 bodova. PUTNAM natjecanje osnovala je 1927. godine Elizabeth Lowell Putnam u spomen na svog supruga Williama Lowella Putnama.

U Hrvatskoj se natjecanja iz matematike za učenike osnovnih i srednjih škola provode od 1959. godine. U studenom i prosincu 1958. godine Društvo matematičara i fizičara Narodne Republike Hrvatske organiziralo je gradsko natjecanje u matematici učenika zagrebačkih gimnazija. Od školske godine 1958./59. u mnogim školama održavala su se školska natjecanja, a iste školske godine organizirana su i prva općinska, gradska i kotarska natjecanja u matematici. Prvu polovicu školske godine 1959./60. obilježio je, za matematička natjecanja u Hrvatskoj, važan događaj. Održano je prvo republičko natjecanje u matematici učenika II., III. i IV. razreda gimnazija. Prvo republičko natjecanje iz matematike učenika osnovnih škola održano je u drugoj polovici školske godine 1964./65. u Pionirskom gradu (danas Grad mladih) u Zagrebu. Od 1965. godine svake se godine održavaju općinska i republička (državna) natjecanja za učenike VII. i VIII. razreda osnovnih škola.

Do godine 1991. natjecanje mladih matematičara Hrvatske na najvišoj razini zvalo se republičko natjecanje. Te godine Hrvatska je postala samostalna, neovisna i suverena država. Sve se promijenilo, pa i sustav natjecanja u Hrvatskoj. Od toga trenutka republičko natjecanje postalo je državno natjecanje u pravom smislu te riječi; hrvatski natjecatelji otada idu u svijet samostalno i pod svojim vlastitim imenom.

Državno natjecanje iz matematike posljednje je natjecanje u godišnjem ciklusu, nakon školskih, općinskih i županijskih natjecanja i obično se organizira početkom svibnja. Na njemu sudjeluju učenici sedmih i osmih razreda osnovne škole te srednjoškolci. Mlađi učenici, od četvrtog do šestog razreda osnovne škole, nakon županijskih natjecanja sudjeluju na regionalnim natjecanjima. Od 2006. godine natjecanje učenika srednjih škola podijeljeno je u dvije kategorije. A kategorija je otvorena za sve učenike, a u B kategoriji natječu se učenici koji ne pohađaju školu po programu matematičke gimnazije.

U Hrvatskoj se, osim općinskih, županijskih i državnih natjecanja, održava *Hrvatska matematička olimpijada* te *Matematički klokan*. *Hrvatska matematička olimpijada* je natjecanje koje se sastoji od nekoliko testova na temelju kojih se određuju ekipe za međunarodna natjecanja MMO i MEMO. Prva *Hrvatska matematička olimpijada* održana je 2010. godine.

Udruga *Klokan bez granica* organizira "igru - natjecanje" *Matematički klokan*. Radi se o međunarodnom natjecanju koje se organizira svake godine u ožujku, istog dana, u isto vrijeme, u svim zemljama sudionicama. Glavni cilj je popularizacija matematike i širenje osnovne matematičke kulture. Glavni "moto" ovog natjecanja je: bez selekcije, bez eliminacije i bez finala. Natjecanje se sastoji od 12 zadataka za dobne skupine: Pčelice (2.

razred OŠ) i Leptirići (3. razred OŠ), odnosno 24 zadatka za dobne skupine: Ecoliers (4. i 5. razred OŠ), Benjamins (6. i 7. razred OŠ), Cadets (8. razred OŠ i 1. razred SŠ), Juniors (2. i 3. razred SŠ) i Students (4. razred SŠ i studenti 1. godine). Namjera ovog natjecanja je motivirati učenike da se bave matematikom izvan redovitih školskih programa. Udruga *Klokan bez granica* osnovana je 1994. godine u Strasbourgu po uzoru na matematičko natjecanje *Klokan* koje su 1991. godine organizirala dva francuska profesora za oko 120 000 natjecatelja. Danas natjecanju pristupi više od 6 000 000 natjecatelja iz više od 50 zemalja. Hrvatska je prvi put sudjelovala u ovom natjecanju 1999. godine s 1000 učenika osnovih i 1000 učenika srednjih škola. Danas sudjeluje nekoliko desetaka tisuća učenika iz Hrvatske. Važno je naglasiti da u natjecanju mogu sudjelovati svi učenici, bez obzira na uspjeh iz matematike u redovnoj nastavi.

Cilj ovog rada je predstaviti niz različitih zadataka kako s domaćih tako i s inozemnih i međunarodnih matematičkih natjecanja koji su vezani uz teoriju brojeva. Teorija brojeva je grana matematike koja ponajprije proučava svojstva skupa prirodnih, cijelih i ponekad racionalnih brojeva. U radu će se navesti definicije i iskazati svojstva bitnih pojmova iz teorije brojeva koji su zastupljeni u natjecateljskim zadatcima. Neke tvrdnje i teoremi su dokazani, no naglasak u radu je stavljen na detaljnom prikazu rješenja zadatka, a u nekim slučajevima ponuđene su i različite metode rješavanja istih. Primjenom definicija, svojstava i teorema neke od zadataka riješili smo na puno kraći i jednostavniji način, nego što ih rješavaju učenici u osnovnoj i srednjoj školi. Rad je podijeljen u tri poglavlja. U prvom poglavlju bavimo se problemima vezanim uz pojam djeljivosti te ostalim pojmovima koji proizlaze iz tog koncepta, u drugom poglavlju onima vezanim uz kongruencije, a u trećem se rješavaju diofantske jednadžbe te daje pregled najčešćih metoda za njihovo rješavanje.

Poglavlje 1

Djeljivost

1.1 Teorem o dijeljenju s ostatkom

Jedna od najvažnijih i temeljnih ideja u teoriji brojeva je pojam djeljivosti.

Definicija 1.1.1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b **djeljiv** s a, odnosno da a **dijeli** b, ako postoji cijeli broj x takav da je $b = a \cdot x$. Zapisujemo $a \mid b$, a ako b nije djeljiv s a, onda $a \nmid b$. Ako $a \mid b$, onda još kažemo da je a **djelitelj** od b, a da je b **višekratnik** od a.*

Na primjer, $2 \mid 18$, $5 \mid 25$, $3 \mid -6$, $2 \nmid 9$, $8 \nmid 15$. Nekoliko jednostavnih svojstava djeljivosti slijede neposredno iz definicije djeljivosti.

Propozicija 1.1.2. *Neka su a, b i c cijeli brojevi .*

(1) Ako $a \mid b$ i $b \mid c$, onda $a \mid c$.

(2) Ako $a \mid b$ i $a \mid c$, onda $a \mid (b \pm c)$.

(3) Ako $a \mid b$ i $b \mid a$, onda $a = \pm b$.

Dokaz. (1) Budući da $a \mid b$ i $b \mid c$, postoje cijeli brojevi u i v takvi da je $au = b$ i $bv = c$. Odmah slijedi da je $auv = c$. Dakle, $a \mid c$.

(2) Budući da $a \mid b$ i $a \mid c$, tada je $as = b$ i $at = c$ za neke $s, t \in \mathbb{Z}$. Iz toga slijedi $b \pm c = a(s \pm t)$, pa $a \mid (b \pm c)$.

(3) Budući da $a \mid b$ i $b \mid a$, postoje cijeli brojevi u i v takvi da je $au = b$ i $bv = a$. Iz toga slijedi da je $u \cdot v = 1$. Dakle, $u = 1$ i $v = 1$ ili $u = -1$ i $v = -1$ odnosno $a = \pm b$.

□

Primjer 1.1.3. [2011., Županijsko natjecanje, 1. razred, A varijanta]
Odredi sve četveroznamenkaste brojeve, čije su prve dvije znamenke međusobno jednake i zadnje dvije znamenke međusobno jednake, a koji su potpuni kvadrati (tj. kvadrati nekog prirodnog broja).

Rješenje. Neka je traženi broj kvadrat broja n, dakle $n^2 = \overline{aabb}$. Vrijedi

$$\overline{aabb} = 1100a + 11b = 11 \cdot (100a + b) = 11 \cdot \overline{a0b}$$

pri čemu su a i b znamenke, $a \neq 0$, tj. broj $\overline{aabb} = n^2$ je djeljiv s 11. Odavde zaključujemo da je n djeljiv s 11, tj. $n = 11k$, za neki $k \in \mathbb{N}$. To znači da je traženi broj oblika $121k^2$.
Da bi taj broj bio četveroznamenkast mora biti $3 \leq k \leq 9$. Računamo redom:

k	3	4	5	6	7	8	9
$121k^2$	1089	1936	3025	4356	5929	7744	9801

Vidimo da je jedino rješenje broj 7744 (kvadrat broja 88). ■

Slijedi fundamentalan teorem koji govori o djeljivosti cijelog broja b s prirodnim brojem a.

Teorem 1.1.4 (Teorem o dijeljenju s ostatkom)**.** *Za proizvoljan prirodan broj a i cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je*

$$b = aq + r,\ 0 \leq r < a.$$

Dokaz. Promotrimo skup $\{b - am : m \in \mathbb{Z}\}$. Najmanji nenegativni član ovog skupa označimo sa r. Dakle,

$$r = \min\{\{b - am : m \in \mathbb{Z}\} \cap \mathbb{N}\}.$$

Tada je po definiciji $0 \leq r < a$ i postoji $q \in \mathbb{Z}$ takav da je $b - qa = r$, tj. $b = qa + r$.

Sada pokažimo jedinstvenost brojeva q i r. Pretpostavimo suprotno, tj. da postoji još jedan par cijelih brojeva q_1, r_1 koji zadovoljava iste uvjete i da je $r \neq r_1$, odnosno da je na primjer $r < r_1$. Tada je $0 < r_1 - r < a$, dok je s druge strane $r_1 - r = a(q - q_1) \geq a$ što je očita kontradikcija. Prema tome je $r_1 = r$, a otuda je i $q_1 = q$. □

Cijeli broj q iz Teorema 1.1.4 zove se *kvocijent*, a broj r zovemo *ostatak*. Primijetimo da r može poprimiti vrijednosti $0, 1, \ldots, a - 1$. Ako je $r = 0$, onda a dijeli b.

Primjer 1.1.5. [2016., Matematički klokan, skupina Junior]
Podijelimo li prirodan broj brojem 6 *ostatak je* 3*. Koliki je ostatak ako broj* $3x$ *podijelimo brojem* 6*?*

Rješenje. Označimo s x prirodan broj koji pri dijeljenju s brojem 6 daje ostatak 3. Sada prema Teoremu o dijeljenju s ostatkom 1.1.4 imamo da je

$$x = 6k + 3$$

za neki prirodan broj k. Množenjem jednakosti s 3 dobivamo:

$$3x = 18k + 9 = 6(3k + 1) + 3 = 6l + 3,$$

gdje je $l = 3k + 1$ očito prirodan broj. Iz toga zaključujemo da je ostatak pri dijeljenju broja $3x$ brojem 6 jednak 3. ■

Primjer 1.1.6. [1976., AHSME]
Neka je r ostatak pri djeljenju brojeva 1059*,* 1417 *i* 2312 *brojem* $d > 1$*. Pronađi vrijednost izraza* $d - r$*.*

Rješenje. Primjenom Teorema o djeljenju s ostatkom 1.1.4 imamo:

$$\begin{aligned} 1059 &= q_1 d + r, \\ 1417 &= q_2 d + r, \\ 2312 &= q_3 d + r, \end{aligned}$$

za neke cijele brojeve q_1, q_2, q_3. Iz toga slijedi:

$$\begin{aligned} 358 &= 1417 - 1059 = (q_2 d + r) - (q_1 d + r) = d(q_2 - q_1), \\ 1253 &= 2312 - 1059 = (q_3 d + r) - (q_1 d + r) = d(q_3 - q_1), \\ 895 &= 2312 - 1417 = (q_3 d + r) - (q_2 d + r) = d(q_3 - q_2). \end{aligned}$$

Dakle, $d \mid 358 = 2 \cdot 179$, $d \mid 1253 = 7 \cdot 179$ i $d \mid 895 = 5 \cdot 179$. Budući da je $d > 1$ zaključujemo da je $d = 179$. Kako je $1059 = 5 \cdot 179 + 164$ slijedi da je $r = 164$. Sada je $d - r = 179 - 164 = 15$. ■

Definicija 1.1.7. *Prirodan broj* $p > 1$ *zove se* ***prost*** *ako p nema niti jednog djelitelja d takvog da je* $1 < d < p$*. Ako prirodan broj* $a > 1$ *nije prost, onda kažemo da je* ***složen****.*

Napomenimo da broj 1 ne smatramo ni prostim ni složenim brojem.

Primjer 1.1.8. [2014., Županijsko, 3. razred, A varijanta]
Odredi sve proste brojeve p za koje postoji prirodni broj n takav da su brojevi $n^2 + 3$ *i* $(n + 1)^2 + 3$ *djeljivi s p.*

Rješenje. Pretpostavimo da p dijeli $n^2 + 3$ i $n^2 + 2n + 4$ za neki $n \in \mathbb{N}$. Stoga p dijeli i njihovu razliku:

$$p \mid (n^2 + 2n + 4) - (n^2 + 3) = 2n + 1.$$

Nadalje, p dijeli i $(2n + 1)^2$, a iz uvjeta da p dijeli $n^2 + 3$ slijedi da p dijeli $4(n^2 + 3)$. Otuda slijedi da

$$p \mid (2n + 1)^2 - 4(n^2 + 3) = 4n - 11.$$

Sada dobivamo

$$p \mid 2(2n + 1) - (4n - 11) = 13,$$

pa je $p = 13$ jedini prost broj koji bi mogao zadovoljiti uvjete zadatka. Odredimo još i neki n za koji $13 \mid n^2 + 3, (n + 1)^2 + 3$. Kako $13 \mid 2n + 1$, slijedi da bi "kandidat" za n mogao biti broj 6. Budući da $13 \mid 6^2 + 3, 7^2 + 3$ slijedi da je $p = 13$ jedini prost broj za koji vrijede uvjeti zadatka. ■

Napomena. Prethodni zadatak možemo proširiti tako da pokušamo odrediti sve prirodne brojeve n za koje $13 \mid n^2 + 3$ i $13 \mid (n + 1)^2 + 3$. Pokazali smo da tada $13 \mid 2n + 1$. No, vrijedi i obrat. Ako $13 \mid 2n + 1$, onda $13 \mid n^2 + 3$ i $13 \mid (n + 1)^2 + 3$. Zaista, kako $13 \mid (2n + 1)^2 = 4n^2 + 4n + 1$, slijedi da $13 \mid 4n^2 + 4n + 1 - 2(2n + 1) + 13 = 4n^2 + 12$, pa $13 \mid n^2 + 3$. Konačno, $13 \mid (n^2 + 3) + (2n + 1) = (n + 1)^2 + 3$. Stoga smo pokazali da $13 \mid n^2 + 3$ i $13 \mid (n + 1)^2 + 3$ ako i samo ako $13 \mid 2n + 1$. Sada možemo zaključiti da su svi prirodni brojevi n za koje vrijede postavljeni uvjeti oblika

$$\frac{13(2k + 1) - 1}{2} = 13k + 6, \quad k \in \mathbb{N}_0.$$

Najmanji među njima je $n = 6$.

Teorem 1.1.9. *Svaki prirodan broj $n > 1$ može se prikazati kao produkt prostih brojeva (s jednim ili više faktora).*

Dokaz. Teorem ćemo dokazati matematičkom indukcijom. Broj 2 je prost broj. Pretpostavimo da je $n > 2$, te da tvrdnja teorema vrijedi za sve m, $2 \leq m < n$. Želimo dokazati da se i n može prikazati kao produkt prostih faktora. Ako je n prost broj, nemamo što dokazivati. U protivnom je $n = n_1 n_2$, gdje je $1 < n_1 < n$ i $1 < n_2 < n$. Po pretpostavci indukcije, n_1 i n_2 su produkti prostih brojeva, pa stoga i n ima to svojstvo. □

No, vrijedi i jača tvrdnja od Teorema 1.1.9.

Teorem 1.1.10 (Osnovni teorem aritmetike)**.** *Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.*

Prema tome, svaki prirodan broj $n > 1$ možemo prikazati u obliku

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \tag{1.1}$$

gdje su $p_1, \ldots, p_r$ različiti prosti brojevi, a $\alpha_1, \ldots, \alpha_r$ prirodni brojevi. Ovakav prikaz broja n zove se *kanonski rastav broja n na proste faktore*. Uobičajeno je rastav pisati u rastućem poretku prostih brojeva, to jest za $p_1 < p_2 < \cdots < p_r$. U tom slučaju kanonski rastav je jedinstven.

U primjenama Teorema 1.1.10 često je praktično prirodan broj a zapisati u obliku

$$a = \prod_p p^{\alpha(p)},$$

gdje je $\alpha(p) \geq 0$ i $\alpha(p) = 0$ ako $p \nmid a$ (odnosno $\alpha(p) > 0$ ako $p|a$). Dakle, podrazumijeva se da je $\alpha(p) = 0$ za skoro sve proste brojeve p, a za njih konačno mnogo je $\alpha(p)$ veći od 0. Ako je $a = 1$, onda je $\alpha(p) = 0$ za sve p.

Nadalje, ako je broj n oblika (1.1), tada je svaki njegov djelitelj $d \in \mathbb{N}$ oblika

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_r^{\beta_r}, \tag{1.2}$$

gdje je $0 \leq \beta_i \leq \alpha_i$, $i = 1, \ldots, k$. (Napomenimo da (1.2) ne predstavlja općenito kanonski rastav broja d jer se u eksponentu može nalaziti i 0.) Sada prema osnovnom kombinatornom principu produkta zaključujemo da je broj svih prirodnih djelitelja od n jednak

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1).$$

Uobičajeno je broj svih prirodnih djelitelja od n označiti s $\tau(n)$. Dakle,

$$\tau : \mathbb{N} \to \mathbb{N},\ \tau(n) = \prod_{i=1}^{r} (\alpha_i + 1), \tag{1.3}$$

pri čemu je n dan s (1.1). Kako i mnoge funkcije u teoriji brojeva i funkcija τ ima svojstvo *multiplikativnosti*, to jest $\tau(1) = 1$ i

$$\tau(mn) = \tau(m)\tau(n),$$

za sve prirodne brojeve m i n takve da je $\text{nzd}(m, n) = 1$.

Primjer 1.1.11. [2013., Državno natjecanje, 4. razred, A varijanta]
Odredi sve prirodne brojeve $n > 1$ takve da je umnožak svih pozitivnih djelitelja broja n jednak n^3. Prikaži ih u kanonskom obliku, tj. pomoću rastava na proste faktore.

Rješenje. Neka su $1 = d_1 < d_2 < \ldots < d_k = n$ svi pozitivni djelitelji broja n. Primjetimo da je

$$d_1 \cdot d_k = d_2 \cdot d_{k-1} = d_3 \cdot d_{k-2} = n.$$

Iz ovoga zaključujemo da je umnožak djelitelja broja n jednak n^3 ako i samo ako n ima točno 6 djelitelja.

Prirodan broj n možemo pisati u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, gdje su $p_1, \ldots, p_r$ različiti prosti brojevi, a $\alpha_1, \ldots, \alpha_r$ prirodni brojevi. Broj djelitelja tog broja jednak je $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1)$. Budući da smo ustanovili da n ima točno 6 djelitelje, dobivamo

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_r + 1) = 6.$$

Kako je svaki od faktora na lijevoj strani veći od 1, postoje samo dvije mogućnosti:

$$r = 1, \alpha_1 = 5 \text{ ili } r = 2, \alpha_1 = 2, \alpha_2 = 1.$$

Stoga je $n > 1$ takav da je umnožak svih njegovih pozitivnih djelitelja jednak n^3 oblika $n = p^5$ za svaki prost broj p ili oblika $n = p^2 q$ za različite proste brojeve p i q. ■

Primjer 1.1.12. [2015., Hrvatska matematička olimpijada]
Neka je $n \geq 2$ prirodan broj i p prost broj. Ako je broj $p - 1$ djeljiv brojem n, a broj $n^3 - 1$ djeljiv brojem p, dokaži da je $4p - 3$ kvadrat nekog prirodnog broja.

Rješenje. Budući da n dijeli $p - 1$, prema definiciji djeljivosti, postoji prirodan broj a takav da je $p - 1 = an$. Uz to je i $p - 1 \geq n$. Stoga uvjet da je $n^3 - 1 = (n - 1)(n^2 + n + 1)$ djeljiv prostim brojem p povlači da je $p \mid n^2 + n + 1$ jer $n - 1$ ne može biti djeljiv s p zbog $1 < n - 1 < p$. Dakle, $an + 1 = p \mid n^2 + n + 1$. Otuda je $an + 1 \leq n^2 + n + 1$, tj. $an \leq n^2 + n$. Stoga, $1 \leq a \leq n + 1$.

S druge strane,

$$an + 1 \mid a(n^2 + n + 1) - n(an + 1) = (a - 1)n + a.$$

Kako je $(a - 1)n + a > 0$, dobivamo $(a - 1)n + a \geq an + 1$, iz čega je $a \geq n + 1$. Dakle, $a = n + 1$, $p = an + 1 = n^2 + n + 1$ te

$$4p - 3 = 4n^2 + 4n + 1 = (2n + 1)^2.$$

■

Zadatak 1.1.12 može se riješiti i na sljedeći način.

Rješenje. Budući da n dijeli $p-1$, postoji prirodni broj a takav da je

$$p-1=an. \tag{1.4}$$

Zaključujemo da je $p-1\geq n$. Iz uvjeta da je $n^3-1=(n-1)(n^2+n+1)$ djeljiv prostim brojem p, slijedi da je n^2+n+1 djeljiv s p. Stoga postoji prirodan broj b takav da je

$$n^2+n+1=bp. \tag{1.5}$$

Kombiniranjem jednakosti (1.4) i (1.5) dobivamo:

$$n^2+n+1=b(an+1),$$

odnosno

$$n(n+1-ab)=b-1.$$

Označimo $c=n+1-ab$. Kako je $b-1\in\mathbb{N}_0$, slijedi da je i $c\in\mathbb{N}_0$ te

$$b=cn+1.$$

Sada imamo

$$n^2+n+1=bp=(cn+1)(an+1)=acn^2+(a+c)n+1,$$

pa oduzimanjem jedinice i dijeljenjem s n dobivamo

$$n+1=acn+a+c.$$

Budući su $a,n\in\mathbb{N}$ prethodna jednakost može biti ispunjena jedino ako je $c=0$ (u suprotnom ako je $c>0$, onda je desna strana jednakosti veća od lijeve). Dakle, slijedi da je $b=1$ i $p=n^2+n+1$ što povlači $4p-3=(2n+1)^2$. ■

Primjer 1.1.13. [2012., Općinsko/Školsko natjecanje, 1. razred, A varijanta]
Odredi sve parove prostih prirodnih brojeva p i q za koje postoji cijeli broj a takav da vrijedi $a^4=pa^3+q$.

Rješenje. Ako su p i q prosti i a cijeli broj za koji vrijedi $a^4=pa^3+q$, onda je $a^3(a-p)=q$, te zaključujemo da a^3 dijeli prost broj q. Stoga a može biti samo 1 ili -1. Ako je $a=1$, onda je $1-p=q$, no takvi prosti brojevi ne postoje. Ako je $a=-1$, slijedi $1+p=q$ a to je jedino moguće za $p=2$ i $q=3$. ■

Primjer 1.1.14. [2016., Županijsko natjecanje, 2. razred, A varijanta]
Koliko ima uređenih parova prirodnih brojeva (m,k) za koje vrijedi $20m=k(m-15k)$?

Rješenje. Izrazimo li m preko k dobivamo

$$m = \frac{15k^2}{k-20}.$$

Odavde slijedi da je m prirodni broj ako i samo ako je $k > 20$ i $k-20$ dijeli $15k^2$. Budući da je

$$\frac{15k^2}{k-20} = \frac{15(k-20)(k+20) + 20^2 \cdot 15}{k-20} = 15(k+20) + \frac{6000}{k-20},$$

m je prirodni broj ako i samo ako je $k > 20$ i $k-20$ dijeli 6000. Kako je $6000 = 2^4 \cdot 3 \cdot 5^3$, svaki pozitivni djelitelj broja 6000 je oblika $2^a \cdot 3^b \cdot 5^c$, pri čemu je $a \in \{0,1,2,3,4\}$, $b \in \{0,1\}$ i $c \in \{0,1,2,3\}$. Zato je broj djelitelja broja 6000 jednak $5 \cdot 2 \cdot 4 = 40$. (tj. vidi (1.3)). Zaključujemo da traženih parova (m,k) ima 40. ■

Primjer 1.1.15. [2013., Županijsko natjecanje, 1. razred, B varijanta]
Za koje cijele brojeve p jednadžba

$$\frac{1}{(x-4)^2} - \frac{p-1}{16-x^2} = \frac{p}{(x+4)^2}$$

ima jedinstveno cjelobrojno rješenje?

Rješenje. Uz uvjet da je $x \neq 4$ i $x \neq -4$, nakon množenja dane jednadžbe s $(x+4)^2(x-4)^2$ dobivamo:

$$\begin{aligned}
(x+4)^2 + (p-1)(x+4)(x-4) &= p(x-4)^2, \\
x^2 + 8x + 16 + (p-1)(x^2-16) &= p(x^2 - 8x + 16), \\
x^2 + 8x + 16 + px^2 - 16p - x^2 + 16 &= px^2 - 8px + 16p, \\
8x + 32 - 16p &= -8px + 16p, \\
8x(p+1) &= 32p - 32, \\
x(p+1) &= 4p - 4.
\end{aligned}$$

Očito $p = -1$ nije rješenje. Stoga je $p \neq -1$ i

$$x = \frac{4p-4}{p+1}.$$

Otuda dobivamo

$$x = \frac{4p-4}{p+1} = \frac{4p+4-8}{p+1} = 4 - \frac{8}{p+1}.$$

Da bi rješenje x bilo cjelobrojno, $p+1$ mora dijeliti broj 8. Tada je $p+1 \in \{\pm 1, \pm 2, \pm 4, \pm 8\}$, odnosno $p \in \{-9, -5, -3, -2, 0, 1, 3, 7\}$. Zbog početnog uvjeta $x \neq 4$ i $x \neq -4$, p ne smije biti jednak 0. Konačno dobivamo $p \in \{-9, -5, -3, -2, 1, 3, 7\}$. ■

Osnovna metoda ispitivanja djeljivosti, konkretno ispitivanja relacije $a \mid b$ za $a, b \in \mathbb{Z}$, sastoji se u tome da broj b zapišemo kao umnožak ax za neki $x \in \mathbb{Z}$. U nekim osnovnim problemima, ovaj način faktorizacije može se dobiti iz nekih osnovnih algebarskih faktorizacija poput kvadrata binoma, kvadrata razlike itd. Posebno se korisnima pokazuju i sljedeće dvije formule faktorizacije razlike, odnosno zbroja n-tih potencija. Ako je n pozitivan cijeli broj, onda vrijedi

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}). \tag{1.6}$$

Ako je n pozitivan neparan broj, onda je

$$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}). \tag{1.7}$$

Primjer 1.1.16. [2014., Općinsko/Školsko, 1. razred, A varijanta]
Dokaži da je broj $2012^9 + 2016^9$ *djeljiv s* 2014.

Rješenje. Koristeći prethodnu formulu (1.7) imamo da je

$$2012^9+2016^9 = (2012+2016)(2012^8-2012^7\cdot 2016+2012^6\cdot 2016^2-\cdots-2012\cdot 2016^7+2016^8).$$

Odavde zaključujemo da $2012+2016 \mid 2012^9+2016^9$. Budući da je $2012+2016 = 4028 = 2 \cdot 2014$ zaključujemo da $2014 \mid 2012^9 + 2016^9$. ■

Mogli smo riješiti primjer i na sljedeći način.

Rješenje. Koristimo faktorizaciju

$$m^3 + n^3 = (m + n)(m^2 - mn + n^2).$$

Iz nje zaključujemo da, ako su m i n cijeli brojevi, onda $m + n \mid m^3 + n^3$. Također, $m^3 + n^3 \mid m^9 + n^9$, pa vrijedi i $m + n \mid m^9 + n^9$. Dakle, $2012 + 2016 \mid 2012^9 + 2016^9$. Budući da je $2012 + 2016 = 4028 = 2 \cdot 2014$ zaključujemo da $2014 \mid 2012^9 + 2016^9$. ■

Primjer 1.1.17. [2012., Županijsko, 1. razred, B varijanta]
Dokažite da je broj $100\ldots01$ *koji ima točno* 2012 *nula složen.*

Rješenje. Zapišimo zadani broj na drugačiji način:

$$100\ldots01 = 10^{2013} + 1 = (10^{671})^3 + 1.$$

Primjenom formule (1.7) imamo:

$$(10^{671})^3 + 1 = (10^{671} + 1)(10^{1342} - 10^{671} + 1).$$

Dakle, $100\ldots01 = (10^{671} + 1)(10^{1342} - 10^{671} + 1)$, a to je složen broj. ■

Primjer 1.1.18. [2015., Državno natjecanje, 1. razred, A varijanta]
Dokaži da ne postoji prirodni broj n takav da $6^n - 1$ *dijeli* $7^n - 1$.

Rješenje. Budući da $6^n - 1$ dijeli $7^n - 1$ slijedi da $6 - 1 = 5$ dijeli $7^n - 1$. Zadnja znamenka potencije 7^n za $n \in \mathbb{N}$ može biti redom 7,9,3,1,7,... pa će broj $7^n - 1$ biti djeljiv s 5 ako i samo ako je $n = 4k$ za neki $k \in \mathbb{N}$.

Sada ispitujemo za koje $k \in \mathbb{N}$ broj $6^{4k} - 1$ dijeli $7^{4k} - 1$. Budući je

$$6^{4k} - 1 = (6^{2k} - 1)(6^{2k} + 1) = (36^k - 1)(6^{2k} + 1) = 35 \cdot m,$$

za neki $m \in \mathbb{N}$, slijedi da $35 \mid 7^{4k} - 1$, tj. $7 \mid 7^{4k} - 1$ što je nemoguće. ■

1.2 Najveći zajednički djelitelj. Najmanji zajednički višekratnik

Definicija 1.2.1. *Neka su b i c cijeli brojevi koji nisu oba jednaka nuli. 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 mnogo zajedničkih djelitelja od b i c. Najveći među njima zove se* ***najveći zajednički djelitelj*** *od b i c i označava se s* $\text{nzd}(b, c)$.

Za proizvoljan $n \in \mathbb{N}$, *analogno se definira najveći zajednički djelitelj cijelih brojeva* $b_1, b_2, \ldots, b_n$ *koji nisu svi jednaki nuli, te se označava s* $\text{nzd}(b_1, b_2, \ldots, b_n)$.

Iz definicije najvećeg zajedničkog djelitelja slijedi nekoliko jednostavnih svojstava.

Propozicija 1.2.2. *Za* $a, b \in \mathbb{Z}$ *vrijedi:*

(1) $\text{nzd}(a, b) \in \mathbb{N}$,

(2) $\text{nzd}(\pm a, \pm b) = \text{nzd}(a, b)$,

(3) $\text{nzd}(a, b) = \text{nzd}(b, a)$,

(4) $\text{nzd}(a, b + ax) = \text{nzd}(a, b)$, *za sve* $x \in \mathbb{Z}$.

Definicija 1.2.3. *Reći ćemo da su cijeli brojevi a i b* ***relativno prosti*** *ako je* $\text{nzd}(a, b) = 1$. *Analogno, za konačno mnogo cijelih brojeva* $a_1, a_2, \ldots, a_n$ *reći ćemo da su* ***relativno prosti*** *ako je* $\text{nzd}(a_1, a_2, \ldots, a_n) = 1$, *a da su u* ***parovima relativno prosti*** *ako je* $\text{nzd}(a_i, a_j) = 1$ *za sve* $1 \leq i < j \leq n$.

Očito je da ako su $a_1, a_2, \ldots, a_n$ u parovima relativno prosti, onda je i $\text{nzd}(a_1, a_2, \ldots, a_n) = 1$. Obrat ne vrijedi. Na primjer, $\text{nzd}(10, 12, 15) = 1$, ali $\text{nzd}(10, 12) = 2$, $\text{nzd}(10, 15) = 5$ i $\text{nzd}(12, 15) = 3$.

Propozicija 1.2.4. *Za $b, c \in \mathbb{Z}$ vrijedi:*

$$\text{nzd}(b, c) = \min(\{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Dokaz. Neka je $g = \text{nzd}(b, c)$, te neka je l najmanji pozitivni član skupa $S = \{bx + cy : x, y \in \mathbb{Z}\}$. To znači da postoje cijeli brojevi x_0 i y_0 takvi da je $l = bx_0 + cy_0$.

Pokažimo da $l \mid b$ i $l \mid c$. Pretpostavimo da npr. $l \nmid b$. Tada po Teoremu 1.1.4 postoje cijeli brojevi q i r takvi da je $b = lq + r$ i $0 < r < l$. Sada je

$$r = b - lq = b - q(bx_0 + cy_0) = b(1 - qx_0) + c(-qy_0) \in S,$$

što je u suprotnosti s minimalnošću od l. Dakle, $l \mid b$, a na isti način se pokazuje da $l \mid c$. To znači da je $l \leq g$.

Budući da je $g = \text{nzd}(b, c)$, to postoje $\beta, \gamma \in \mathbb{Z}$ takvi da je $b = g\beta$ i $c = g\gamma$, pa je $l = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0)$. Odavde slijedi da je $g \leq l$ pa smo dokazali da je $g = l$. □

Prema Propoziciji 1.2.4 slijedi da za cijele brojeve a i b postoje $x, y \in \mathbb{Z}$ takvi da je

$$ax + by = \text{nzd}(a, b). \tag{1.8}$$

Prethodna relacija naziva se *Bezoutov identitet*. Posebno, ako se cijeli broj c može prikazati u obliku $c = ax + by$, onda je $\text{nzd}(a, b)$ djelitelj od c. Stoga, ako je

$$ax + by = 1,$$

onda je $\text{nzd}(a, b) = 1$.

Iz prethodnog identiteta (1.8) mogu se dokazati sljedeća svojstva:

Propozicija 1.2.5. *Ako je p prost broj i $p \mid ab$, onda $p \mid a$ ili $p \mid b$.*

Dokaz. Pretpostavimo da $p \nmid a$. Onda je $\text{nzd}(p, a) = 1$ pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$. Pomnožimo li jednakost s b dobivamo

$$axb + pyb = b.$$

Budući da $p \mid ab$ slijedi da $p \mid axb$ i $p \mid pyb$ pa zaključujemo da $p \mid b$. □

Propozicija 1.2.6. *Neka su $a, b, c, m \in \mathbb{Z}$ takvi da sljedeće tvrdnje imaju smisla.*

(1) Ako $m \mid a$ i $m \mid b$, onda $m \mid \text{nzd}(a, b)$.

(2) Ako je $m > 0$, onda je $\text{nzd}(ma, mb) = m\,\text{nzd}(a, b)$.

(3) Ako je $\text{nzd}(a, m) = \text{nzd}(b, m) = 1$, onda je $\text{nzd}(ab, m) = 1$.

(4) Ako $b \mid ac$ *i* $\text{nzd}(b, c) = 1$*, onda* $b \mid a$*.*

Sada ćemo definirati najmanji zajednički višekratnik.

Definicija 1.2.7. *Neka su a i b dva cijela broja ne oba nula. Broj koji je višekratnik i od a i od b zove se* ***zajednički višekratnik*** *brojeva a i b.*

Neka su a i b cijeli brojevi različiti od nule. Najmanji prirodan broj c za koji vrijedi da je višekratnik i od a i od b tj. za koji vrijedi da $a \mid c$ *i* $b \mid c$ *zove se* ***najmanji zajednički višekratnik*** *brojeva a i b i označava s* $\text{nzv}(a, b)$*. Slično definiramo najmanji zajednički višekratnik više cijelih brojeva,* $a_1, a_2, \ldots, a_n$ *različitih od nule i označavamo s* $\text{nzv}(a_1, a_2, \ldots, a_n)$*.*

Očito, postoji beskonačno mnogo zajedničkih višekratnika od a i b. Slijedi nekoliko glavnih svojstava najmanjeg zajedničkog višekratnika.

Propozicija 1.2.8. *Neka su a i b cijeli brojevi različiti od nule.*

(1) Najmanji zajednički višekratnik od a i b dijeli svaki zajednički višekratnik od a i b.

(2) Najveći zajednički djelitelj i najmanji zajednički višekratnik od a i b zadovoljavaju sljedeću jednakost:

$$\text{nzd}(a, b) \cdot \text{nzv}(a, b) = |ab| .$$

Primjenom Teorema 1.1.10 u Propoziciji 1.2.8.(2), brojeve a i b zapisujemo kao

$$a = \prod_p p^{\alpha(p)}, \; b = \prod_p p^{\beta(p)},$$

gdje su $\alpha(p) \geq 0, \beta(p) \geq 0$. Sada prema (1.2) imamo da je

$$\text{nzd}(a, b) = \prod_p p^{\min(\alpha(p),\beta(p))}, \; \text{nzv}(a, b) = \prod_p p^{\max(\alpha(p),\beta(p))}.$$

Otuda slijedi

$$\text{nzd}(a, b) \cdot \text{nzv}(a, b) = \prod_p p^{\min(\alpha(p),\beta(p))} \cdot \prod_p p^{\max(\alpha(p),\beta(p))} = \prod_p p^{\min(\alpha(p),\beta(p))+\max(\alpha(p),\beta(p))}.$$

Kako je $\min(\alpha(p), \beta(p)) + \max(\alpha(p), \beta(p)) = \alpha(p) + \beta(p)$, dobivamo

$$\text{nzd}(a, b) = \prod_p p^{\alpha(p)+\beta(p)} = |ab| .$$

Time smo dokazali svojstvo (2) iz Propozicije 1.2.8.

Uočimo da u slučaju kada imamo više od dva broja, prethodno svojstvo ne vrijedi.

Propozicija 1.2.9. *Ako su cijeli brojevi $a_1, a_2, \ldots, a_k$ u parovima relativno prosti, onda vrijedi:*

$$\text{nzv}(a_1, a_2, \ldots, a_k) = |a_1 a_2 \cdots a_k|.$$

Dokaz. Neka je

$$|a_1| = \prod_p p^{\alpha_1(p)},\ |a_2| = \prod_p p^{\alpha_2(p)},\ \ldots,\ |a_k| = \prod_p p^{\alpha_k(p)},$$

gdje su $\alpha_1(p), \alpha_2(p), \ldots, \alpha_k(p) \geq 0$. Sada je

$$\text{nzv}(a_1, a_2, \ldots, a_k) = \prod_p p^{\max(\alpha_1(p), \alpha_2(p), \ldots, \alpha_k(p))}.$$

Budući da su $a_1, a_2, \ldots, a_k$ u parovima relativno prosti slijedi da je za svaki prost broj p ili $\alpha_1(p) = \alpha_2(p) = \ldots = \alpha_k(p) = 0$ ili je točno jedan od $\alpha_1(p), \alpha_2(p), \ldots, \alpha_k(p)$ različit od nule. Stoga je

$$\text{nzv}(a_1, a_2, \ldots, a_k) = \prod_p p^{\alpha_1(p)+\alpha_2(p)+\ldots+\alpha_k(p)} = \prod_p p^{\alpha_1(p)} \cdot \prod_p p^{\alpha_2(p)} \cdots \prod_p p^{\alpha_k(p)} = |a_1 \cdot a_2 \cdots a_k|.$$

□

Iz Propozicije 1.2.9 i Propozicije 1.2.8 (1) znamo da ako $a_1 \mid d$, $a_2 \mid d$, ..., $a_k \mid d$ i $a_1, a_2, \ldots, a_k$ su u parovima relativno prosti, onda $a_1 a_2 \cdots a_k \mid d$.

Primjer 1.2.10. [2016., Općinsko/Školsko, 6. razred]
Umnožak dva prirodna broja je 68040*, a njihov najmanji zajednički višekratnik* 3780*. Odredi te brojeve.*

Rješenje. Neka su a i b traženi brojevi i $a < b$. Tada je $a \cdot b = 68040$ i $\text{nzv}(a, b) = 3780$. Znamo da vrijedi $\text{nzd}(a, b) \cdot \text{nzv}(a, b) = |ab|$ pa slijedi

$$\text{nzd}(a, b) = \frac{|68040|}{\text{nzv}(a, b)} = \frac{68040}{3780} = 18.$$

Kako je $18 = 2 \cdot 3 \cdot 3$ i $3780 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7$ postoje sljedeće mogućnosti:

a	b
$2 \cdot 3 \cdot 3$	$2 \cdot 3 \cdot 3 \cdot 2 \cdot 3 \cdot 5 \cdot 7$
$2 \cdot 3 \cdot 3 \cdot 2$	$2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 \cdot 7$
$2 \cdot 3 \cdot 3 \cdot 3$	$2 \cdot 3 \cdot 3 \cdot 2 \cdot 5 \cdot 7$
$2 \cdot 3 \cdot 3 \cdot 5$	$2 \cdot 3 \cdot 3 \cdot 2 \cdot 3 \cdot 7$
$2 \cdot 3 \cdot 3 \cdot 7$	$2 \cdot 3 \cdot 3 \cdot 2 \cdot 3 \cdot 5$
$2 \cdot 3 \cdot 3 \cdot 2 \cdot 3$	$2 \cdot 3 \cdot 3 \cdot 5 \cdot 7$
$2 \cdot 3 \cdot 3 \cdot 2 \cdot 5$	$2 \cdot 3 \cdot 3 \cdot 3 \cdot 7$
$2 \cdot 3 \cdot 3 \cdot 2 \cdot 7$	$2 \cdot 3 \cdot 3 \cdot 3 \cdot 5$

Traženi brojevi su:

a	b
18	3780
36	1890
54	1260
90	756
126	540
108	630
180	378
252	270

■

Zadatak možemo riješiti i na drugi način.

Rješenje. Neka su a i b traženi brojevi i $a < b$. Tada je $a \cdot b = 68040$ i $\text{nzv}(a, b) = 3780$. Znamo da vrijedi $\text{nzd}(a, b) \cdot \text{nzv}(a, b) = |ab|$ pa slijedi $\text{nzd}(a, b) = 68040 : 3780 = 18$. Tada je $a = 18x$ i $b = 18y$ za neke $x, y \in \mathbb{N}$, $\text{nzd}(x, y) = 1$ i $x < y$. Sada imamo:

$$18x \cdot 18y = 68040 \;\Leftrightarrow\; 324xy = 68040 \;\Leftrightarrow x \cdot y = 210.$$

Kako 210 možemo napisati kao

$$210 = 1 \cdot 210 = 2 \cdot 105 = 3 \cdot 70 = 5 \cdot 42 = 6 \cdot 35 = 7 \cdot 30 = 10 \cdot 21 = 14 \cdot 15,$$

slijedi da je

$$(x, y) \in \{(1, 210), (2, 105), (3, 70), (5, 42), (6, 35), (7, 30), (10, 21), (14, 15)\}.$$

Dakle, traženi brojevi su

$$(a, b) \in \{(18, 3780), (36, 1890), (54, 1260), (90, 756), (108, 630), (126, 540), (180, 378), (252, 270)\}.$$

■

Primjer 1.2.11. [1986., USAMO]
Postoji li 14 *uzastopnih cijelih brojeva od kojih je svaki djeljiv s jednim ili više prostih brojeva* p *iz intervala* $2 \leq p \leq 11$*?*

Rješenje. Prvo, uočimo da za bilo kojih 14 uzastopnih pozitivnih cijelih brojeva, točno 7 je parnih (djeljivih s 2) i stoga zadovoljavaju kriterij. Dakle, problem možemo pojednostaviti na sljedeće pitanje, ekvivalentno početnom: "Postoji li 7 uzastopnih pozitivnih neparnih cijelih brojeva od kojih je svaki djeljiv s jednim ili više prostih brojeva p iz intervala $3 \leq p \leq 11$?"

Među uzastopnih 7 pozitivnih neparnih cijelih brojeva vrijedi:

- 2 ili 3 djeljiva su s 3,
- 1 ili 2 djeljiva su s 5,
- točno 1 je djeljiv sa 7,
- 0 ili 1 djeljiva su s 11.

Da bi svaki od tih 7 brojeva bio djeljiv s $3, 5, 7$ ili 11, među njima mora biti 3 višekratnika broja 3, 2 višekratnika broja 5, 1 višekratnik broja 7 i 1 višekratnik broja 11. Dodatno, niti jedan od tih brojeva ne smije biti višekratnik od nikoja dva od prethodno spomenuta četiri prosta broja. Neka su $a_1, a_2, a_3, \ldots, a_7$ uzastopni pozitivni neparni cijeli brojevi. Tada a_1, a_4 i a_7 moraju biti višekratnici broja 3 te stoga ne mogu biti višekratnici brojeva 5, 7, ili 11. No, ako postoje dva višekratnika broja 5, moraju biti jedan od dva para (a_1, a_6) i (a_2, a_7). Međutim, svaki od tih parova sadrži višekratnik broja 3 te stoga barem jedan od 7 uzastopnih pozitivnih neparnih cijelih brojeva nije djeljiv niti s jednim od prostih brojeva 3, 5, 7 ili 11. Dakle, odgovor je ne. ■

Primjer 1.2.12. [2005., AIME]
Koliko ima prirodnih brojeva koji su djelitelji barem jednog od brojeva 10^{10}, 15^7, 18^{11}*?*

Rješenje. Rastavom brojeva na proste faktore dobivamo:

$$10^{10} = 2^{10} \cdot 5^{10}$$

$$15^7 = 3^7 \cdot 5^7$$

$$18^{11} = 2^{11} \cdot 3^{22}$$

Prema (1.3) slijedi da broj:

- 10^{10} ima $(10 + 1)(10 + 1) = 11 \cdot 11 = 121$ djelitelj,
- 15^7 ima $(7 + 1)(7 + 1) = 8 \cdot 8 = 64$ djelitelja,
- 18^{11} ima $(11 + 1)(22 + 1) = 12 \cdot 23 = 276$ djelitelja.

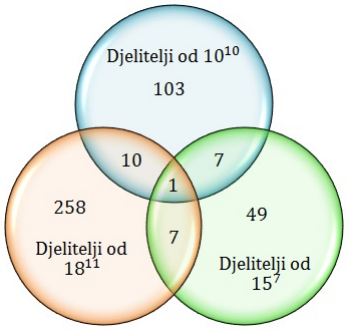
U zbroju 121 + 64 + 276 smo dva puta brojali zajedničke djelitelje dva broja. Stoga moramo oduzeti broj zajedničkih djelitelja od 10^{10} i 15^7, 10^{10} i 18^{11} te 15^7 i 18^{11}. Broj svih zajedničkih djelitelja dva broja jednak je broju djelitelja njihovog najvećeg zajedničkog djelitelja:

- $\text{nzd}(10^{10}, 15^7) = 5^7$ pa 10^{10} i 15^7 imaju točno $7 + 1 = 8$ djelitelja,
- $\text{nzd}(15^7, 18^{11}) = 3^7$ pa 15^7 i 18^{11} imaju točno $7 + 1 = 8$ djelitelja,
- $\text{nzd}(10^{10}, 18^{11}) = 2^{10}$ pa 10^{10} i 18^{11} imaju točno $10 + 1 = 11$ djelitelja.

Stoga je broj "potencijalnih" djelitelja jednak $121 + 64 + 276 - 8 - 8 - 11$. Uočimo da smo u zbroju djelitelja pojedinačnih brojeva ($121 + 64 + 276$) i zbroju djelitelja parova brojeva ($8 + 8 + 11$) tri puta prebrojali zajedničke djelitelje sva tri broja, pa taj broj moramo pribrojiti. Srećom, vidimo da je jedini broj koji je djelitelj sva tri broja broj 1 pa konačno dobivamo da je broj djelitelja barem jednog od brojeva 10^{10}, 15^7, 18^{11} jednak:

$$121 + 64 + 276 - 8 - 8 - 11 + 1 = 435.$$

Ustanovimo da smo zadatak zapravo riješili pomoću *formule uključivanja i isključivanja* (tj. FUI). Zorno ga možemo prikazati Vennovim dijagramom (Slika 1.1). ■



Slika 1.1: Vennov dijagram

Sljedeći teorem služi nam kako bismo pronašli najveći zajednički djelitelj brojeva. U njemu je opisan *Euklidov algoritam* jedan je od najstarijih, ali ujedno i jedan od najvažnijih algoritama u teoriji brojeva.

Teorem 1.2.13 (Euklidov algoritam)**.** *Neka su b i $c > 0$ cijeli brojevi. Pretpostavimo da je uzastopnom primjenom Teorema 1.1.4 dobiven niz jednakosti*

$$\begin{aligned} b &= cq_1 + r_1, 0 < r_1 < c, \\ c &= r_1q_2 + r_2, 0 < r_2 < r_1, \\ r_1 &= r_2q_3 + r_3, 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1}q_j + r_j, 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_jq_{j+1}. \end{aligned}$$

Tada je $\text{nzd}(b, c)$ *jednak r_j, posljednjem ostatku različitom od nule. Vrijednosti od x_0 i y_0 u izrazu* $\text{nzd}(b, c) = bx_0 + cy_0$ *mogu se dobiti izražavanjem svakog ostatka r_i kao linearne kombinacije od b i c.*

Dokaz. Koristeći svojstvo (4) iz Propozicije 1.2.2 najvećeg zajedničkog djelitelja imamo

$$\begin{aligned} \text{nzd}(b, c) &= \text{nzd}(b - cq_1, c) = \text{nzd}(r_1, c) \\ &= \text{nzd}(r_1, c - r_1q_2) = \text{nzd}(r_1, r_2) \\ &= \text{nzd}(r_1 - r_2q_3, r_2) = \text{nzd}(r_3, r_2). \end{aligned}$$

Nastavljajući ovaj proces dobivamo: $\text{nzd}(b, c) = \text{nzd}(r_{j-1}, r_j) = \text{nzd}(r_j, 0) = r_j$.

Indukcijom ćemo dokazati da je svaki r_i linearna kombinacija od b i c. To je točno za r_1 i r_2, pa pretpostavimo da vrijedi za r_{i-1} i r_{i-2}. Budući da je r_i linearna kombinacija od r_{i-1} i r_{i-2}, po pretpostavci indukcije dobivamo da je i linearna kombinacija od b i c. □

Primjetimo da ako $\text{nzd}(a, b) \mid a$ i $\text{nzd}(a, b) \mid b$ onda $\text{nzd}(a, b) \mid ax + by$, za sve $x, y \in \mathbb{Z}$. Rješenja jednadžbe $bx + cy = \text{nzd}(b, c)$ mogu se efikasno dobiti na sljedeći način: ako je

$$r_{-1} = b, \quad r_0 = c, \quad r_i = r_{i-2} - q_ir_{i-1};$$

$$x_{-1} = 1, \quad x_0 = 0, \quad x_i = x_{i-2} - q_ix_{i-1};$$

$$y_{-1} = 0, \quad y_0 = 1, \quad y_i = y_{i-2} - q_iy_{i-1};$$

onda je

$$bx_i + cy_i = r_i, \text{ za } i = -1, 0, 1, \dots, j + 1.$$

Ova formula je točna za $i = -1$ i $i = 0$, pa tvrdnja trivijalno slijedi indukcijom, jer obje strane formule zadovoljavaju istu rekurzivnu relaciju. Posebno, vrijedi:

$$bx_j + cy_j = \text{nzd}(b, c).$$

Verzija Euklidovog algoritma koja računa, ne samo nzd(b, c), već i cijele brojeve x i y takve da je $bx + cy = \text{nzd}(b, c)$ naziva se *prošireni Euklidov algoritam.*

Na primjer, odredimo $g = \text{nzd}(423, 198)$ i nađimo cijele brojeve x, y takve da je $423x + 198y = g$. Primjenom Euklidovog algoritma imamo:

$$\begin{aligned} 423 &= 198 \cdot 2 + 27 \\ 198 &= 27 \cdot 7 + 9 \\ 27 &= 9 \cdot 3 \end{aligned}$$

Dakle, $g = \text{nzd}(423, 198) = 9$. Primjenom proširenog Euklidovog algoritma odredimo cijele brojeve x, y takve da je $423x + 198y = 9$. U tu svrhu koristimo tablicu:

i	-1	0	1	2
q_i			2	7
x_i	1	0	1	-7
y_i	0	1	-2	15

Dakle, $x = -7$ i $y = 15$ tj. $423 \cdot (-7) + 198 \cdot 15 = 9$.

Primjer 1.2.14. [1986., AIME]
Odredi najveći prirodan broj n za koji je $n^3 + 100$ *djeljivo s* $n + 10$*.*

Rješenje. Ako $n + 10 \mid n^3 + 100$ onda je $\text{nzd}(n^3 + 100, n + 10) = n + 10$. Primjenom Euklidovog algoritma (1.2.13) dobivamo:

$$\text{nzd}(n^3+100, n+10) = \text{nzd}(-10n^2+100, n+10) = \text{nzd}(100n+100, n+10) = \text{nzd}(-900, n+10).$$

Dakle, $n + 10 \mid 900$. Najveći prirodan broj za koji $n + 10$ dijeli 900 je 890. ■

1.3 Najveće cijelo

Definicija 1.3.1. *Neka je x realan broj. Najveći cijeli broj koji nije veći od x označavamo sa* $\lfloor x \rfloor$ *i zovemo* ***najveće cijelo*** *od x. Sa* $\{x\} = x - \lfloor x \rfloor$ *označavamo* razlomljeni dio od x*.*

Na primjer, za $x = 5.25$ je $\lfloor 5.25 \rfloor = 5$ i $\{5.25\} = 0.25$, za $x = -4.5$ je $\lfloor -4.5 \rfloor = -5$, a $\{-4.5\} = 0.5$.

Primjer 1.3.2. [2016., Županijsko natjecanje, 4. razred, B varijanta]
Za broj kažemo da je naizgled–prost *broj ako je složen, ali nije djeljiv s* 2*,* 3 *ili* 5*. Tri najmanja naizgled–prosta broja su* 49*,* 77 *i* 91*. Postoji* 168 *prostih brojeva koji su manji od* 1000*. Koliko je naizgled–prostih brojeva koji su manji od* 1000*?*

Rješenje. Brojeva manjih od 1000 koji su djeljivi s:

- 2 ima $\left\lfloor \frac{999}{2} \right\rfloor = 499$,
- 3 ima $\left\lfloor \frac{999}{3} \right\rfloor = 333$,
- 5 ima $\left\lfloor \frac{999}{5} \right\rfloor = 199$,
- 6 ima $\left\lfloor \frac{999}{6} \right\rfloor = 166$,
- 10 ima $\left\lfloor \frac{999}{10} \right\rfloor = 99$,
- 15 ima $\left\lfloor \frac{999}{15} \right\rfloor = 66$,
- 30 ima $\left\lfloor \frac{999}{30} \right\rfloor = 33$.

Prema FUI ukupan broj brojeva manjih od 1000 koji su djeljivi s 2 ili s 3 ili s 5 je:

$$499 + 333 + 199 - 166 - 99 - 66 + 33 = 733.$$

Ostalih brojeva ima $999 - 733 = 266$. Među njima su svi prosti brojevi manji od 1000 osim brojeva 2, 3 i 5, ukupno njih $168 - 3 = 165$. Među preostalim brojevima je i broj 1 koji nije ni prost ni složen. Stoga je ukupan broj naizgled-prostih brojeva koju su manji od 1000 jednak

$$266 - 165 - 1 = 100.$$

■

Teorem 1.3.3. *Potencija s kojom zadani prosti broj p ulazi u rastav broja $n!$ na proste faktore jednak je*

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

Dokaz. U produktu $n! = 1 \cdot 2 \cdot 3 \cdots n$ ima $\lfloor \frac{n}{p} \rfloor$ faktora koji su višekratnici od p. Među njima je $\lfloor \frac{n}{p^2} \rfloor$ onih koji su višekratnici od p^2, $\lfloor \frac{n}{p^3} \rfloor$ onih koji su višekratnici od p^3, itd. Primijetimo da je u sumi $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$ svaki faktor koji je višekratnik od p^m, ali nije od p^{m+1}, brojen točno m puta: kao višekranik od $p, p^2, \ldots, p^m$. Primijetimo također da je ta suma konačna, jer za dovoljno velik j vrijedi $p^j > n$, pa je $\lfloor \frac{n}{p^j} \rfloor = \lfloor \frac{n}{p^{j+1}} \rfloor = \cdots = 0$. □

Primjer 1.3.4. [2016., Županijsko natjecanje, 1. razred, B varijanta]
S koliko nula završava broj koji se dobije množenjem prvih 2016 *prirodnih brojeva?*

Rješenje. Treba izračunati s koliko nula završava broj

$$1 \cdot 2 \cdot 3 \cdot 4 \cdots 2015 \cdot 2016 = 2016!.$$

Nula se dobije umnoškom $2 \cdot 5$, odnosno ako se množi višekratnik broja 2 s višekratnikom broja 5. Očito je višekratnika broja 5 manje nego višekratnika broja 2. Broj nula u danom umnošku jednak je eksponentu najveće potencije broja 5 kojom je djeljiv dani umnožak. Dakle, treba prebrojiti višekratnike brojeva 5, 5^2, 5^3 i 5^4 (jer je $5^5 > 2016$). Prema Teoremu 1.3.3 slijedi da je eksponent najveće potencije broja 5 koja se javlja u umnošku $1 \cdot 2 \cdot 3 \cdot 4 \cdots 2015 \cdot 2016$ jednak:

$$\left\lfloor \frac{2016}{5} \right\rfloor + \left\lfloor \frac{2016}{25} \right\rfloor + \left\lfloor \frac{2016}{125} \right\rfloor + \left\lfloor \frac{2016}{625} \right\rfloor = 403 + 80 + 16 + 3 = 502.$$

Dakle, dani umnožak završava s 502 nule. ■

Poglavlje 2

Kongruencije

2.1 Kongruencije

Kongruencije predstavljaju važan koncept u teoriji brojeva i šire. Uveo ih je Carl Friedrich Gauss (1777-1855), jedan od najvećih matematičara svih vremena.

Definicija 2.1.1. *Ako prirodan broj n dijeli razliku $a-b$, onda kažemo da je a* ***kongruentan*** *b* ***modulo*** *n i pišemo*

$$a \equiv b \pmod{n}.$$

U protivnom, kažemo da a ***nije kongruentan*** *b modulo n i pišemo* $a \not\equiv b \pmod{n}$.

Iz same definicije je jasno da je a kongruentno b modulo n ako i samo ako postoji $k \in \mathbb{Z}$ takav da je $nk = a - b$, odnosno ako i samo ako a i b daju isti ostatak pri dijeljenju s n. Sljedeća propozcija nam kaže da je relacija "biti kongruentan modulo n" relacija ekvivalencije na skupu $\mathbb{Z}$.

Propozicija 2.1.2. *Neka je* $n \in \mathbb{N}$.

(1) Relacija biti kongruentan modulo n je refleksivna*, to jest* $a \equiv a \pmod{n}$*, za sve* $a \in \mathbb{Z}$.

(2) Relacija biti kongruentan modulo n je simetrična*, to jest ako je* $a \equiv b \pmod{n}$ *onda je i* $b \equiv a \pmod{n}$*, za sve* $a, b \in \mathbb{Z}$.

(3) Relacija biti kongruentan modulo n je tranzitivna*, to jest ako je* $a \equiv b \pmod{n}$ *i* $b \equiv c \pmod{n}$ *onda je* $a \equiv c \pmod{n}$*, za sve* $a, b, c \in \mathbb{Z}$.

U onom što slijedi navest ćemo neka osnovna svojstva kongruencija koja se uglavnom lako pokazuju iz same definicije.

Propozicija 2.1.3. *Za $a, b, c, d \in \mathbb{Z}$ i $n \in \mathbb{N}$ vrijedi:*

(1) Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$ onda je $a \pm c \equiv b \pm d \pmod{n}$.

(2) Ako $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$ onda je $ac \equiv bd \pmod{n}$.

Uzastopnom primjenom svojstava (1) i (2) iz prethodne propozicije slijedi:

Korolar 2.1.4. *Neka je f polinom s cjelobrojnim koeficijentima, te $a, b \in \mathbb{Z}$ i $n \in \mathbb{N}$. Ako je $a \equiv b \pmod{n}$, onda je $f(a) \equiv f(b) \pmod{n}$.*

Primjer 2.1.5. [2012., Općinsko/Školsko natjecanje, 8. razred]
Odredi sve prirodne brojeve n za koje je $10^n + 5$ djeljivo s 15.

Rješenje. Kako je $15 = 3 \cdot 5$, onda broj $10^n + 5$ treba biti djeljiv i s 3 i s 5. Broj 10^n u dekadskom zapisu ima jednu 1 i n nula pa je zbroj znamenaka broja $10^n + 5$ uvijek 6. Prema tome, broj $10^n + 5$ je djeljiv s 3 za svaki prirodni broj n. Nadalje, znamenka jedinica broja $10^n + 5$ je uvijek 5 što znači da je taj broj djeljiv s 5 za svaki prirodni broj n. Dakle, broj $10^n + 5$ je djeljiv s 15 za svaki prirodni broj n. ■

Rješenje. [2. način] Vrijedi

$$10^n + 5 \equiv 0 \pmod{5}, \; 10^n + 5 \equiv 1 + 2 \equiv 0 \pmod{3},$$

pa je $10^n + 5 \equiv 0 \pmod{15}$ za sve $n \in \mathbb{N}$. ■

Propozicija 2.1.6. *Neka je $a, b, c \in \mathbb{Z}$ i $n \in \mathbb{N}$. Ekvivalentno je*

1. $ac \equiv bc \pmod{n}$,
2. $a \equiv b \pmod{\frac{n}{\text{nzd}(n,c)}}$.

Iz Propozicijue 2.1.6 slijedi da ako je $\text{nzd}(c, n) = 1$ onda kongruenciju $ac \equiv bc \pmod{n}$ možemo "kratiti" s brojem c bez da se modul promijeni, to jest slijedi da je $a \equiv b \pmod{n}$.

Propozicija 2.1.7. *(1) Ako je $a \equiv b \pmod{n}$ i $d \mid n$ onda je $a \equiv b \pmod{d}$.*

(2) Ako je $a \equiv b \pmod{n}$ i $d \neq 0$, onda je $da \equiv db \pmod{dn}$.

(3) Ako je $a \equiv b \pmod{n_i}$, $i = 1, 2, \ldots, k$, onda je $a \equiv b \pmod{\text{nzv}(n_1, n_2, \ldots, n_k)}$.

Uočimo da u svojstvu (3) Propozicije 2.1.7 ako su $n_1, n_2, \ldots, n_k$ u parovima relativno prosti, onda je $a \equiv b \pmod{n_1 n_2 \cdots n_k}$.

Primjer 2.1.8. [1987., Republičko (državno) natjecanje, 1. razred]
Neka je n prirodan broj. Dokažite da je najveći zajednički djelitelj brojeva n^2+1 i $(n+1)^2+1$ ili 1 ili 5, te dokažite da je jednak 5 ako i samo ako je $n \equiv 2 \pmod 5$.

Rješenje. Neka je $d = \text{nzd}(n^2+1, (n+1)^2+1)$. Tada d dijeli broj

$$((n+1)^2+1) - (n^2+1) = 2n+1,$$

te broj

$$n(2n+1) - 2(n^2+1) = n-2.$$

Prema tome, d dijeli

$$(2n+1) - 2(n-2) = 5,$$

pa je $d \in \{1, 5\}$.

Ako broj n daje ostatke $0, 1, 2, 3, 4$ pri dijeljenju s 5, onda broj n^2+1 daje ostatke redom $1, 2, 0, 0, 2$, a $(n+1)^2+1$ ostatke redom $2, 0, 0, 2, 1$. Prema tome, brojevi n^2+1 i $(n+1)^2+1$ istovremeno su djeljivi s 5 ako i samo ako je $n \equiv 2 \pmod 5$. ■

Primjer 2.1.9. [2010., AIME]
Koliki je ostatak pri djeljenju broja $9 \cdot 99 \cdot 999 \cdots \underbrace{99\ldots9}_{9999}$ s brojem 1000?

Rješenje. Uočimo da je

$$999 \equiv 9999 \equiv \cdots \equiv \underbrace{99\ldots9}_{9999} \equiv -1 \pmod{1000}.$$

To je ukupno $999 - 3 + 1 = 997$ brojeva i njihov umnožak je kongruentan $-1 \pmod{1000}$. Stoga, cijeli izraz je kongruentan $(-1) \cdot 9 \cdot 99 = -891 \equiv 109 \pmod{1000}$. Dakle, ostatak pri dijeljenju broja $9 \cdot 99 \cdot 999 \cdots \underbrace{99\ldots9}_{9999}$ s brojem 1000 jednak je 109. ■

Primjer 2.1.10. [2016., Općinsko/Školsko natjecanje, 2. razred, B varijanta]
Dokažite da jednadžba $5x^2 - 4y^2 = 2015$ nema rješenja u skupu cijelih brojeva.

Rješenje. Kako je

$$5x^2 - 4y^2 \equiv x^2 \pmod 4$$

i

$$2015 \equiv 3 \pmod 4,$$

slijedi da je

$$x^2 \equiv 3 \pmod 4$$

što je nemoguće jer je $x^2 \equiv 0$ ili $1 \pmod 4$ za svaki cijeli broj x. ■

Rješenje. [2. način] Ako je x paran broj, lijeva je strana jednakosti parna, a desna neparna pa jednadžba nema rješenja. Ako je x neparan broj, $x = 2k + 1$, $k \in \mathbb{Z}$, tada mora vrijediti

$$5x^2 - 4y^2 = 5(2k + 1)^2 - 4y^2 = 20k^2 + 20k + 5 - 4y^2 = 2015.$$

Dana jednadžba prelazi u jednadžbu

$$20k^2 + 20k - 4y^2 = 2010$$

kojoj je lijeva strana djeljiva s 4, a desna nije. Zato jednadžba nema rješenja u skupu cijelih brojeva.

■

Rješenje. [3. način] Zapišimo danu jednadžbu u sljedećem obliku:

$$5(x^2 - 1) - 4y^2 = 2010.$$

Izraz $4y^2$ je paran pa i $5(x^2 - 1)$ mora biti paran. To znači da je x neparan broj. No, tada su $x^2 - 1$ i $4y^2$ djeljivi s 4, što povlači da i 2010 mora biti djeljiv s 4. Kako to nije točno, početna jednadžba nema rješenja. ■

2.2 Kineski teorem o ostatcima

Prije nego što iskažemo i dokažemo poznati Kineski teorem o ostatcima, ispitat ćemo rješivost linearne kongruencije $ax \equiv b \pmod{m}$ te ukoliko je rješiva opisati skup njenih rješenja.

Teorem 2.2.1. *Neka su a, b cijeli brojevi i m prirodan broj. Kongruencija*

$$ax \equiv b \pmod{m} \tag{2.1}$$

ima rješenja ako i samo ako $d = \text{nzd}(a, m)$ dijeli b. Ako je ovaj uvjet zadovoljen, onda kongruencija (2.1) ima točno d rješenja modulo m.

Iz prethodnog teorema slijedi da ako je p prost broj i a nije djeljiv s p, onda kongruencija $ax \equiv b \pmod{p}$ uvijek ima rješenje i to rješenje je jedinstveno.

Ako $d = \text{nzd}(a, m)$ dijeli b, tada je kongruencija (2.1) ekvivalentna kongruenciji

$$a'x \equiv b' \pmod{m'}$$

gdje je $\text{nzd}(a', m') = 1$. Budući da je $\text{nzd}(a', m') = 1$, prema Bezoutovom identitetu (1.8) slijedi da postoje brojevi $u, v \in \mathbb{Z}$ takvi da je $a'u + m'v = 1$, a u, v se efektivno mogu naći pomoću Euklidovog algoritma. Sada je $a'u \equiv 1 \pmod{m'}$, pa se pokazuje da su sva rješenja kongruencije (2.1)

$$x \equiv ub' \pmod{m'}.$$

Teorem 2.2.2 (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*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots, x \equiv a_r \pmod{m_r} \tag{2.2}$$

ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja sustava kongruencija (2.2) dana s $x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}$.

Dokaz. Neka je $m = m_1 m_2 \cdots m_r$, te neka je $n_j = \frac{m}{m_j}$ za $j = 1, \ldots, r$. Tada je $\text{nzd}(m_j, n_j) = 1$, pa postoji cijeli broj x_j takav da je $n_j x_j \equiv a_j \pmod{m_j}$. Promotrimo broj

$$x_0 = n_1 x_1 + \cdots + n_r x_r.$$

Za njega vrijedi: $x_0 \equiv 0 + \cdots + 0 + n_j x_j + 0 + \cdots + 0 \equiv a_j \pmod{m_j}$. Prema tome, x_0 je rješenje od (2.2).

Ako su sada x, y, dva rješenja od (2.2), onda je $x \equiv y \pmod{m_j}$ za $j = 1, \ldots, r$, pa jer su m_j u parovima relativno prosti, dobivamo da je $x \equiv y \pmod{m}$. □

Napomenimo da prema ovom važnom teoremu slijedi da ako sustav kongruencija (2.2) ima rješenje, tada ih ima beskonačno mnogo, a sva rješenja su međusobno kongruentna modulo produkt zadanih djelitelja.

Primjer 2.2.3. [2012., Županijsko natjecanje, 1. razred, B varijanta]
Odredite sve troznamenkaste prirodne brojeve koji su djeljivi sa 7*, a pri dijeljenju s* 9 *daju ostatak* 5*.*

Rješenje. Treba odrediti sve $x = \overline{abc} = 100a + 10b + c$, $a, b, c \in \{0, 1, \ldots, 9\}$, $a \neq 0$ takve da je

$$x \equiv 0 \pmod{7}, \quad x \equiv 5 \pmod{9}.$$

Prethodni sustav kongruencija ispunjava uvjete Kineskog teorema o ostatcima 2.2.2 i zaključujemo da ima jedinstveno rješenje modulo 63. Sva rješenja druge kongruencija u sustavu nenegatvnih ostataka modulo 63 su

$$5, 14, 23, 32, 41, 50, 59$$

a jedini među njima djeljiv sa 7 je 14 pa je

$$x \equiv 14 \pmod{63}.$$

Sada još treba odrediti sve troznamenkaste brojeve koji su kongruentni 14 modulo 63, tj. sve $n \in \mathbb{N}$ takve da je $n = 63 \cdot k + 14$ i $100 \leq n \leq 999$. Otuda je

$$1.3 < \frac{86}{63} \leq k \leq \frac{985}{63} < 15.7$$

Stoga dobivamo po jedno rješenje za svaki $k = 2, 3, \ldots, 15$:

$$140, 203, 266, 329, 392, 455, 518, 581, 644, 707, 770, 833, 896, 959.$$

■

Primjer 2.2.4. [2015., Županijsko natjecanje, 3. razred, B varijanta]
Odredite zadnju znamenku umnoška prvih sto prirodnih brojeva koji pri djeljenju s 5 *daju ostatak* 3.

Rješenje. Svi prirodni brojevi koji prilikom dijeljenja s 5 daju ostatak 3 mogu se zapisati u obliku $5k + 3, k \in \mathbb{N}_0$. Zapišimo umnožak prvih sto takvih brojeva:

$$3 \cdot 8 \cdot 13 \cdot 18 \cdot 23 \cdot 28 \cdot 33 \cdots (5k + 3) \cdots 498 =$$
$$(3 \cdot 8) \cdot (13 \cdot 18) \cdot (23 \cdot 28) \cdot (33 \cdot 38) \cdots ((5k - 2) \cdot (5k + 3)) \cdots (493 \cdot 498).$$

Svaki od 50 umnožaka u zagradama završava znamenkom 4. Zaista,

$$n = (5k - 2)(5k + 3) \equiv -6 \equiv 4 \pmod 5,$$

te je očito n paran jer je $5k + 3 - (5k - 2) = 5$. Prema, Kineski teorem o ostatcima 2.2.2, sustav kongruencija

$$n \equiv 4 \pmod 5, \quad n \equiv 0 \pmod 2,$$

ima jedinstveno rješenje modulo 10, pa je to npr. 4, a sva su rješenja $n \equiv 4 \pmod{10}$. (Na drugi način, uočimo da izraz

$$(5k - 2)(5k + 3) = 25k^2 + 5k - 6 = 20k^2 + 5k(k + 1) - 10 + 4$$

pri dijeljenu s 10 daje ostatak 4 jer je $k(k + 1)$ paran broj.)

Zadnja znamenka našeg umnoška je zadnja znamenka potencije 4^{50}. Kako je $4^{50} = 16^{25}$, a potencije broja 16 uvijek završavaju znamenkom 6, traženi umnožak završava znamenkom 6. ■

2.3 Eulerova funkcija

Definicija 2.3.1. *Označimo s $\varphi(m)$ broj članova niza $1, 2, \ldots, m$ koji su relativno prosti s brojem m. Funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ koja je definirana s $m \mapsto \varphi(m)$ zovemo* ***Eulerova funkcija****.*

Primjerice, $\varphi(10) = 4$, jer u nizu

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10$$

ima ukupno 4 broja koji su relativno prosti s brojem 10. To su brojevi $1, 3, 7, 9$.
Iz same definicije Eulerove funkcije slijedi da za svaki prosti broj p vrijedi:

$$\varphi(p) = p - 1,$$

jer su u nizu $1, 2, \ldots, p-1, p$ svi brojevi osim p relativno prosti s p, a njih ima točno $p-1$.

Da bismo odredili vrijednosti funkcije za složene brojeve, koristimo sljedeća svojstva funkcije φ:

Propozicija 2.3.2. *(1) Ako su* $m, n \in \mathbb{N}$ *i* $\text{nzd}(m, n) = 1$ *onda je* $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$.

(2) Za prosti broj p *vrijedi da je* $\varphi(p^a) = p^{a-1}(p-1)$.

(3) Ako je $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}$ *kanonski rastav prirodnog broja* m *na proste faktore, onda vrijedi*

$$\varphi(m) = m\left(1 - \frac{1}{p_1}\right) \cdot \left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_i}\right).$$

Sada kada smo definirali Eulerovu funkciju i naveli neka njena svojstva, iskažimo Eulerov teorem.

Teorem 2.3.3 (Eulerov teorem)**.** *Ako je* $\text{nzd}(a, m) = 1$*, onda je* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Iz Eulerovog teorema izravno slijedi Mali Fermatov teorem.

Teorem 2.3.4 (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* $a^p \equiv a \pmod{p}$.

Mali Fermatov teorem jedan je od važnijih teorema u teoriji brojeva, iako je samo specijalan slučaj Eulerovog teorema. Pokazuje se kao izuzetno korisno sredstvo kod računanja kongruencija što ćemo vidjeti u daljnjim primjerima.

Primjer 2.3.5. [2012., Županijsko natjecanje, 2. razred, B varijanta]
Kojom znamenkom završava broj $2012^3 + 3^{2012}$*?*

Rješenje. Broj 2012^3 završava znamenkom 8. Potencije broja 3, 3^1, 3^2, 3^3, 3^4, 3^5, 3^6, ... redom završavaju znamenkom $3, 9, 7, 1, 3, 9, \ldots$, odnosno svaka se peta znamenka ponavlja pa je duljina perioda ponavljanja znamenaka jednaka 4. Stoga broj $3^{2012} = (3^4)^{503}$ ima znamenku jedinica kao i broj 3^4, a to je broj 1. Kako je $8 + 1 = 9$, to broj $2012^3 + 3^{2012}$ završava znamenkom 9. ■

U rješenju prethodnog primjera koristili smo svojstvo cikličnosti posljednje znamenke u nizu potencija, no isti se primjer može riješiti i direktnom primjenom Eulerovog teorema 2.3.3.

Rješenje. [2. način] Prema Teoremu 2.3.3 je $3^{\varphi(10)} = 3^4 \equiv 1 \pmod{10}$ pa je $3^{2012} = (3^4)^{503} \equiv 1 \pmod{10}$, te je $2012^3 + 3^{2012} \equiv 8 + 1 = 9 \pmod{10}$. Dakle, broj $2012^3 + 3^{2012}$ završava znamenkom 9. ■

Primjer 2.3.6. [1994., Bjelorusija]
Pokaži da 1994 *dijeli* $10^{900} - 2^{1000}$.

Rješenje. Kako je $1994 = 2 \cdot 997$, slijedi da moramo ispitati dijeli li prost broj 997 broj $10^{900} - 2^{1000}$. Prema Malom Fermatovom teoremu slijedi

$$10^{996} \equiv 1 \pmod{997}, \quad 2^{996} \equiv 1 \pmod{997}.$$

Otuda je

$$2^{1000} \equiv 2^4 = 16 \pmod{997}.$$

Nadalje,

$$10^{900} \cdot 10^{96} \equiv 1 \pmod{997}.$$

Sada uočimo da je $10^3 \equiv 3 \pmod{997}$ pa je

$$10^{96} \equiv 3^{32} = (3^{16})^2 \equiv 249^2 \equiv 187 \pmod{997},$$

pa kongruenciju

$$\underbrace{10^{900}}_{=x} \cdot 187 \equiv 1 \pmod{997}$$

možemo shavatiti kao linearnu kongruenciju u nepoznanici x. Prema Teoremu 2.2.1 ova linearna kongruencija ima jedinstveno rješenje modulo 997. Rješenje je

$$x \equiv a \pmod{997}$$

gdje je $a \in \mathbb{Z}$ takav da je $187a + 997b = 1$ (vidi Propoziciju 1.2.4). Cijele brojeve a i b određujemo pomoću Proširenog Euklidovog algoritma i dobivamo $a = 16$, $b = -3$. Stoga je i

$$x \equiv 16 \pmod{997}$$

te je

$$10^{900} - 2^{1000} \equiv 16 - 16 = 0 \pmod{997}.$$

■

Primjer 2.3.7. [2014., Državno natjecanje, 1. razred, B varijanta]
Odredite ostatak pri dijeljenju broja $(7^{2012})^{2014} - (3^{12})^{14}$ *s* 10.

Rješenje. Budući da je $\text{nzd}(7, 10) = 1$ prema Eulerovom teoremu 2.3.3 slijedi

$$7^{\varphi(10)} = 7^4 \equiv 1 \pmod{10}$$

pa je

$$7^{2012} \equiv 1 \pmod{10}$$

te

$$(7^{2012})^{2014} \equiv 1 \pmod{10}.$$

Analogno,

$$3^{\varphi(10)} = 3^4 \equiv 1 \pmod{10},$$

iz čega slijedi da je

$$(3^{12})^{14} \equiv 1 \pmod{10}.$$

Imamo da je $(7^{2012})^{2014} - (3^{12})^{14} \equiv 0 \pmod{10}$ pa zaključujemo da je ostatak broja $(7^{2012})^{2014} - (3^{12})^{14}$ pri dijeljenju s 10 jednak 0. ■

Rješenje. [2. način] Potencije broja 7 završavaju redom znamenkom $7, 9, 3, 1, 7, 9, 3, \ldots$, odnosno, svaka se četvrta znamenka ponavlja. Stoga broj $(7^{2012})^{2014} = ((7^4)^{503})^{2014}$ ima znamenku jedinica kao i broj 7^4, a to je broj 1.

Analogno dobijemo da broj $(3^{12})^{14} = ((3^4)^3)^{14}$ ima znamenku jedinica kao i broj 3^4, a to je broj 1. Dakle, broj $(7^{2012})^{2014} - (3^{12})^{14}$ ima znamenku jedinica 0 pa je ostatak pri dijeljenju s 10 jednak 0. ■

Primjer 2.3.8. [2003., Kanada]
Odredi posljednje tri znamenke broja $2003^{2002^{2001}}$.

Rješenje. Uočimo

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}.$$

Primijenimo Eulerov teorem (2.3.3) na $a = 3^{2002}$ i $m = 1000$ i dobivamo

$$a^{\varphi(1000)} \equiv a^{400} \equiv 1 \pmod{1000}.$$

Stoga je

$$a^{2001} \equiv a = 3^{2002} \equiv 3^2 = 9 \pmod{1000}$$

pa su zadnje 3 znamenke 009. ■

Primjer 2.3.9. [2015., Županijsko natjecanje, 1. razred, B varijanta]
Odredite zadnje tri znamenke broja

$$2^{2015} - 2^{2013} + 2^{2010}.$$

Rješenje. Nakon izlučivanja zajedničkog faktora dobivamo:

$$2^{2015} - 2^{2013} + 2^{2010} = 2^{2010}(2^5 - 2^3 + 1) = 2^{2010} \cdot 25 = 2^{2008} \cdot 2^2 \cdot 25 = 2^{2008} \cdot 100.$$

Potencije broja dva (veće od 1) imaju zadnju znamenku redom 2, 4, 8, 6, 2, 4, 8, 6, ... Dakle, ako im je eksponent djeljiv s 4, zadnja znamenka je 6. Tada je zadnja znamenka broja 2^{2008} jednaka 6, a množenjem sa 100 dobivamo da su zadnje tri znamenke 6, 0, 0. ■

Rješenje. [2. način] Treba odrediti $x \in \mathbb{Z}$ takav da je $0 \leq x < 1000$ i

$$2^{2015} - 2^{2013} + 2^{2010} \equiv x \pmod{1000}.$$

Uočimo da za potencije broja 2 i modul $m = 1000$ ne možemo primijeniti Eulerov teorem 2.3.3 jer $\text{nzd}(2, 1000) = 2 > 1$. No, $1000 = 2^3 \cdot 5^3$ pa ga primijenimo na $n = 125$. Vrijedi

$$2^{2015} - 2^{2013} + 2^{2010} = 2^{2000}(2^{15} - 2^{13} + 2^{10}) \equiv 2^{15} - 2^{13} + 2^{10} \equiv 100 \pmod{125}$$

jer je $2^{100} \equiv 1 \pmod{125}$ prema Teoremu 2.3.3. Budući da $2^3 | 2^{2015} - 2^{2013} + 2^{2010}$ slijedi da x zadovoljava sljedeći sustav kongruencija

$$x \equiv 0 \pmod{8}, \; x \equiv 100 \pmod{125}.$$

Prema Kineskom teoremu o ostatcima 2.2.2 sustav ima jedinstveno rješenje modulo 1000. Sva rješenja druge kongruencije $x \equiv 100 \pmod{125}$ za $0 \leq x < 1000$ su

$$100, 225, 350, 475, 600, 725, 850, 975.$$

Među njima je jedino 600 djeljiv s 8 pa je $x = 600$. ■

Primjer 2.3.10. [2016., Državno natjecanje, 4. razred, A varijanta]
Odredi sve trojke prirodnih brojeva (m, n, k) *takve da vrijedi* $3^m + 7^n = k^2$.

Rješenje. Budući da je $7^n = k^2 - 3^m$ slijedi da k^2 i 3^m moraju davati isti ostatak pri dijeljenju sa 7, a to je moguće samo ako je m paran broj. Zaista, $k^2 \equiv 1, 2, 4 \pmod{7}$, a $3^m \equiv 1, 2, 4 \pmod{7}$ samo ako je m paran. Dakle, $m = 2l$ za neki prirodan broj l, pa možemo pisati

$$7^n = (k - 3^l)(k + 3^l).$$

Iz gornje jednadžbe slijedi da su oba faktora potencije od 7, tj.

$$k - 3^l = 7^a,$$

$$k + 3^l = 7^b,$$

gdje su a i b neki nenegativni cijeli brojevi i $a < b$. Oduzimanjem prve jednadžbe od druge dobivamo

$$2 \cdot 3^l = 7^b - 7^a = 7^a(7^{b-a} - 1).$$

Budući da $2 \cdot 3^l$ nije djeljivo sa 7, slijedi da je $a = 0$ i

$$1 + 2 \cdot 3^l = 7^b.$$

Za $l = 1$ dobijemo da je $m = 2$, $b = 1$ i $k = 4$, pa je $n = 1$.

Ako je $l \geq 2$, onda $7^b = 1 + 2 \cdot 3^l$ daje ostatak 1 pri djeljenju s 9. Prema Eulerovom teoremu 2.3.3 je

$$7^{\varphi(9)} = 7^6 \equiv 1 \pmod 9.$$

Za najmanji $d \in \mathbb{N}$ takav da je $7^d \equiv 1 \pmod 9$ (tj. za *red* broja 7 modulo 9) mora vrijediti da $d|\varphi(9) = 6$. Stoga ispitamo

$$7^2 \equiv 4 \pmod 9,\ 7^3 \equiv 1 \pmod 9$$

i zaključujemo da je $d = 1$, pa je $7^{3s} \equiv 1 \pmod 9$ za sve $s \in \mathbb{N}$. Dakle,

$$7^{3s} - 1 = 2 \cdot 3^l$$

za neki $s \in \mathbb{N}$. Očito je lijeva strana prethodne jednakosti djeljiva s $7^3 - 1 = 342 = 2 \cdot 3^2 \cdot 19$, tj. s 19, a desna to nije, pa zaključujemo da nema rješenja u slučaju $l \geq 2$. Jedino rješenje je $(m, n, k) = (2, 1, 4)$. ■

2.4 Kvadratni ostatci

U natjecateljskim zadatcima često se ispituje djeljivost kvadrata nekog prirodnog broja. Tako se, na primjer lako može uočiti da kvadrat prirodnog broja pri dijeljenju s 4 mogu davati ostatke 0 i 1, a ne mogu 2 i 3. Zaista, za kvadrat parnog broja vrijedi

$$(2n)^2 = 4n^2 \equiv 0 \pmod 4,$$

a neparnog

$$(2n + 1)^2 = 4n^2 + 4n + 1 \equiv 1 \pmod 4.$$

Nadalje, pojavljuje se i problem zadnje znamenke kvadrata prirodnog broja. Prema Teoremu o dijeljenju s ostatkom 1.1.4 svaki prirodan broj n možemo napisati kao

$$n = 10q + k,\ q \in \mathbb{N}_0,\ k \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}.$$

Stoga je

$$n^2 = (10q + k)^2 = 100q^2 + 20qk + k^2 \equiv k^2 \pmod{10}.$$

Kako je

$$0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2, 8^2, 9^2 \equiv 0, 1, 4, 9, 6, 5, 6, 9, 4, 1 \pmod{10}$$

zaključujemo da kvadrat prirodnog broja može završavati znamenkama 0,1,4,5,6 i 9, odnosno nije moguće da zadnja znamenka kvadrata bude 2,3,7 ili 8.

U teoriji brojeva kvadratni ostatci imaju istaknuto mjesto. Definiraju se na sljedeći način:

Definicija 2.4.1. *Neka je* $\text{nzd}(a, m) = 1$. *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.*

Na primjer, svi kvadratni ostatci modulo 5 su kongruentni 1 i 4 modulo 5, a neostatci su kongruentni 2 i 3. Zaista, kvadriranjem brojeva iz reduciranaog sustava ostataka modulo 5 (to jest onih ostataka koji su relativno prosti s 5) dobivamo:

$$\begin{aligned} 1^2 = 1 &\equiv 1 \pmod{5}, \\ 2^2 = 4 &\equiv 4 \pmod{5}, \\ 3^2 = 9 &\equiv 4 \pmod{5}, \\ 4^2 = 16 &\equiv 1 \pmod{5}. \end{aligned}$$

Uočimo da je moguće da $x^2 \equiv 0 \pmod{5}$ ako i samo $5|x$. No, u ovom slučaju 0 ne predstavlja kvadratni ostatak modulo 5 jer $\text{nzd}(5, x) = 5$. Općenito, u u reduciranom sustavu ostataka modulo p, gdje je p neparan prost broj, imamo točno $\dfrac{p-1}{2}$ kvadratnih ostataka i isto toliko kvadratnih neostataka. Zaista, jer je

$$1, 2, \ldots, \frac{p-1}{2}, \frac{p+1}{2}, \ldots, p-1 \equiv 1, 2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2} \ldots, -1 \pmod{p}$$

slijedi da će kvadratne ostatke činiti brojevi kongruentni

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$$

modulo p.

Primjer 2.4.2. [2016., Županijsko natjecanje, 4. razred, B varijanta]
Odredite sve prirodne brojeve x, y za koje vrijedi $1! + 2! + \cdots + x! = y^2$.

Rješenje. Razlikujemo sljedeće slučajeve:

- Ako je $x = 1$, $1! = 1^2$.
- Ako je $x = 2$, $1! + 2! = 3 \neq y^2$.
- Ako je $x = 3$, $1! + 2! + 3! = 9 = 3^2$.
- Ako je $x = 4$, $1!+2!+3!+4! = 33 \neq y^2$. Ako je $x \geq 5$, onda $x!$ završava znamenkom 0, a zbroj $1!+2!+3!+4!\cdots+x!$ završava znamenkom 3. Budući da kvadrat prirodnog broja y ne može završavati znamenkom 3 jedina rješenja dobivamo za $x = 1$ i $x = 3$, odnosno
$$(x, y) \in \{(1, 1), (3, 3)\}.$$

■

Primjer 2.4.3. [2013., Županijsko natjecanje, 2. razred, A varijanta]
Dokaži da jednadžba
$$3x^4 + 2013 = 25y^2 - 24x^2$$
nema cjelobrojnih rješenja.

Rješenje. Napišimo danu jednadžbu u obliku
$$3x^4 + 24x^2 - 25y^2 + 2013 = 0.$$
Kako su svi pribrojnici osim $25y^2$ djeljivi s 3, i $25y^2$ mora biti djeljiv s 3, pa i y mora biti djeljiv s 3. Neka je $y = 3y_1$. Nakon dijeljenja s 3 promatrana jednadžba postaje
$$x^4 + 8x^2 - 75{y_1}^2 + 671 = 0.$$
Ako je x djeljiv s 3, onda su svi pribrojnici osim 671 djeljivi s 3, što je nemoguće. Ako x nije djeljiv s 3, onda njegov kvadrat daje ostatak 1 pri dijeljenju s 3, a isto vrijedi i za njegovu četvrtu potenciju (odnosno 1 je kvadratni ostatak modulo 3). To znači da je x^4+8x^2 djeljivo s 3 (tj. $x^4 + 8x^2 \equiv 1 + 8 \cdot 1 \equiv 0 \pmod 3$). I u ovom slučaju je $x^4 + 8x^2 - 75{y_1}^2$ djeljivo s 3, a 671 nije djeljivo s 3. Stoga dana jednadžba nema cjelobrojnih rješenja. ■

2.5 Wilsonov teorem

Wilsonov teorem jedan je od poznatijih teorema iz teorije brojeva koji ima vrlo široku primjenu.

Teorem 2.5.1 (Wilsonov teorem)**.** *Ako je p prost broj, onda je* $(p-1)! \equiv -1 \pmod{p}$.

Dokaz. Za $p = 2$ i $p = 3$ kongruencija je očito zadovoljena. Stoga smijemo pretpostaviti da je $p \geq 5$. Grupirajmo članove skupa $\{2, 3, \ldots, p-2\}$ u parove (i, j) sa svojstvom $i \cdot j \equiv 1 \pmod{p}$. Očito je $i \neq j$ jer bi inače broj $(i-1)(i+1)$ bio djeljiv sa p, a to je nemoguće zbog $0 < i - 1 < i + 1 < p$. Tako dobivamo $\frac{p-3}{2}$ parova i ako pomnožimo odgovarajućih $\frac{p-3}{2}$ kongruencija, dobit ćemo

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

pa je

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

□

Očito je da vrijedi i obrat Wilsonovog teorema. Zaista, neka vrijedi

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

i pretpostavimo da p nije prost. Tada p ima djelitelj d, $1 < d < p$ i d dijeli $(p-1)!$. No, tada d mora dijeliti i $p - 1$, što je kontradikcija.

Primjer 2.5.2. *Dokažite da za svaki prost broj p vrijedi*

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

Rješenje. Prema Wilsonovom teoremu 2.5.1 je

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

Dalje imamo redom,

$$(p-2)! \cdot (p-1) + 1 \equiv 0 \pmod{p},$$
$$(p-2)! \cdot p - (p-2)! + 1 \equiv 0 \pmod{p},$$
$$(p-2)! \equiv 1 \pmod{p}.$$

■

Primjer 2.5.3. [1970, IMO]
Pronađi sve pozitivne cijele brojeve n sa svojstvom da se skup

$$\{n, n+1, n+2, n+3, n+4, n+5\}$$

može podijeliti na dva skupa tako da produkt brojeva u jednom skupu bude jednak produktu brojeva u drugom skupu.

Rješenje. Pokazat ćemo da takva podjela nije moguća. Najprije pretpostavimo da postoji podjela skupa $\{n, n+1, n+2, n+3, n+4, n+5\}$ da je produkt jednog podskupa jednak A, a drugog B. Razlikujemo dva slučaja.

U prvom slučaju je točno jedan član skupa $\{n, n+1, n+2, n+3, n+4, n+5\}$ djeljiv sa 7 iz čega slijedi da je točno jedan od A ili B djeljiv sa 7. Iz toga slijedi da produkt $A \cdot B$ nije djeljiv sa 7^2 tj. $A \cdot B$ nije potpun kvadrat pa je $A \neq B$.

U drugom slučaju, svi članovi skupa su relativno prosti sa 7. Sada prema Wilsonovm teoremu (2.5.1) imamo:

$$n(n+1)\cdots(n+5) \equiv 1 \cdot 2 \cdots 6 \equiv -1 \pmod 7.$$

S druge strane je

$$n(n+1)\cdots(n+5) = A \cdot B$$

pa je $AB \equiv -1 \pmod 7$. No, ako je $A = B$ onda iz prethodne kongruencije slijedi da je $A^2 \equiv -1 \pmod 7$, što je nemoguće jer -1 nije kvadratni ostatak modulo 7. Dakle, ne postoji niti jedan pozitivan cijeli broj koji zadovoljava navedeno svojstvo. ■

Primjer 2.5.4. [1999, AHSME]
Postoje jedinstveni brojevi $a_2, a_3, a_4, a_5, a_6, a_7$ takvi da

$$\frac{5}{7} = \frac{a_2}{2!} + \frac{a_3}{3!} + \frac{a_4}{4!} + \frac{a_5}{5!} + \frac{a_6}{6!} + \frac{a_7}{7!}$$

pri čemu je $0 \leq a_i < i$ za $i = 2, 3, \ldots, 7$. Pronađi $a_2 + a_3 + a_4 + a_5 + a_6 + a_7$.

Rješenje. Moženjem cijele jednakosti sa 7! dobivamo

$$5 \cdot 6! = (3 \cdot 4 \cdot 5 \cdot 6 \cdot 7)a_2 + (4 \cdot 5 \cdot 6 \cdot 7)a_3 + (5 \cdot 6 \cdot 7)a_4 + 42a_5 + 7a_6 + a_7.$$

Prema Wilsonovom teoremu 2.5.1 je

$$a_7 + 7(a_6 + 6a_5 + \cdots) \equiv 5 \cdot 6! \equiv -5 \equiv 2 \pmod 7$$

iz čega slijedi $a_7 = 2$. "Prebacimo" a_7 na lijevu stranu i podijelimo cijelu jednakost sa 7 te dobivamo:

$$\frac{5 \cdot 6! - 2}{7} = 514 = 360a_2 + 120a_3 + 30a_4 + 6a_5 + a_6.$$

Sada je

$$a_6 + 6(a_5 + 5a_4 + 20a_3 + 60a_2) \equiv 514 \equiv 4 \pmod 6,$$

iz čega slijedi $a_6 = 4$. Analogno, kao a_7 i a_6, odredimo a_5, a_4, a_3, a_2. Konačno, dobivamo jedinstveno rješenje $(a_2, a_3, a_4, a_5, a_6, a_7) = (1, 1, 1, 0, 4, 2)$ pa je

$$a_2 + a_3 + a_4 + a_5 + a_6 + a_7 = 9.$$

■

Poglavlje 3

Diofantske jednadžbe

Neka je f polinom s n varijabli i cjelobrojnim koeficijentima. Jednadžba oblika

$$f(x_1, x_2, \ldots, x_n) = 0,$$

čija su rješenja cijeli brojevi naziva se *diofantska jednadžba*. Jednadžbe takve vrste razmatrao je starogrčki matematičar Diofant (Diofant iz Aleksandrije, oko 250. g.) i njemu u čast su ove jednadžbe i dobile ime.

3.1 Linearne diofantske jednadžbe

Najjednostavnije diofantske jednadžbe su linearne diofantske jednadžbe oblika

$$a_1x_1 + \ldots + a_nx_n = m,$$

gdje su $a_1, \ldots, a_n \in \mathbb{Z}$. Od linearnih diofantskih jednadžbi u zadatcima s natjecanja najčešće se pojavljuju one s dvije nepoznanice, tj. jednadžbe oblika

$$ax + by = c, \quad a, b, c \in \mathbb{Z}.$$

Teorem 3.1.1. *Neka su a, b, c cijeli brojevi i $d = \text{nzd}(a, b)$. Ako $d \nmid c$, onda jednadžba*

$$ax + by = c \tag{3.1}$$

nema cjelobrojnih rješenja. Ako $d \mid c$, onda jednadžba 3.1 ima beskonačno mnogo cjelobrojnih rješenja. Ako je (x_1, y_1) jedno rješenje, onda su sva rješenja dana s

$$x = x_1 + \frac{b}{d} \cdot t, \; y = y_1 - \frac{a}{d} \cdot t,$$

za $t \in \mathbb{Z}$.

Dokaz. Ako (3.1) ima rješenja, onda očito $d \mid c$. Pretpostavimo sada da $d \mid c$ i promotrimo kongruenciju

$$ax \equiv c \pmod{b}. \tag{3.2}$$

Po Teoremu 2.2.1 ova kongruencija ima rješenja i ako je x_1 neko rješenje, onda su sva rješenja od (3.2) dana sa $x \equiv x_1 \pmod{b'}$, gdje je $b' = b/d$. Stoga su sva rješenja od (3.1) u skupu cijelih brojeva dana s

$$x = x_1 + b't = x_1 + \frac{b}{d} \cdot t,\ t \in \mathbb{Z}.$$

Uvrstimo li ovo u (3.1), dobivamo

$$by = c - ax_1 - \frac{ab}{d} \cdot t = by_1 - \frac{ab}{d} \cdot t,$$

pa je

$$y = y_1 - \frac{a}{d} \cdot t.$$

□

Rješenje (x_1, y_1) jednadžbe (3.1) nazivamo *partikularno rješenje* diofantske jednadžbe. Opće rješenje je zbroj partikularnog rješenja i cjelobrojnog rješenja homogene jednadžbe $ax + by = 0$.

Teorem 3.1.2. *Neka su $a_1, a_2, \ldots, a_n$ cijeli brojevi različiti od nule. Tada linearna diofantska jednadžba*

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c \tag{3.3}$$

ima rješenja ako i samo ako $(a_1, a_2, \ldots, a_n) \mid c$. Nadalje, ako jednadžba (3.3) ima barem jedno rješenje, onda ih ima beskonačno mnogo.

Primjer 3.1.3. [2010., Županijsko natjecanje, 7. razred]
Koliko parova troznamenkastih prirodnih brojeva (x, y) zadovoljava uvjet $15x+3y = 2010$?

Rješenje. Nakon dijeljenja zadane jednadžbe s 3 dobivamo

$$5x + y = 670.$$

Tada je $y = 670 - 5x$. Kako su x i y troznamenkasti prirodni brojevi imamo

$$100 \leq x < 1000,\ 100 \leq y < 1000,$$

odnosno

$$100 \leq 670 - 5x < 1000,$$

to jest

$$114 \geq x > 66.$$

Kako je x troznamenkast slijedi

$$100 \leq x \leq 114$$

što znači da 15 parova troznamenkastih prirodnih brojeva (x, y) zadovoljava jednadžbu $15x + 3y = 2010$. (Troznamenkasta rješenja dane jednadžbe u skupu prirodnih brojeva su (100,170), (101, 165), (102, 160), ..., (113, 105), (114, 100).) ■

Rješenje. [2. način] Lako se vidi da je partikularno rješenje jednadžbu $5x+y = 670$ uređeni par $(1, 665)$. Sada prema Teoremu 3.1.1 slijedi da su sva rješenja početne jednadžbe dana s $(1 + t, 665 - 5t)$, $t \in \mathbb{Z}$. Kako se traže parovi troznamenkastih brojeva, imamo:

$$100 \leq 1 + t \leq 999,\ 100 \leq 665 - 5t \leq 999$$

iz čega slijedi da je $t \in [99, 113] \cap \mathbb{Z}$. Dakle, imamo 15 troznamenkastih parova prirodnih brojeva koji zadovoljavaju početni uvjet. ■

Sljedeći primjer rješili smo u odjeljku 2.2 pomoću Kineskog teorema o ostatcima (Primjer 2.2.3), a sada ćemo ga riješiti pomoću Teorema 3.1.1.

Primjer 3.1.4. [2012., Županijsko natjecanje, 1. razred, B varijanta]
Odredite sve troznamenkaste prirodne brojeve koji su djeljivi sa 7*, a pri dijeljenju s* 9 *daju ostatak* 5*.*

Rješenje. Iz uvjeta zadatka slijedi

$$n = 7x \text{ i } n = 9y + 5, x, y \in \mathbb{N}.$$

Rješavamo diofantsku jednadžbu $7x = 9y + 5$, odnosno

$$7x - 9y = 5.$$

Jedno njezino rješenje je $x_0 = 2$ i $y_0 = 1$. Tada je opće rješenje $x = 2 + 9t$, $y = 1 + 7t$, $t \in \mathbb{N}$. Kako je $100 < n < 1000$, a $n = 7x = 14 + 63t$, vrijedi

$$\begin{aligned} 100 < 14 + 63t < 1000, \\ 86 < 63t < 986, \\ 1.3 < t < 15.6, \end{aligned}$$

pa je $t \in \{2, 3, 4, \ldots, 15\}$. Stoga

$$n = 14 + 63t,\ t \in \{2, 3, 4, \ldots, 15\},$$

ili ispisano

$$n \in \{140, 203, 266, 329, 392, 455, 518, 581, 644, 707, 770, 83, 896, 959\}.$$

■

Primjer 3.1.5. [2015., Matematički klokan, skupina Cadet]
Vlak ima 12 *vagona. Svaki vagon ima isti broj kupea. Marko putuje u trećem vagonu, u* 18. *kupeu od lokomotive. Ivana putuje u* 7. *vagonu, u* 50. *kupeu od lokomotive. Koliko kupea ima svaki vagon?*

Rješenje. Označimo s x broj kupea u svakom vagonu. Tada je $2x + y = 18$ i $50 = 6x + z$, gdje je y redni broj kupea u trećem vagonu gdje se nalazi Marko, a z je redni broj kupea u 7. vagonu gdje se nalazi Ivana. Očito su $x, y, z \in \mathbb{N}$ te vrijedi da su y i z manji od x. Imamo:

$$y = 18 - 2x \text{ i } z = 50 - 6x$$

iz čega slijedi da je

$$18 - 2x < x \text{ i } 50 - 6x < x,$$

odnosno

$$x > 7.$$

Za $x = 8$ dobivamo da je $y = 2$ i $z = 2$. Za $x > 8$, y i z nisu prirodni brojevi (tj. manji su od 0) pa zaključujemo da je jedino rješenje $x = 8$ odnosno da svaki vagon ima 8 kupea. ■

3.2 Nelinearne diofantske jednadžbe

Sve diofantske jednadžbe koje nisu linearne nazivamo nelinearnim diofantskim jednadžbama. U njima se nepoznanica pojavljuje u članovima višeg reda, kao na primjer u jednadžbi

$$x^2 + 2y^3 = 8,$$

gdje se nepoznanice x i y pojavljuju u članovima drugog, odnosno trećeg reda. Univerzalna metoda rješavanja nelinearnih diofantskih jednadžbi ne postoji, ali zato postoji niz metoda kojima rješavamo neke specijalne tipove nelinearnih diofantskih jednadžbi. Neke od tih metoda su:

- metoda faktorizacije
- metoda kvocijenta
- metoda posljednje znamenke

- metoda kongruencija
- metoda zbroja potencija s parnim eksponentima
- metoda nejednakosti.

Kod diofantskih jednadžbi bez rješenja najčešće se koriste kongruencije. Prikazat ćemo primjere zadataka s natjecanja pri čijem rješavanju koristimo navedene metode.

Primjer 3.2.1. [2014., Županijsko natjecanje, 7. razred]
U skupu cijelih brojeva riješi jednadžbu $xy - 3x + y = 5$.

Rješenje. Zadatak ćemo riješiti metodom faktorizacije. Lijevu stranu jednakosti rastavimo na faktore:

$$(xy - 3x) + (y - 3) - 2 = 0,$$

$$x(y - 3) + (y - 3) - 2 = 0,$$

$$(x + 1)(y - 3) = 2.$$

Dakle, produkt cjelobrojnih izraza $x + 1$ i $y - 3$ jednak je 2, a to je moguće samo u slučajevima koji su dani u tablici:

$x + 1$	2	1	-1	-2
$y - 3$	1	2	-2	-1

Konačno rješenje je $(x, y) \in \{(1, 4), (0, 5), (-2, 1), (-3, 2)\}$. ■

Primjer 3.2.2. [2008., AIME]
Postoje jedinstveni pozitivni cijeli brojevi x *i* y *koji zadovoljavaju jednadžbu* $x^2 + 84x + 2008 = y^2$. *Odredi* $x + y$.

Rješenje. Dana je nelinearna diofantska jednadžba $x^2 + 84x + 2008 = y^2$ koju ćemo riješiti metodom faktorizacije. Početna jednadžba ekvivalentna je

$$y^2 = x^2 + 84x + 1764 + 244 = (x + 42)^2 + 244$$

iz čega slijedi da je

$$y^2 - (x + 42)^2 = 244.$$

Primjenom formule za razliku kvadrata dobivamo

$$(y - x - 42)(y + x + 42) = 244.$$

Budući da su x, y pozitivni cijeli brojevi, slijedi da je $y+x+42 > 0$ te je produkt cjelobrojnih izraza $y - x - 42$ i $y + x + 42$ jednak 244 samo u slučajevima koi su dani u tablici:

$y-x-42$	1	2	4	244	122	61
$y+x+42$	244	122	61	1	2	4

Dakle, razlikujemo 6 slučajeva. Rješavanjem sustava dvije jednadžbe s dvije nepoznanice u svakom od slučajeva iz dane tablice dobivamo da je jedino rješenje početne jednadžbe $(x, y) = (18, 62)$ pa je $x + y = 80$. ■

Primjer 3.2.3. [1995., Županijsko natjecanje, 7. razred]
Odredi parove cijelih brojeva x i y koji zadovoljavaju jednadžbu

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{xy} = 1.$$

Rješenje. Očito za rješenja mora vrijediti da je $x, y \neq 0$. Množenjem jednadžbe s xy dobivamo

$$y + x + 1 = xy.$$

Jednadžbu rješavamo metodom kvocijenta. Izrazimo jednu nepoznanicu, na primjer y.

$$y = \frac{x+1}{x-1} = 1 + \frac{2}{x-1}.$$

Izraz $\frac{2}{x-1}$ je cjelobrojan samo ako je $x - 1$ djelitelj broja 2, tj. $x - 1 \in \{1, -1, 2, -2\}$. Otuda dobivamo da je $x \in \{2, 0, 3, -1\}$, a pripadni y je iz skupa $\{3, -1, 2, 0\}$. No, budući da je $x, y \neq 0$ jedina rješenja početne jednadžbe su $(x, y) \in \{(2, 3), (3, 2)\}$. ■

Primjer 3.2.4. [2013., Županijsko natjecanje, 7. razred]
Dokaži da jednadžba $n \cdot (n - 5) = 408408408$ nema rješenja u skupu cijelih brojeva.

Rješenje. Budući da se na desnoj strani jednakosti nalazi "veliki" broj, zadatak ćemo riješiti metodom posljednje znamenke. Imamo:

$$n \cdot (n - 5) = n^2 - 5n = 408408408.$$

Kako kvadrat cijelog broja završava sa znamenkom $0, 1, 4, 5, 6$ ili 9, a broj $5y$ sa znamenkom 0 ili 5, slijedi da zbroj na lijevoj strani završava s $0, 1, 4, 5, 6$ ili 9, a nikako s 8. Dakle, početna jednadžba nema rješenja u skupu cijelih brojeva. ■

Primjer 3.2.5. [2013., Županijsko natjecanje, 1. razred, A varijanta]
Dokaži da jednadžba $x^2 = 2y^2 - 75y + 5$ nema cjelobrojnih rješenja.

Rješenje. Zadatak ćemo riješiti metodom kongruencija, promatrat ćemo ostatke pri dijeljenju s 5. (Budući da eksponent 2 dijeli $\varphi(5) = 4$.) Za lijevu stranu jednakosti je

$$x^2 \equiv 1, 4 \pmod 5,$$

a za desnu vrijedi

$$2y^2 - 75y + 5 \equiv 2, 3 \pmod 5.$$

Kako je $1, 4 \not\equiv 2, 3 \pmod 5$, slijedi da početna jednadžba nema cjelobrojnih rješenja. ■

Primjer 3.2.6. [2006., Mala olimpijada]
Dokaži da jednadžba $x^5 + y^5 + z^5 = 20152015$ *nema cjelobrojnih rješenja.*

Rješenje. Zadatak ćemo riješiti metodom kongrunecija, promatrat ćemo ostatke pri dijeljenju s 11. (Budući da eksponent 5 dijeli $\varphi(11) = 10$, gledamo jednadžbu modulo 11.)

Za desnu stranu jednakosti vrijedi

$$20152015 \equiv 4 \pmod{11},$$

a za lijevu koristimo Mali Fermatov teorem 2.3. Ako $11 \nmid a$, onda $11 \mid a^{10} - 1 = (a^5 - 1)(a^5 + 1)$, pa je $a^5 \equiv \pm 1 \pmod{11}$, pa je lijeva strana kongruentna nekom od brojeva $-3, -2, -1, 0, 1, 2, 3$ (tj. $8, 9, 10, 1, 2, 3$) modulo 11. Budući da 4 nije među tim brojevima, ova jednadžba zaista nema rješenja. ■

Primjer 3.2.7. [2010., Županijsko natjecanje, 1. razred, B varijanta]
Odredite sve cijele brojeve x, y *za koje vrijedi* $y^4 + x^{2010} = 2y^2 - 1$.

Rješenje. Zadatak ćemo riješiti metodom zbroja potencija s parnim eksponentima. Jednadžbu zapišemo u obliku

$$y^4 - 2y^2 + 1 + x^{2010} = 0$$

odakle slijedi

$$(y^2 - 1)^2 + x^{2010} = 0.$$

Potencije su parne pa su vrijednosti oba izraza s lijeve strane veća ili jednaka 0. Budući da je s desne strane nula, jedina mogućnost je da su izrazi jednaki 0. Imamo:

$$y^2 - 1 = 0 \text{ i } x = 0.$$

Dakle, rješenja su $(x, y) \in \{(0, 1), (0, -1)\}$ ■

Primjer 3.2.8. [1972., Republičko (državno) natjecanje, 4. razred]
Dokažite da jednadžba

$$x! + y! = 10z + 9$$

nema rješenja u skupu prirodnih brojeva.

Rješenje. Zadatak ćemo riješiti metodom nejednakosti. Budući da je desna strana jednadžbe neparan broj, zaključujemo da je točno jedan od brojeva x, y jednak 1. Neka je $x = 1$. Tada je $y! = 10z + 8$. Kako broj $10z + 8$ nije djeljiv s 5, mora biti $y \leq 4$. Lako se provjeri da niti jedan od brojeva $y = 2, 3, 4$ nije rješenje dane jednadžbe u skupu prirodnih brojeva. ■

Primjer 3.2.9. [1979., Republičko natjecanje, 7. razred]
Odredi $x, y, z \in \mathbb{N}$, takve da je $x < y < z$ i

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1.$$

Rješenje. U zadatku se pojavljuje nelinearna diofantska jednadžba koju ćemo riješiti metodom nejednakosti. Ako je $x = 1$, onda vrijedi $1 + \frac{1}{y} + \frac{1}{z} = 1$ odnosno $\frac{1}{y} + \frac{1}{z} = 0$, što je nemoguće za prirodne brojeve y i z, pa zaključujemo da je $x > 1$.

Iz $x < y < z$ slijedi da je $\frac{1}{x} > \frac{1}{y} > \frac{1}{z}$ pa dobivamo

$$\frac{1}{x} + \frac{1}{x} + \frac{1}{x} > \frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1,$$

odnosno $\frac{3}{x} > 1$ ili $x < 3$. Dakle, imamo da je $1 < x < 3$, tj. $x = 2$. Stoga je

$$\frac{1}{y} + \frac{1}{z} = \frac{1}{2}.$$

Ako je $y = 2$, onda je $\frac{1}{z} = 0$, što je nemoguće, pa zaključujemo da je $y > 2$.

Iz $y < z$ slijedi redom

$$\frac{1}{y} > \frac{1}{z}, \frac{1}{y} + \frac{1}{y} > \frac{1}{y} + \frac{1}{z},$$

odnosno $\frac{2}{y} > \frac{1}{2}$ ili $y < 4$. Dakle, $2 < y < 4$, tj. $y = 3$. Sada lako možemo odrediti da je $z = 6$. Prema tome, traženi brojevi su $x = 2, y = 3$ i $z = 6$. ■

3.3 Pellova jednadžba

Jednadžba je dobila ime po engleskom matematičaru Johnu Pellu (1611.-1685.) kojemu je Leonhard Euler (1707. - 1783.), po svemu sudeći, pogrešno pripisao zasluge za njezino rješavanje. Joseph Louis Lagrange (1736. - 1813.) prvi je dao njeno cjelovito rješenje.

Definicija 3.3.1. *Diofantska jednadžba*

$$x^2 - dy^2 = 1, \tag{3.4}$$

gdje je $d \in \mathbb{N}$ i d nije potpun kvadrat, zove se ***Pellova jednadžba****. Jednadžbu oblika*

$$x^2 - dy^2 = N, \tag{3.5}$$

gdje je d kao i gore i $N \in \mathbb{N}$ zovemo pellovska jednadžba.

Obje jednadžbe, i Pellovu i pellovske, rješavat ćemo u skupu prirodnih brojeva. Pellova jednadžba (3.4) ima beskonačno mnogo rješnja u $\mathbb{N}$ za svaki prirodni broj d koji nije potpuni kvadrat. Za razliku od toga, pellovske jednadžbe ne moraju imati rješenja.

Ako je $d \in \mathbb{N}$ potpun kvadrat, tada Pellova jednadžba (3.4) ima samo trivijalna rješenja. Naime, iz $(x - \sqrt{d}y)(x + \sqrt{d}y) = 1$ slijedi $x - \sqrt{d}y = x + \sqrt{d}y = \pm 1$. Analogno vrijedi da ako je d potpun kvadrat, onda pellovska jednadžba (3.5) ima najviše konačno mnogo rješenja.

Neka je (x_1, y_1) rješenje Pellove jednadžbe takvo da je $x_1 > 0$, $y_1 > 0$ i $x_1 + y_1\sqrt{d}$ najmanje moguće. To rješenje zovemo *fundamentalno rješenje* Pellove jednadžbe. Sljedeći teorem opravdava naziv fundamentalno rješenje, tj. pokazuje da se sva ostala rješenja Pellove jednadžbe mogu dobiti iz tog istaknutog rješenja.

Teorem 3.3.2. *Pellova jednadžba $x^2 - dy^2 = 1$ ima beskonačno mnogo rješenja. Ako je (x_1, y_1) njeno fundamentalno rješenje, onda su sva rješenja ove jednadžbe u skupu prirodnih brojeva dana s*

$$x_n + y_n\sqrt{d} = \left(x_1 + y_1\sqrt{d}\right)^n, n \in \mathbb{N}.$$

Teorem 3.3.3. *Rješenja Pellove jednadžbe (3.4) u skupu prirodnih brojeva (x_n, y_n) zadovoljavaju rekurzivne relacije*

$$\begin{aligned} x_n &= x_1x_{n-1} + dy_1y_{n-1}, \\ y_n &= y_1x_{n-1} + x_1y_{n-1}, n \geq 1, \end{aligned}$$

pri čemu je (x_1, y_1) fundamentalno, a $(x_0, y_0) = (1, 0)$ trivijalno rješenje od 3.4.

Do sada smo ustanovili da je Pellova jednadžba uvijek rješiva, te da je najbitnije pronaći najmanje rješenje u skupu prirodnih brojeva - fundamentalno rješenje. U zadatcima s natjecanja, gotovo uvijek je lako odrediti fundamentalno rješenje. U slučaju da fundamentalno rješenje ne možemo lako odrediti, metoda koja se pokazuje djelotvornom leži u razvoju broja $\sqrt{d}$ u jednostavni verižni razlomak. Stoga ćemo prije svega definirati verižni razlomak.

Neka je $\alpha \in \mathbb{R}$. Definiramo cijeli broj

$$a_0 = \lfloor \alpha \rfloor.$$

Ako je $\{\alpha\} = \alpha - a_0 > 0$, onda stavimo

$$\frac{1}{\alpha_1} = \alpha - a_0.$$

Očito je $\frac{1}{\alpha_1} > 1$ jer je $\{\alpha\} < 1$ i vrijedi

$$\alpha = a_0 + \frac{1}{\alpha_1}.$$

Sada definiramo prirodan

$$a_1 = \lfloor \alpha_1 \rfloor.$$

Ako je $\{\alpha_1\} = \alpha_1 - a_1 > 0$, onda stavimo

$$\frac{1}{\alpha_2} = \alpha_1 - a_1.$$

Očito je $\frac{1}{\alpha_2} > 1$ i vrijedi

$$\alpha_1 = a_1 + \frac{1}{\alpha_2}.$$

Postupak se nastavlja sve dok je $a_n \neq \alpha_n$. Može ustanoviti da će se postupak ponavljati u nedogled ako i samo ako je α iracionalan broj, odnosno da ćemo stati nakon konačno mnogo koraka ako i samo ako je α racionalan broj. Razvoj u jednostavni verižni razlomak broja α je konačan ako i samo ako je α racionalan broj. Nadalje, iz opisane procedure se vidi da broj α možemo zapisati u obliku tzv. *beskonačnog jednostavnog verižnog razlomka*

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ddots}},$$

ako je α iracionalan, odnosno u obliku *konačnog jednostavnog verižnog razlomka*

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}},$$

ako je α racionalan. Brojevi $a_0, a_1, \ldots$ zovu se *kvocijenti* verižnog razlomka. U slučaju kada je $\alpha = \frac{a}{b}$ racionalan brojevi $a_0, a_1, \ldots, a_n$ upravo odgovaraju kvocijentima iz Euklidovog algoritma za brojeve a i b. Razvoj u verižni razlomak obično kraće zapisujemo na sljedeći način

$$\alpha = [a_0; a_1, a_2, \ldots],$$

za $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, odnosno

$$\alpha = [a_0; a_1, a_2, \ldots, a_n],$$

za $\alpha \in \mathbb{R}$.

Za iracionalan broj α ima smisla promatrati racionalne brojeve

$$\frac{p_n}{q_n} = [a_0; a_1, \ldots, a_n].$$

Ti se racionalni brojevi nazivaju *konvergentama* razvoja u verižni razlomak broja α. Konkretno, $\frac{p_n}{q_n}$ se zove n-ta *konvergenta*. Konvergente zadovoljavaju mnoga važna svojstva. Neka od njih istaknut ćemo u sljedećoj propoziciji.

Propozicija 3.3.4. *Neka je $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, te $\frac{p_n}{q_n}$ pripadne konvergente verižnog razvoja od α.*

(1) Brojnici i nazivnici konvergenti zadovoljavaju sljedeće rekurzije:

$$\begin{aligned} p_n &= a_n p_{n-1} + p_{n-2}, p_{-1} = 1, p_{-2} = 0, \\ q_n &= a_n q_{n-1} + q_{n-2}, q_{-1} = 0, q_{-2} = 1, n \geq 0. \end{aligned}$$

(2) Niz konvergenti s parnim indeksom je rastući, tj. $\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots$.

(3) Niz konvergenti s neparnim indeksom je padajući, tj. $\frac{p_1}{q_1} > \frac{p_3}{q_3} > \frac{p_5}{q_5} > \cdots$.

(4) $\frac{p_{2n}}{q_{2n}} < \frac{p_{2n+1}}{q_{2n+1}}$, za sve $n \in \mathbb{N}_0$.

(5) $\lim_{n\to\infty} \frac{p_{2n}}{q_{2n}} = \lim_{n\to\infty} \frac{p_{2n+1}}{q_{2n+1}} = \lim_{n\to\infty} \frac{p_n}{q_n} = \alpha$.

Osim što iz prethodne propozicije vidimo da konvergente aproksimiraju broj α, bit će važne i za Pellovu jednadžbu. Naime, rješenja Pellove jednadžbe nalaze se među kovergentama verižnog razlomka broja $\sqrt{d}$. Broj $\sqrt{d}$ ima specifičan razvoj u verižni razlomak, te se kvocijenti mogu odrediti pomoću jednostavnog algoritma. Preciznije, vrijede sljedeće tvrdnje.

Teorem 3.3.5. *Verižni razlomak realnog broja $\sqrt{d}$ gdje d nije potpun kvadrat je oblika*

$$\sqrt{d} = [a_0; \overline{a_1, a_2, \ldots, a_{r-1}, 2a_0}],$$

gdje je $a_0 = \lfloor \sqrt{d} \rfloor$, a ostali kvocijenti se dobivaju pomoću rekurzije

$$s_{i+1} = a_i t_i - s_i, t_{i+1} = \frac{d - s_{i+1}^2}{t_i}, a_{i+1} = \left\lfloor \frac{s_{i+1} + a_0}{t_{i+1}} \right\rfloor, i = 0, \ldots, r-1 \tag{3.6}$$

uz početne uvjete $s_0 = 0, t_0 = 1$.

Kvocijenti $a_1, a_2, \ldots, a_{r-1}$ su centralno simetrični, to jest $a_1 = a_{r-1}, a_2 = a_{r-2}, \ldots$

Budući da ne znamo unaprijed duljinu perioda u razvoju broja $\sqrt{d}$, algoritam (3.6) provodimo sve dok se vrijednosti s_1 i t_1 ne ponove. Ako je duljina perioda jednaka r onda ćemo dobiti da je $(s_1, t_1) = (s_{r+1}, t_{r+1})$ što će nam biti znak da prestajemo s postupkom.

Sljedećim teorem opisujemo vezu između rješenja Pellove jednadžbe i kovergenti verižnog razlomka broja $\sqrt{d}$.

Teorem 3.3.6. *Neka je r duljina perioda u razvoju $\sqrt{d}$, te neka su $\frac{p_n}{q_n}$ konvergente od $\sqrt{d}$.*

Ako je r paran, sva rješenja jednadžba $x^2 - dy^2 = 1$ dana su sa (p_{nr-1}, q_{nr-1}) za $n \in \mathbb{N}$. Posebno, fundamentalno rješenje je (p_{r-1}, q_{r-1}).

Ako je r neparan, sva rješenja jednadžbe $x^2 - dy^2 = 1$ dana su sa (p_{2nr-1}, q_{2nr-1}) za $n \in \mathbb{N}$. Posebno, fundamentalno rješnje je (p_{2r-1}, q_{2r-1}).

Sada ćemo prikazati nekoliko zadataka s međunarodnih i inozemnih matematičkih natjecanja u kojima se pojavljuje Pellova jednadžba.

Primjer 3.3.7. [W.L. Putnam Mathematical Competition]
Dokaži da postoji beskonačno mnogo parova uzastopnih pozitivnih cijelih brojeva $(n, n+1)$ sa svojstvom da kad god prost broj p dijeli n ili $n+1$, onda kvadrat od p isto dijeli taj broj.

Rješenje. Dva primjera takvih parova su $(8, 9)$ i $(288, 289)$. Vidimo da je u oba primjera drugi broj potpun kvadrat, a prvi je udvostručeni potpun kvadrat. Dakle, drugi broj je x^2 a prvi $2y^2$ za neke cijele brojeve x i y. Budući da se ta dva broje razlikuju za 1, dobivamo sljedeću Pellovu jednadžbu: Stoga je prirodno razmotriti Pellovu jednadžbu

$$x^2 - 2y^2 = 1.$$

Prema Teoremu 3.3.2 Pelova jednadžba ima beskonačno mnogo rješenja (x_n, y_n) u skupu prirodnih brojeva. Budući je fundamentalno rješenje ove Pellove jednadžbe $(3, 2)$, slijedi da je $x_n, y_n > 1$ pa parovi uzastopnih brojeva $(2y_n^2, x_n^2)$ imaju potrebno svojstvo za $p > 2$. Za $p = 2$ još samo treba ustanoviti da je y_n paran. Zaista, $2y_n^2 = x_n^2 - 1 \equiv 0 \pmod 4$ (jer je x_n očito neparan broj) pa je y_n paran. ■

Napomena. Uočimo ako je a trokutasti broj, tj. $a = \dfrac{n(n+1)}{2}$, onda je $8a + 1 = (2n + 1)^2$ pa $(8a, 8a + 1)$, tj. $(4n(n + 1), (2n + 1)^2)$ mogu predstavljati "dobrog" kandidata koji zadovoljava uvjete Primjera 3.3.7. Zaista, za $n = 1$ dobivamo upravo par $(8, 9)$. Sljedeći par možemo konstruirati iz prethodnog za $n = 8$, $(4n(n+1), (2n+1)^2) = (4\cdot 8\cdot 9, (2\cdot 8+1)^2) = (288, 289)$. I tako dalje možemo nastaviti opisanu proceduru i dobiti niz brojeva s traženim svojstvom. Dakle, sljedeći par bi bio $(4 \cdot 288 \cdot 289, (2 \cdot 288 + 1)^2) = (332928, 332929)$.

Primjer 3.3.8. [2001., IMO]
Odredi najveći realni broj k takav da ako su a, b, c, d pozitivni cijeli brojevi takvi da je $a + b = c + d$, $2ab = cd$ i $a > b$ onda vrijedi $\dfrac{a}{b} \geq k$.

Rješenje. Iz uvjeta zadatka imamo

$$8ab = 4cd \leq (c+d)^2 = (a+b)^2$$

što je ekvivalentno s

$$8ab \leq a^2 + 2ab + b^2,$$

odnosno

$$\left(\frac{a}{b}\right)^2 - 6 \cdot \frac{a}{b} + 1 \geq 0$$

Rješenje ove kvadratne nejednadžbe je unija intervala $\langle -\infty, 3 - 2\sqrt{2}\rangle$ i $\langle 3 + 2\sqrt{2}, +\infty\rangle$. Budući da je $a > b$ i a, b pozitivni slijedi $\frac{a}{b} > 1$, pa je jedino rješenje interval $\langle 3+2\sqrt{2}, +\infty\rangle$, odnosno $\frac{a}{b} \geq 3 + 2\sqrt{2}$. Stoga smo pokazali da je $k \geq 3 + 2\sqrt{2}$.

Pokažimo sada da je $k = 3 + 2\sqrt{2}$. U tu svrhu ispitajmo može li $\frac{a}{b}$ postići vrijednost $3 + 2\sqrt{2}$. Kvadriranjem jednakosti $c + d = a + b$ i oduzimanjem $4cd$ dobivamo:

$$c^2 - 2cd + d^2 = a^2 + 2ab + b^2 - 4cd.$$

Kako je $4cd = 8ab$ slijedi

$$(c-d)^2 = a^2 - 6ab + b^2.$$

Sada pretpostavimo da je $(c-d)^2 = 1$. Stoga je $a^2 - 6ab + b^2 = 1$ tj.

$$(a-3b)^2 - 2(2b)^2 = 1. \tag{3.7}$$

Uvođenjem supstitucije $x = a - 3b$ i $y = 2b$ dobivamo Pellovu jednadžbu

$$x^2 - 2y^2 = 1.$$

Da bi odredili rješenja ove jednadžbe, razvijmo $\sqrt{2}$ u verižni razlomak.
$s_0 = 0, t_0 = 1, a_0 = \lfloor \sqrt{2} \rfloor = 1,$
$s_1 = a_0 t_0 - s_0 = 1, t_1 = \frac{d - s_1^2}{t_0} = 1, a_1 = \lfloor \frac{s_1 + a_0}{t_1} \rfloor = \lfloor \frac{1+1}{1} \rfloor = 2,$
$s_2 = 1, t_2 = 1, a_2 = \lfloor \frac{1+1}{1} \rfloor = 2,$
Vidimo da je $(s_1, t_1) = (s_2, t_2)$ pa je $\sqrt{2} = [1; \overline{2}]$. Dakle, period $r = 1$ je neparan. Prema Teoremu 3.3.6 fundamentalno rješenje jednadžbe $x^2 - 2y^2 = 1$ je

$$(x_1, y_1) = (p_1, q_1) = (a_1 p_0 + p_{-1}, a_1 q_0 + q_{-1}) = (2 \cdot 1 + 1, 2 \cdot 1 + 0) = (3, 2),$$

a sva rješenja su dana s (p_{2n-1}, q_{2n-1}). Prema Propoziciji 3.3.4 (3) i (5) je niz $\left(\frac{p_{2n-1}}{q_{2n-1}}\right)$ padajući i $\lim_{n\to\infty} \frac{p_{2n-1}}{q_{2n-1}} = \sqrt{2}$. Kako je niz $\frac{p_{2n-1}}{q_{2n-1}}$ padajući, konvergira broju $\sqrt{2}$ odozgo pa je $\frac{x_n}{y_n} = \frac{p_{2n-1}}{q_{2n-1}} \geq \sqrt{2}$.

Za rješenje (a, b) jednadžbe (3.7) vrijedi da je

$$a - 3b = x_n,\ 2b = y_n,$$

za $n \in \mathbb{N}$ takav da je y_n paran. Ispitajmo za koje $n \in \mathbb{N}$ vrijedi da je y_n paran. Prema Teoremu 3.3.3 je

$$y_n = 2x_{n-1} + 3y_{n-1},\ n \in \mathbb{N}$$

Budući da je $y_1 = 2$, tj. paran broj, iz prethodne rekurzije slijedi da je y_n paran za svaki prirodan broj n. Dakle, sva rješenja od (3.7) su

$$a_n = x_n + \frac{3y_n}{2},\ b_n = \frac{y_n}{2}$$

za $n \in \mathbb{N}$. Kako je

$$\frac{a_n}{b_n} = \frac{2x_n + 3y_n}{y_n} = 3 + 2\frac{x_n}{y_n}$$

i $\frac{x_n}{y_n} \geq \sqrt{2}$ slijedi da je $\frac{a_n}{b_n} \geq 3 + 2\sqrt{2}$. Našli smo niz $\frac{a_n}{b_n}$ koji zadovoljava uvjete zadatka i vrijedi da je

$$\lim_{n\to\infty} \frac{a_n}{b_n} = 3 + 2\sqrt{2}.$$

Dakle, $k = 3 + 2\sqrt{2}$. ■

Primjer 3.3.9. [1986., USAMO]
Koji je najmanji prirodan broj n veći od 1*, za koji je kvadratna sredina brojeva 1,2, . . . n cijeli broj? Kvadratnu sredinu brojeva* $a_1, a_2, \ldots, a_n$ *računamo kao*

$$\left(\frac{a_1^2 + a_2^2 + \cdots + a_n^2}{n}\right)^{\frac{1}{2}}.$$

Rješenje. Suma kvadrata prvih n prirodnih brojeva jednaka je

$$\frac{n(n+1)(2n+1)}{6}.$$

Stoga problem možemo svesti na određivanje najmanjeg broja n za koji postoji prirodan broj m takav da je

$$\frac{(n+1)(2n+1)}{6} = m^2.$$

Množenjem jednakosti s 48 i nadopunom do kvadrata dobivamo

$$(4n+3)^2 - 3(4m)^2 = 1,$$

odnosno Pellovu jednadžbu

$$x^2 - 3y^2 = 1$$

uz $x = 4n + 3$ i $y = 4m$. Fundamentalno rješenje ove Pellove jednadžbe je očito $(2, 1)$, a prema Teoremu 3.3.3 sva ostala rješenja su dana rekurzijom

$$x_{k+1} = 2x_k + 3y_k, y_{k+1} = x_k + 2y_k,\ k \in \mathbb{N}_0.$$

Budući da je $x = 4n + 3$ i $n \in \mathbb{N}$ u obzir dolaze samo rješenja $x_k > 7$, te rješenja za koja je $x_k \equiv 3 \pmod 4$ i $y_k \equiv 0 \pmod 4$. Prvih nekoliko rješenja Pellove jednadžbe su $(7, 4), (26, 15), (97, 56), (362, 209), (1351, 780)$. Zadnji par je prvi koji zadovoljava gore navedene uvjete. Dobivamo:

$$4n + 3 = 1351$$

iz čega slijedi da je rješenje $n = 337$. ■

Napomena. Promotrimo niz rješenja (x_k, y_k) Pellove jednadžbe $x^2 - 3y^2 = 1$ modulo 4. Imamo:

$$\begin{aligned}
x_1 &= 2, y_1 = 1 \\
x_2 &= 2x_1 + 3y_1 = 7 \equiv 3 \pmod 4,\ y_2 = x_1 + 2y_1 = 4 \equiv 0 \pmod 4 \\
x_3 &= 2x_2 + 3y_2 = 6 \equiv 2 \pmod 4,\ y_3 = x_2 + 2y_2 = 3 \equiv 3 \pmod 4 \\
x_4 &= 2x_3 + 3y_3 = 13 \equiv 1 \pmod 4,\ y_4 = x_3 + 2y_3 = 8 \equiv 0 \pmod 4 \\
x_5 &= 2x_4 + 3y_4 = 2 \equiv 2 \pmod 4,\ y_5 = x_4 + 2y_4 = 1 \equiv 1 \pmod 4
\end{aligned}$$

Uočimo da je $x_1 = x_5 \equiv 2 \pmod 4$ i $y_1 = y_5 \equiv 1 \pmod 4$ pa zaključujemo da se ostatci pri dijeljenju s 4 periodički ponavljaju s periodom duljine 4. Prvo rješenje koje zadovoljava uvjete zadatka je $(x_6, y_6) = (1351, 780)$, iduće $(x_{10}, y_{10}) = (262087, 151316)$, te su sva rješenja dana s (x_{2+4l}, y_{2+4l}), za $l \in \mathbb{N}$. Sada su svi prirodni brojevi veći od 1 za koje je kvadratna sredina brojeva $1, 2, \ldots, n$ cijeli broj dani s

$$n_l = \frac{x_{2+4l} - 3}{4}, l \in \mathbb{N}.$$

Primjer 3.3.10. [Leningrad Mathematical Olympiad]
Dokaži da ako pellovske jednadžbe $x^2 - 5y^2 = a$ i $x^2 - 5y^2 = b$ imaju rješenja, onda rješenje ima i jednadžba $x^2 - 5y^2 = ab$.

Rješenje. Pretpostavimo da su $x_1, x_2, y_1, y_2 \in \mathbb{Z}$ rješenja pellovskih jednadžbi $x^2 - 5y^2 = a$ i $x^2 - 5y^2 = b$. Tada vrijedi $x_1^2 - 5y_1^2 = a$ i $x_2^2 - 5y_2^2 = b$. Imamo

$$\begin{aligned}
ab &= (x_1^2 - 5y_1^2)(x_2^2 - 5y_2^2) \\
&= x_1^2x_2^2 + 25y_1^2y_2^2 - 5y_1^2x_2^2 - 5x_1^2y_2^2 \\
&= (x_1x_2)^2 + (5y_1y_2)^2 + 10x_1x_2y_1y_2 - 5(y_1x_2)^2 - 5(x_1y_2)^2 - 10x_1x_2y_1y_2 \\
&= (x_1x_2 + 5y_1y_2)^2 - 5(y_1x_2 + x_1y_2)^2.
\end{aligned}$$

Cijeli brojevi $x = x_1x_2+5y_1y_2$ i $y = y_1x_2+x_1y_2$ zadovoljavaju pellovsku jednadžbu $x^2-5y^2 = ab$. ■

Bibliografija

[1] N. Adžaga, *Diofantske jednadžbe*, dostupno na http://natjecanja.math.hr/wp-content/uploads/2015/07/N-Diofantske-jednadzbe-Nikola-Adzaga.pdf (svibanj, lipanj 2017.)

[2] T. Andreescu, R. Gelca, *Mathematical Olympiad Challenges, Second Edition*, Birkhäuser, Boston, 2000.

[3] S. Bingulac, I. Matić, *Kineski teorem o ostatcima za polinome*, Osječki matematički list, 12(2012), 105-126.

[4] K. Burazin, *Nelinearne diofantske jednadžbe*, Osječki matematički list, 7(2007), 11-21.

[5] A. Dujella, *Uvod u teoriju brojeva*, dostupno na https://web.math.pmf.unizg.hr/ duje/utb/utblink.pdf (lipanj 2017.)

[6] A. Dujella, *Diskretna matematika*, dostupno na https://web.math.pmf.unizg.hr/ duje/diskretna/diskretna.pdf (travanj 2017.)

[7] A. Dujella, M. Bombardelli, S. Slijepčević, *Matematička natjecanja učenika srednjih škola*, Element, Zagreb, 1997.

[8] Z. Franušić, *Pellova jednadžba*, dostupno na https://web.math.pmf.unizg.hr/nastava/etb/materijali/pellova-web.pdf (lipanj 2017.)

[9] Y. Hong - Bing, *Problems od Number Theory in Mathematical Competitions (Mathematical Olympiad Series)*, World Scientific Publishing Company, 2009.

[10] A. Horvatek, Zadatci s natjecanja iz matematike u RH http://www.antonija-horvatek.from.hr/natjecanja-iz-matematike/zadaci-OS.htm (lipanj 2017.)

[11] I. Ilišević, *Wilsonov teorem*, Osječki matematički list, 4(2004), 1-9.

[12] Z. Kurnir, *Dvije pedesetogodišnjice i jedna četrdesetpetogodišjnica*, MiŠ, 50(2009), 231-234.

[13] I. Mandić, I. Soldo, *Pellova jednadžba*, Osječki matematički list, 8(2008), 29-36.

[14] M. Marić, Prezentacija o povijesti Klokana bez granica, dostupno na http://www.antonija-horvatek.from.hr/natjecanja-iz-matematike/klokan-bez-granica.htm (lipanj 2017.)

[15] I. Nakić, *Diskretna matematika*, dostupno na https://web.math.pmf.unizg.hr/nastava/komb/predavanja/predavanja.pdf (svibanj 2017.)

[16] D. A. Santos, *Number Theory for Mathematical Contests*, dostupno na http://docplayer.net/217662-Number-theory-for-mathematical-contests-david-a-santos-dsantos-ccp-edu.html (travanj 2017.)

[17] V. Stošić, *Natjecanja učenika osnovnih škola*, Matkina biblioteka, Zagreb, 2000.

[18] A. Tafro, *Kongruencije*, Playmath, 1(2003), 9-15.

[19] P. Vandendriessche, H. Lee, *Problems in elementary number theory*, dostupno na http://www.problem-solving.be/pen/published/pen-20070711.pdf (lipanj 2017.)

[20] S. Varošanec, *Diofantske jednadžbe*, dostupno na https://web.math.pmf.unizg.hr/nastava/metodika/materijali/diofant.pdf (lipanj 2017.)

[21] D. Žubrinić, *Osnovno o matematičkim natjecanjima*, dostupno na http://www.croatianhistory.net/mat/natj.html (lipanj 2017.)

[22] Art of Problem Solving https://artofproblemsolving.com/ (lipanj 2017.)

[23] Hrvatski matematički elektronički časopis http://e.math.hr/natjecanja/index.html (lipanj 2017.)

[24] International Mathematical Olympiad http://www.imo-official.org/problems.aspx (travanj,svibanj 2017.)

[25] Wikipedia: William Lowell Putnam Mathematical Competition http://en.wikipedia.org/wiki/William_Lowell_ Putnam_Mathematical_Competition(lipanj 2017.)

Sažetak

Teorija brojeva jedna je od najstarijih i najljepših grana matematike. Budući da mnogi problemi u teoriji brojeva ne zahtijevaju veliko znanje i imaju puno varijacija, često se pojavljuju u matematičkim natjecanjima. Proučavajući zadatke s raznih domaćih, međunarodnih i inozemnih matematičkih natjecanja, u ovom radu prikazali smo zadatke s natjecanja i njihova rješenja vezane za djeljivost, proste brojeve i faktorizaciju, kongruencije te diofantske jednadžbe.

Summary

Number Theory is one of the oldest and one most beautiful branches of Mathematics. Since many problems in this branch use little knowledge and have many variations, they frequently occur in mathematical competitions. Studying assignments from various domestic, overseas and international math competitions, in this thesis we have included mathematics contest problems and their solutions related to divisibility, prime numbers and factorization, congruences and Diophantine equations.

Životopis

Rođena sam 8.4.1993. godine u Našicama. Do svoje jedanaeste godine živjela sam u selu Podgorač, nedaleko od Našica, gdje sam završila prvih 6 razreda Osnovne škole Hinka Juhna. Zatim s obitelji selim u Našice gdje 2007. godine završavam Osnovu školu Dore Pejačević te iste godine upisujem u Srednjoj školi Isidora Kršnjavoga u Našicama prirodoslovno matematičku gimnaziju. Srednju školu završila sam 2011. godine i nakon položene državne mature upisala Preddiplomski studij Matematika-nastavnički smjer na Prirodoslovno-matematičkom fakultetu u Zagrebu, Matematički odsjek. Preddiplomski studij završila sam u roku te 2014. godine upisala Diplomski studij Matematika-smjer nastavnički na istom Fakultetu. Diplomski studij završavam 2017. godine. Dana 12. rujna 2015. godine sam se udala te promijenila prezime iz Anić u Logarušić.