Teorija brojeva
Okvirni program rada sa nadarenim učenicima osnovnih škola

Hasan Jamak
Prirodno-matematički fakultet Sarajevo

January 24, 2012

Uvod

U Bosni i Hercegovini već pedesetak godina se organizuju regionalna i republička takmičenja iz matematike. U cilju postizanja što boljih rezultata na tim takmičenjima pojedine škole sistematski tokom cijele školske godine rade sa učenicima, a pojedine škole i njihovi nastavnici sjete se, sdmicu ili dvije pred takmičenje, i onda pokušavaju da na brzinu pripreme učenike za takmičenje. Budući da su zadaci na takmičenju zahtjevniji od školskih zadataka, to je pogrešno je očekivati da se za desetak dana mogu postići neki rezultati na takmičenju. Samo trajna znanja mogu doći do izražaja na takmičenju, a ona se stiču postepenim i smišljenim sistematskim radom.

Ovdje nam je želja da postaknemo sistematski i planski osmišljen rad sa nadarenim učenicima. osnovne i srednje škole. Daćemo neke smjernice za rad sa težištem na Teoriju brojevu.

Prije nego što zaigramo neku utakmicu potrebno je da naučimo hodati i trčati. Tako je i sa matematikom. Prije nego što pođemo na takmičenje moramo znati matematički razmišljati i povezivati ranije stečena znanja u cilju sticanja novih znanja. Zbog toga treba naš rad osmisliti tako da nam prevashodno bude cilj razvijanje matematičkog mišljenja, a ne samo uvjež bavanje određenih radnji.

Djeljivost

Krenimo od operacija sabiranja, oduzimanja i množenja cijelih brojeva. Kao što znamo ove operacije se mogu neograničeno vršiti u skupu cijelih brojeva. No, kao što znamo neki cio broj može biti paran i neparan. Odmah se nameću sljedeća pitanja:

1. Kada će zbir dva broja biti paran, a kada neparan?
2. Kada će proizvod dva broja biti paran, odnosno neparan?
3. Kada će proizvod tri broja biti paran, a kada će biti neparan broj?
4. Kada će zbir tri broja biti paran, a kada neparan?

Nakon toga uraditi zadatak tipa:
Zadatak Da li su tačne sljedeće tvrdnje? Vaš odgovor obrazložiti.

i) Ako je zbir dva cijela broja paran broj, onda je njihova razlika takođe paran broj.

ii) Ako je zbir dva cijela broja neparan broj, onda je njihova razlika takođe neparan broj.

iii) Ako je zbir dva cijela broja neparan broj, onda je njihov proizvod paran.

iv) Ako je proizvod tri cijela broja neparan, onda je njihov zbir takođe neparan broj.

Operacija djeljenja u skupu cijelih brojeva nije uvijek moguća, zato treba posvetiti dužnu pažnju djeljenju cijelih brojeva.

Definicija 1. *Neka su a i b nenulti cijeli brojevi. Ako postoji cio broj c takav da je $a = bc$, onda kažemo da b dijeli a i pišemo $b \mid a$. Ako je $a \neq bc$ za svaki cio broj c, onda kažemo da b ne dijeli a i pišemo $b \nmid a$.*

Sada treba obraditi djeljivost cijelih brojeva sa 2,3,4,5,6,8,9,10,11,12 i 15.

Iz definicije djeljivosti mogu se izvesti sljedeće osobine djeljivosti.

Teorem 2. *a) Ako $b \mid a$, onda za svako $c \in \mathbb{Z}$, $b \mid ac$.*

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

c) Ako $a \mid b$ i $a \mid c$, onda za svako $x, y \in \mathbb{Z}$ $a \mid (bx + cy)$.

d) Ako $a \mid b$ i $b \mid a$, onda je $a = \pm b$.

e) Ako $a \mid b$ i $a > 0, b > 0$, onda je $a \leq b$.

f) Ako je neka suma djeljiva cijelim brojem i svi sabirci osim jednog su djeljivi tim cijelim brojem, onda je i taj sabirak djeljiv cijelim brojem.

U nižim razredima ovaj teorem ilustrirati na nekoliko primjera, a u višim razredima dokazati. Obavezno uraditi nekoliko zadataka u kojima će se primjeniti tvrdnje ovog teorema.

Prosti brojevi

U Teoriju brojeva posebno mjesto zauzimaju prosti brojevi.

Definicija 3. *Za prirodan broj p veći od jedan kažemo da je prost ako je djeljiv samo sa jedan i samim sobom. Za prirodan broj koji nije prost kažemo da je* ***složen.***

Navesti nekoliko prostih brojeva. Zati postaviti pitanje da li je skup prostih brojeva konačan skup. Odgovor na to pitanje daje

Teorem 4 (Euklid)**.** *Postoji beskonačno mnogo prostih brojeva.*

Sljedeći teorem daje jednu jako lijepu osobinu prostih brojeva.

Teorem 5. *Neka je p prost broj. Ako $p \mid (ab)$, onda $p \mid a$ ili $p \mid b$.*

Na nekoliko primjera pokazati kako se cijeli brojevi rastavljaju na proizvod prostih faktora. Nakon toga navesti sljedeći teorem koji nam govori da ova faktorizacija vrijedi za sve cijele brojeve

Teorem 6 (Osnovni stav aritmetike)**.** *Svaki cio broj n može se napisati kao proizvod potencija prostih brojeva*

$$n = \pm 2^{e_1} 3^{e_2} 5^{e_3} 7^{e_4} \cdots p_k^{e_k},$$

gdje su e_i $(i = 1, 2, \ldots, k)$ nengativni cijeli brojevi. Znak plus se uzima ako je n pozitivan, a znak minus ako je n negativan broj. Ovaj prikaz je jednoznačno određen (do poretka faktora u proizvodu).

Primjer $90 = 2^1 3^2 5^1$ i $924 = 2^2 3^1 7^1 11^1$.

Teorem 7. *Neka prirodni brojevi m i n imaju faktorizaciju*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}, \ m = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}.$$

Tada $m \mid n$ ako i samo ako je

$$0 \le d_i \le e_i \ (i = 1, 2, \ldots, k).$$

Teorem 8. *Prirodan broj*

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

ima tačno

$$\tau(n) = (e_1 + 1)(e_2 + 1) \cdots (e_k + 1)$$

pozitivnih djelitelja.

Primjer Pretpostavimo da je n prirodan broj takav da broj $2n$ ima 28 pozitivnih djelitelja, a broj $3n$ ima 30 pozitivnih djelitelja. Koliko pozitivnih djelitelja ima broj $6n$?

Rješenje Broj n prikažimo u obliku $n = 2^{e_1}3^{e_2}p_3^{e_3}\cdots p_k^{e_k}$. Tada je

$$\begin{aligned}2n &= 2^{1+e_1}3^{e_2}p_3^{e_3}\cdots p_k^{e_k},\\ 3n &= 2^{e_1}3^{1+e_2}p_3^{e_3}\cdots p_k^{e_k},\\ 6n &= 2^{1+e_1}3^{1+e_2}p_3^{e_3}\cdots p_k^{e_k}.\end{aligned}$$

Prema uslovu zadatka je

$$\begin{aligned}(2+e_1)(e_2+1)(e_3+1)\cdots(e_k+1) &= 28,\\ (1+e_1)(e_2+2)(e_3+1)\ldots(e_k+1) &= 30,\end{aligned}$$

Stavimo $t = (e_3+1)\cdots(e_k+1)$. Tada je $(2+e_1)(e_2+1)t = 28$ i $(1+e_1)(e_2+2)t = 30$. Dakle, t je zajednički djelilac brojeva 28 i 30 pa je $t = 1$ ili $t = 2$.

Ako je $t = 1$, onda je $(2+e_1)(e_2+1) = 28$ i $(1+e_1)(e_2+2) = 30$. Odavde nalazimo $e_1 = 5$ i $e_2 = 3$. Tada je

$$\tau(6n) = (2+e_1)(2+e_2)t = 7\cdot 5\cdot 1 = 35.$$

Ako je $t = 2$, onda je $(2+e_1)(e_2+1) = 14$ i $(1+e_1)(e_2+2) = 15$. Jednostavno se provjerava da ova jednačina nema rješenja u skupu cijelih brojeva.

Teorem 9 (Algoritam o djeljenju)**.** *Svaki cio broj a može se na jedinstven način pomoću datog prirodnog broja b predstaviti u obliku*

$$a = bq + r, \quad 0 \le r < b,$$

gdje su q i r cijeli brojevi.

Broj q se naziva *količnikom,* a broj r *ostatkom* djeljenja broja a brojem b.

Na osnovu algoritma o djeljenju zaključiti:

1. Svaki cio broj se može napisati u obliku: $2k$ ili $2k+1$.
2. Svaki cio broj se može napisati u obliku: $3k$, ili $3k+1$ ili $3k+2$.
3. Svaki cio broj se može napisati u obliku: $4k$ ili $4k+1$ ili $4k+2$ ili $4k+3$.

Svaki prosti broj veći od tri može se predstaviti u obliku $6k+1$ ili $6k-1$, gdje je k nenegativan cio broj.

Podvući da se umjesto brojeva 2,3,4 mogu uzeti i drugi brojevi, tj. generalizirati tvrdnju. Koristeći ovu činjenicu dokazati da je proizvod dva uzastopna broja uvijek paran, da je proizvod tri uzastopna broja djeljiv sa 6, da je proizvod četiri uzastopna broja djeljiv sa 24=(4!). Generalizirati. Uraditi nekoliko zadataka iz ove oblasti.

Zadaci

1. Koliko djelilaca ima broj 6!?
2. Ako prirodan broj n ima neparan broj različitih prostih djelilaca, on je potpun kvadrat.
3. Naći a ako $3 \mid a$, $4 \mid a$ i $\tau(a) = 14$.
4. Ako je $ab = cd$, onda je broj $a^2 + b^2 + c^2 + d^2$ složen.
5. Ako je n neparan broj, onda je broj $n^2 - 1$ djeljiv sa 8.
6. Dokazati $12 \mid (n^4 - n^2)$.
7. Svaki prost broj veći od 3 može napisati u obliku $6k + 1$ ili $6k + 5$.
8. Ako su p i $8p^2 + 1$ prosti brojevi, dokazati da je i $8p^2 + 2p + 1$ prost broj.
9. Odrediti prost broj p ako se zna da su brojevi $p + 10$ i $p + 14$ prosti brojevi.
10. Ako su p i $p^2 + 2$ prosti brojevi, onda je $p^3 + 2$ prost broj.
11. Dokazati
    (a) $6 \mid (n^3 + 5n)$,
    (b) $30 \mid (n^5 - n)$,
    (c) Za koje n $120 \mid (n^5 - n)$?
12. $(3 \mid a, 3 \mid b) \Leftrightarrow 3 \mid (a^2 + b^2)$.
13. $21 \mid (a^2 + b^2) \Rightarrow 441 \mid (a^2 + b^2)$.
14. $6 \mid (a + b + c) \Leftrightarrow 6 \mid (a^3 + b^3 + c^3)$.
15. Ako je p prost broj veći od 3, onda $24 \mid (n^2 - 1)$.
16. Ako su p i q prosti brojevi veći od 3, onda $24 \mid (p^2 - q^2)$.
17. $19 \mid (3x + 7y) \Rightarrow 19 \mid (43x + 75y)$,
18. $17 \mid (3a + 2b) \mid\Rightarrow 17 \mid (10a + b)$.
19. Ako $9 \mid (a^2 + ab + b^2)$, onda $3 \mid a$ i $3 \mid b$.
20. Ako je p prost broj veći od 3, onda je $p^2 = 24t + 1$ za neki prirodan broj t.
21. Naći sve proste brojeve p i q tako da je $p^2 - 2q^2 = 1$.

Najveći zajednički djelilac

Definicija 10. *Cio broj d je* ***zajednički djelilac*** *brojeva a i b, ako $d \mid a$ i $d \mid b$.*

Cio broj d je ***najveći zajednički djelilac*** *brojeva a i b ako vrijedi*

(i) d je zajednički djelilac brojeva a i b;

(ii) za svaki zajednički djelilac q brojeva a i b vrijedi $q \mid d$.

Svaki nenulti cio broj ima konačno mnogo zajedničkih djelilaca, pa među njima postoji onaj najveći i njega nazivamo najvećim zajedničkim djeliocem.

Najveći zajednički djelilac brojeva a i b označavamo sa $nzd(a, b)$. Neki autori koriste oznaku (a, b). Ja izbjegavam ovu oznaku iz razloga što može doći do zabune sa uređenim parom (a, b). Može se koristiti i engleska oznaka $gcd(a, b)$ ili $< a, b >$.

Definicija 11. *Za cijele brojeve a i b kažemo da su* ***uzajamno (relativno) prosti*** *ako je $nzd(a, b) = 1$.*

Teorem 12. *Neka su a, b i c nenulti cijeli brojevi takvi da je $ab = c^2$. Tada je $a = du^2$ i $b = dv^2$, gdje je $d = nzd(a, b)$.*

Ovdje je važno uočiti sljedeću činjenicu: Ako je $d = nzd(a, b)$, onda postoje cijeli brojevi u i v takvi da je $a = du$ i $b = dv$. Brojevi u i v su uzajamno prosti.

Prilikom računanja najvećeg zajedničkog djelioca treba koristiti sljedeće očigledne činjenice:

$$nzd(a, 1) = 1,\ nzd(a, a) = a,\ nzd(a, 0) = a,$$

$$nazd(a, b) = nzd(b, a), nzd(a, aq) = a.$$

Koristeći formulu

$$nzd(a, b) = nzd(b, a - b)$$

mi možemo računati najveći zajednički djelitelj zamjenjujući veći broj sa razlikom većeg i manjeg broja.

Primjer

$$\begin{aligned} nzd(63, 28) &= nzd(28, 35) = nzd(28, 7) = nzd(7, 21) \\ &= nzd(7, 14) = nzd(7, 7) = 7. \end{aligned}$$

Primjer[IMO 1959.] Dokazati da se razlomak $\frac{21n+4}{14n+3}$ ne može skratiti ni za jednu vrijednost prirodnog broja n.

Rješenje

$$\begin{aligned} nzd(21n+4, 14n+3) &= nzd(14n+3, 7n+1) \\ &= nzd(7n+1, 7n+2) = nzd(7n+1, 1) = 1. \end{aligned}$$

Kako je $nzd(21n+4, 14n+3) = 1$, to se ovi brojevi nemaju zajedničkih faktora osim jedan, pa se razlomak ne može skratiti ni za jedan cio broj n.

Teorem 13. *Ako je k prirodan broj, onda je $nzd(ka, kb) = k \cdot nzd(a, b)$.*

Teorem 14. *Ako su brojevi b i c relativno prosti, onda iz $c \mid ab$ slijedi $c \mid a$.*

Teorem 15. *Ako je $a = bq + r$, onda je $nzd(a, b) = nzd(b, r)$.*

Na prethodnom teoremu se zasniva Euklidov algoritam.

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 \leq r_1 < b, \\ b &= r_1 q_2 + r_2, \quad 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 \leq r_3 < r_2, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 \leq r_n < r_{n-1}, \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Pošto brojevi

$$r_1, r_2, \ldots, r_k, \ldots$$

čine opadajući niz prirodnih brojeva to će se ovaj niz nakon konačnog broja koraka završiti, tj. doći do jednakosti oblika $r_{n-1} = r_n q_{n+1}$. Posljednji ostatak koji je različit od nule predstavlja najveći zajednički djelilac brojeva a i b.

Teorem 16. *Ako je d najveći zajednički djelilac cijelih brojeva a i b, onda postoje cijeli brojevi x i y takvi da je $d = ax + by$.*

Postavlja se pitanje kako odrediti ove cijele brojeve x i y? Njih je najjednostavnije odrediti iz tzv. proširenog Euklidovog algoritama.

Teorem 17. *Neka su a i b prirodni brojevi. Tada je*

$$nzd(a, b) = s_n a + t_n b,$$

gdje su s_n i t_n $n-ti$ članovi niza definisanog rekurzijom kako slijedi

$$\begin{array}{ll} s_0 = 1, & t_0 = 0 \\ s_1 = 0, & t_1 = 1 \\ s_j = s_{j-2} - q_{j-1} s_{j-1}, & t_j = t_{j-2} - q_{j-1} t_{j-1} \end{array}$$

za $j = 2, 3, \ldots, n$ gdje su q_j količnici u divizionom Euklidovom algoritmu za nalaženje najvećeg zajedničkog djelioca brojeva a i b.

Primjer Neka je $a = 252$ i $b = 198$. Koristeći Euklidov algoritam odredimo $nzd(a,b)$, a zatim prikažimo $nzd(a,b)$ kao linearnu kombinaciju brojeva a i b.

Imamo

$$\begin{aligned} 252 &= 1\cdot 198 + 54 \\ 198 &= 3\cdot 54 + 36 \\ 54 &= 1\cdot 36 + 18 \\ 36 &= 2\cdot 18. \end{aligned}$$

Dakle, $nzd(252,198) = 18$. Količnici su redom: $q_1 = 1$, $q_2 = 3$, $q_3 = 1$ i $q_4 = 2$. Sada koristimo algoritam prethodne teoreme za određivanje nizova s_i i t_i.

$$\begin{array}{ll} s_0 = 1, & t_0 = 0 \\ s_1 = 0, & t_1 = 1, \\ s_2 = s_0 - s_1q_1 = 1 - 0\cdot 1 = 1, & t_2 = t_0 - t_1q_1 = 0 - 1\cdot 1 = -1, \\ s_3 = s_1 - s_2q_2 = 0 - 1\cdot 3 = -3, & t_3 = t_1 - t_2q_2 = 1 - (-1)\cdot 3 = 4, \\ s_4 = s_2 - s_3q_3 = 1 - (-3)\cdot 1 = 4, & t_4 = t_2 - t_3q_3 = -1 - 4\cdot 1 = -5. \end{array}$$

Pošto je $r_4 = nzd(252,198) = 18$ to je

$$18 = 4\cdot 252 - 5\cdot 198.$$

Ovo se može složiti u tabelu sličnu Hornerovoj šemi.

i	0	1	2	3	4
q_i	-	1	3	1	2
$s_i = s_{i-2} - q_{i-1}s_{i-1}$	1	0	1	-3	4
$t_i = t_{i-2} - q_{i-1}t_{i-1}$	0	1	-1	4	-5

Tada je $nzd(a,b) = s_4a + t_4b = 4\cdot 252 + (-5)\cdot 198$.

Definicija 18. ***Zajedničkim sadržiocem*** *nenultih cijelih brojeva a i b podrazumjevamo svaki cio broj koji je djeljiv brojevima a i b. Najmanji među pozitivnim zajedničkim sadržiocima brojeva a i b naziva se* ***najmanji zajednički sadržilac*** *brojeva a i b i označavamo ga sa $nzs(a,b)$.*

Za najmanji sajednički sadržilac i najveći zajednički djelilac brojeva a i b vrijedi

$$nzs(a,b)\cdot nzd(a,b) = |ab|.$$

Naime, ako je $d = nzad(a,b)$, onda je $a = du$, $b = dv$, gdje su u i v relativno prosti cijeli brojevi. Tada je $nzs(a,b) = d|uv|$, pa je

$$nzs(a,b)\cdot nzd(a,b) = d|uv|\cdot d = |du\cdot dv| = |ab|.$$

Zadaci

1. Dokazati da se razlomci

$$\frac{12n+1}{30n+2} \text{ i } \frac{21n+4}{14n+3}$$

ne mogu skratiti ni za jednu vrijednost broja n.

2. Dokazati da je

$$nzd(5a+3b, 13a+8b) = nzd(a,b).$$

3. Naći sve brojeve s kojima se može skratiti razlomak

$$\frac{5n+5}{8n+7}.$$

4. Ako se razlomak

$$\frac{an+b}{cn+d}\ (n \in \mathbb{N})$$

može skratiti sa k, onda je cio broj $ad-bc$ djeljiv sa k.

5. Neka je $d_n = nzd(3n+5, 5n+3)$ $n \in \mathbb{N}$. Odrediti $A = \{d_n | n \in \mathbb{N}\}$. Za svako $k \in A$ odrediti $B_k = \{(n \in \mathbb{N} | k = nzd(3n+5, 5n+3)\}$.

6. Najmanji zajednički sadržilac dva broja je za 10 veći od njihovog zajedničkog djelioca. Naći ta dva broja.

7. Dat je pravougaonik sa stranicama 324cm i 141cm. Prvo je odrezujemo jedan po jedan kvadrat sa stranicom 141cm sve dok ne dobijemo pravougaonik u jojem je jedna stranica manja od 141cm. Od ovog pravougaonika odrezujemo jedan po jedan kvadrat čija je dužina stranice jednaka manjoj stranici ovo pravougaonika sve dok ne dobijemo pravougaonik kod kojeg je jedna stranica manja od manje strane ovog pravougaonika itd. Kolika je stranica posljednjeg odrezanog kvadrata? Koliko smo odrezali ukupno kvadrata i kojih dimenzija?

8. Nađite (bar jedan) par prirodnih brojeva a i b, tako da se od pravougaonika $a \times b$ mogu izrezati tačno 6 kvadrata maksimalnih i različitih dimenzija.

9. Tri automata na ulazu primaju uređene parove cijelih brojeva i na izlazu takođe daju uređeni par cijelih brojeva. Ako je na sva ulazu sva tri automata par (m, n), onda na izlazu prvog automata je par $(m+n, n)$, drugog automa par $(m-n, n)$ i trećeg automata par (n, m).

   a)Da li se automati mogu uvezati tako da par $(19, 18)$ na ulazu u niz automata daje na izlazu $(7, 13)$ ili $(12, 21)$? (Na raspolaganju svakog tipa automata imamo dovoljan broj.)

   b) Odrediti potreban i dovoljan uslov da ulaz (a, b) daje izlaz (c, d).

10. Neka je na milimetarskom papiru nacrtan pravougaonik dimenzija $272\,mm\times 204\,mm$ tako da mu stranicice idu duž linija na milimetarskom papiru. Povucimo jednu njegovu dijagonalu i odredimo kroz koliko čvorišta milimetarskog papira prolazi dijagonala. Drgim riječima, koliko parova cijelih brojeva leži na dijagonali. Generalizirati ovo za paralelogram stranica $a\,mm$ i $b\,mm$.

Kongruencije

Definicija 19. *Neka su a i b cijeli brojevi i m prirodan broj veći od 1. Ako $m \mid (a-b)$, onda kažemo da je a* ***kongruentno*** *broju b modulo m i pišemo $a \equiv b\,(\mod m)$.*

Teorem 20 (Osnovne osobine kongruencije)**.**

a) Ako je $a \equiv b\,(\mod m)$, onda brojevi a i b imaju isti ostatak pri djeljenju sa m.

b) Ako je $a \equiv b\,(\mod m)$ i $c \equiv d\,(\mod m)$, onda je $a \pm c \equiv b \pm d\,(\mod m)$.

c) Ako je $a \equiv b\,(\mod m)$ i $c \equiv d\,(\mod m)$, onda je $ac \equiv bd\,(\mod m)$.

d) Ako je $a \equiv b\,(\mod m)$ i $c \equiv d\,(\mod m)$, onda je $a^k \equiv b^k\,(\mod m)$.

e) Ako je $a \equiv b\,(\mod m)$ i $c \equiv d\,(\mod m)$, onda je $P(a) \equiv P(b)\,(\mod m)$ za svaki polinom $P(x)$ sa cjelobrojnim koeficijentima.

Primjer Naći ostatak pri djeljenju broja 1978^{20} sa 125.
Rješenje Kako je $1978 = 2000 - 22$ i broj 2000 je djeljiv sa 125, to je

$$1978 \equiv -22\,(\text{mod } 125).$$

Tada je

$$1978^{20} \equiv (-22)^{20} \pmod{125}.$$

Nadalje, je

$$(-22)^{20} = 484^{10} \equiv (-16)^{10} \,(\text{mod } 125) = 256^5 \equiv 6^5 \pmod{125} \equiv 26 \pmod{125}.$$

Primjer Ako su za neki prirodan broj n brojevi $2n+1$ i $3n+1$ potpuni kvadrati, onda $40 \mid n$.

Rješenje Neka je $2n+1 = a^2$ i $3n+1 = b^2$, gdje su a i b prirodni brojevi. Posmatrajmo kongruencije po modulu 8.

n	0	1	2	3	4	5	6	7
2n+1	1	3	5	7	1	3	5	7

Dakle, $2n+1$ daje ostatke $\{1,3,5,7\}$ pri djeljenju sa 8. Nadalje, imamo

a	0	1	2	3	4	5	6	7
a^2	0	1	4	1	0	1	4	1

Dakle, a^2 ima ostatke 0,1,4. Kao je $a^2 = 2n+1$, to ostaci moraju biti isti. To znači mora biti $a^2 \equiv 1 \,(\text{mod } 8)$ i

$$2n+1 \equiv 1 \,(\text{mod } 8).$$

Odavde slijedi da je $n = 4k$. Tada je $b^2 = 12k+1$. Primjenimo kongruenciju po modulu 8. Imamo

$$b^2 \equiv 12k+1 \equiv 4k+1 \,(\text{mod } 8).$$

k	0	1	2	3	4	5	6	7
4k+1	1	5	1	5	1	5	1	5

Dakle, $b^2 \equiv 1$ ili $5 \,(\text{mod } 8)$. Kako kvadrat prirodnog broja može biti kongruentan 0 ili 1 ili 4, to imamo samo jednu mogućnost $b^1 = equiv 1 \,(\text{mod } 8)$. Dakle, $b^2 = 8i+1$, pa je $12k+1 = 8i+1$, tj. $3k = 2i$. Dakle, k je paran broj, tj. $k = 2j$, pa je $n = 4k = 8j$. Dakle, n je djeljiv sa 8. Potrebno je da pokažemo da je $n \equiv 0 \,(\text{mod } 5)$.

a	0	1	2	3	4
a^2	0	1	4	4	1

n	0	1	2	3	4
2n+1	1	3	0	2	3
3n+1	1	4	2	0	3

Kako je $a^2 \equiv 2n+1$ i $b^2 \equiv 3n+1$ po modulu 5, to vidimo da samo slučaj $n \equiv 0 \pmod 5$ zadovoljva uslove. Naime, za $n \equiv 1 (\mathrm{mod}\ 5)$ i $n \equiv 4 (\mathrm{mod}\ 5)$ je $2n+1 \equiv 3 (\mathrm{mod}\ 5)$, a a^2 ne može nikad biti kongruentno 3 po modulu 5. Za $n \equiv 2 \pmod 5$ je $b^2 \equiv 3n+1 \equiv 2$, što je nemoguće. Ako je $n \equiv 3 \pmod 5$, onda je $a^2 \equiv 2n+1 \equiv 2 \pmod 5$, što je nemoguće. Dakle, $n \equiv 0 \pmod 5$.

Zadaci

1. Odrediti ostatk pri djeljenju broja 2^{22} sa 13.
2. Odrediti ostatak pri djeljenju broja 317^{258} sa 15.
3. Odrediti posljednju cifru u dekadskom zapisu broja 3^{400}.
4. Odrediti najmanji prirodan broj n takav da je broj n^2+1 djeljiv sa 13.
5. Dokazati da $4n^2+4$ nije djeljivo sa 19 ni za jedna prirodan broj n.
6. Odrediti sve prirodne brojeve n, takve da broj $n^8 - n^2$ nije djeljiv sa 504.
7. Naći sve prirodne brojeve n za koje je broj 10^n+8 djeljiv sa 72.
8. Ako su trocifrenom broju djeljivom sa 7, dvije posljednje cifre iste, dokazati da je zbir cifara tog broja djeljiv sa 7.
9. Naći najmanji prirodan broj n takav da je $2001^n - 1$ djeljiv sa 2^{2002}.
10. Neka je prirodan broj n relativno prost sa 10. Dokazati da 101 potencija broja n ima iste tri posljednje cifre kao n.
11. Ako prirodan broj n nije djeljiv sa 7, dokazati da je jedan od brojeva n^3-1 i n^3+1 djeljiv sa 7.
12. Ako je n proizvoljan neparan prirodan broj, dokazati da je broj $(n^2-1)(n+3)$ djeljiv sa 24.
13. Petocifreni broj $\overline{a378b}$ je djeljiv sa 72. Odrediti cifre a i b.
14. Naći sve prirodne brojeve n (sa bar tri cifre) koji imaju osobinu da se brojevi x i x^2 u dekadskom sistemu završavaju sa tri iste cifre.
15. Da li postoje cijeli brojevi m i n takvi da je $m^2+2010=n^2$?

Diofantove jednačine

Jednačine čija se rješenja posmatraju u skupu cijelih brojeva ili u nekom njegovom podskupu nazivaju se Diofantove jednačine.

Definicija 21. *Jednačina oblika*

$$ax + by = c,$$

gdje su a, b *i* c *cijeli brojevi naziva se linearna Diofantova jednačina. Uređeni par cijelih brojeva* (s, t) *za koji je*

$$as + bt = c$$

naziva se rjšenje linearne Diofantove jednačine.

Teorem 22. *Linearna Diofantova jednačina*

$$ax + by = c$$

ima rješenje ako i samo ako $nzd(a, b) \mid c$. *U tom slučaju je opšte rješenje jednačine oblika*

$$\begin{aligned} x &= \frac{c}{nzd(a,b)}u + \frac{b}{nzd(a,b)}t, \\ y &= \frac{c}{nzd(a,b)}v - \frac{a}{nzd(a,b)}t \ (t \in \mathbb{Z}), \end{aligned}$$

gdje su u *i* v *cijeli brojevi određeni Euklidovim algoritmom tj.* $au+bv = nzd(a, b)$.

Ako su brojevi a i b uzajamno prosti, onda jednačina $ax + by = c$ ima uvijek rješenje.

Primjer Neka je p prost broj. U skupu prirodnih brojeva riješiti jednačinu

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

Rješenje Kako je $\frac{1}{p} > \frac{1}{x}$ i $\frac{1}{p} > \frac{1}{y}$ to je $p < x$ i $p < y$. Neka je $x = p + u$, $y = p + v$ gdje su u i v prirodni brojevi. Tada je

$$\frac{1}{p+u} + \frac{1}{p+v} = \frac{1}{p}.$$

Nakon sređivanja dobije se $p^2 = uv$. Neka je $d = nzd(u, v)$. Tada iz $p^2 = uv$ slijedi $u = da^2$, $v = db^2$ gdje su a i b prirodni brojevi. Tada je $p = dab$. Kako je

p prost broj, to imamo sljedeće mogućnosti: $d = p, a = b = 1$, $a = p$, $b = d = 1$ i $b = p$, $a = d = 1$. Tada je

$$x = p + u = p + da^2$$

pa je $x = 2p$ ili $x = p + p^2$ ili $x = p + 1$. Analogno nalazimo da je $y = 2p$, ili $y = p + 1$ ili $y = p + p^2$. Dakle,

$$(x, y) \in \{(2p, 2p), (p(p + 1), p + 1), (p + 1, p(p + 1))\}.$$

Primjer U skupu cijelih brojeva riješiti jednačinu

$$15x^2 - 7y^2 = 9.$$

Rješenje Posmatrajmo kongruenciju po modulu 3. Tada je $-y^2 \equiv 0 \pmod 3$, pa je $y = 3y_1$. Tada imamo

$$5x^2 - 21y_1^2 = 3.$$

Ponovo primjenjujemo kongruenciju po modulu 3 i zaključujemo da $3midx$, pa je $x = 3x_1$. Dalje je $15x_1^2 - 7y_1^2 = 1$. Ponovo kongrunecija po modulu 3 i dobijamo $y_1^2 \equiv -1 \pmod 3$, što je nemoguće. Dakle, jednačina nema rješenja u skupu cijelih brojeva.

Primjer Riješiti sistem linearnih kongruencija

$$x \equiv 3 \;(\text{ mod } 10),\; x \equiv 5 \pmod{14}.$$

Rješenje Iz prve kongruencije imamo $x = 10t + 3$ za neki cio broj t. Iz druge kongruencije imamo $x = 14s + 5$ za neko $s \in \mathbb{Z}$. Odavde imamo $10t = 14s + 2$, tj. $5t = 7s + 1$. Primjenom kongruencije po modulu 5 dobije se $2s + 1 \equiv 0 \pmod 5$. Dakle, $2s + 1 = 5u \,(u \in \mathbb{Z})$. Odavde slijedi da je u neparan broj, pa je $u = 2v + 1$ $(v \in \mathbb{Z})$. Tada je $s = 5v + 2$ i $x = 70v + 33$ $(v \in \mathbb{Z})$.

Zadaci

1. Naći sve parove (p, q) prostih brojeva tako da je $p^3 - q^5 = (p + q)^2$.

2. Naći sva cjelobrojna rješenja jednačine $x^3 - 2y^3 - 4z^3 = 0$.

3. Naći cjelobrojna rješenja jednačine $xy + 3x - 5y + 3 = 0$.

4. Riješiti sistem kongruencija

$$x \equiv 3 \pmod 8,\; x \equiv 7 \pmod{12}.$$

5. Učenik je na testu imao 20 zadataka. Za svaki ispravno riješen zadatak dobio je 8 bodova, za svaki pogrešno riješen zadatak dobio je minus pet bodova, a za zadatak koji nije ni pokušao riješiti dobio je nula bodova. Na kraju je učenik imao 29 bodova. Koliko je zadataka ispravno riješio i koliko zadataka nije ni pokušao riješiti?

6. Da li je moguće 30 KM razmijeniti u 12 novčanica od 1KM, 2KM i 5KM. Ako je odgovor pozitivan onda naći broj različitih načina.

7. Naći najmanji prirodan broj sa sljedećim svojstvima: njegova polovina je kvadrat cujelog broja, njegova trećina je kub cijelog broja i njegova petina je peti stepen nekog prirodnog broja.

8. U skupu cijelih brojeva riješiti jednačinu $(x+y)(x+3y)=p$, gdje je p prost broj.

9. U skupu prirodnih brojeva riješiti jednačinu
$$\frac{1}{n}+\frac{1}{m}=\frac{1}{mn}+\frac{2}{5}.$$

10. Dokazati da jednačina $2x^2-5y^2=7$ nema cjelobrojnih rješenja.

11. Dokazati da jednačina $15x^2-7y^2=9$ nema rješenja u skupu cijelih brojeva.

12. Neki cio broj u decimalnom zapisu piše se sa 300 jedinica i izvjesnog broja nula. Da li taj broj može biti potpun kvadrat?

13. Neka je b cifra jedinica broja 2^n i neka je $2^n=10a+b$. Dokazati da je broj ab djeljiv sa 6.

14. Izvjestan broj od 15 listova papira isječen je na po 10 dijelova, zatim se od dobijenih listova isjeku još neki na po deset djelova itd. Kad su izbrojani dobijeni listići, pokazalo se da ih ima 2012. Dokazati da su listovi pogrešno izbrojani.

15. Naći najmanji prirodan broj čiji je ostatk pri djeljenju sa 2,3,5,7 i 11 jednak jedinici.

16. Nađite bilo koja tri susjedna prirodna broja, od kojih je svaki od njih djeljiv sa kvadraton nekog cjelog broja većeg od 1. Da li se ova tvrdnja može generalizirati, tj. da li za svaki cio broj k postoji niz od susjednih prirodnih brojeva od kojih je svaki djeljiv sa kvadratom nekog prirodnog broja većeg od 1?

17. Naći najveci prirodan broj n za koji postoji tačno jedan prirodan broj k takav da je

$$\frac{5}{9} < \frac{n}{n+k} < \frac{9}{16}.$$

18. Odrediti sve proste brojeve p takve da je $2p^4 - p^2 + 16$ potpun kvadrat.

19. Odrediti sve uredene trojke (a, b, p) prirodnih brojeva takve da je p prost broj i da je

$$p = \frac{b}{4}\sqrt{\frac{2a-b}{2a+b}}.$$

20. Dokazati da zbir tri i više uzastopnih prirodnih brojeva nije nikada prost broj.

21. Ako je prirodan broj n kvadrat nekog prirodnog broja, dokazati da je proizvod dvije zadnje cifre broja n (cifre desetica i cifre jedinica) paran broj.

22. Naći sve trocifrene prirodne brojeve sljedećih osobina: ako se ispred posmatranog broja napiše ista cifra koja stoji na mjestu jedinica dobije se četvorocifreni broj koji je za 18 manji od sedmostrukog posmatranog broja.

23. Napisati sve parove uzajamno prostih prirodnih brojeva čiji je proizvod 415800.

24. Napišimo cifre nekog broja u obrnutom poretku. Dokazati da tako dobijeni broj ne može biti dvaput veći od početnog broja.

25. Naći četvorocifreni broj $\overline{abcd}$ takav da je

$$\overline{abcd} = d \cdot \overline{dba}.$$

26. Jedan broj se može rastaviti na dva faktora čija je razlika 6, a zbir njihovih četvrtih stepena je 272. Koji je to broj?

27. Dokazati da je zbir kvadrata bilo kojih pet uzastopnih cijelih brojeva djeljiv sa 5, ali nije djeljiv sa 25.

28. Ako su p i $8p - 1$ prosti brojevi, dokazati da je broj $8p + 1$ složen broj.

29. Kvadrat nekog prirodnog broja je šestocifreni broj koji se sastoji, kada se posmatraju dvije po dvije cifre, od tri dvocifrena broja. Prvi i treći od njih su jednaki, a srednji je dvaput manji. Odrediti broj sa ovom osobinom.

30. Dokazati da izraz

$$\frac{3n^4 + 6n^3 - 2n^2 - 3n + 3}{n^2 + 3n + 2} \quad (n \in \mathbb{N})$$

nije cio broj ni za jedno $n \in \mathbb{N}$.

31. Naći četvorocifren broj koji je potpun kvadrat i čije su prve dvije cifre, kao i posljednje dvije cifre, jednake.

32. Dokazati da kvadrat proizvoljnog prostog broja veég od tri, pri djeljenju sa 12 daje ostatak 1.

33. Zbir dvocifrenog broja i broja koji ima iste te cifre, ali napisane obrnutim redom, daje potpun kvadrat. Naći sve takve brojeve.

34. Svaki cijeli stepen trocifrenog broja završava se na one tri cifre, kojima se piše taj broj (red pisanja cifara je nepromjenjen). Koji je to broj?

35. Naći četvorocifreni broj koji pri djeljenju sa 131 daje ostatak 112, a djeljenjem sa 132 daje ostak 98.

36. Odrediti sve dvocifrene brojeve koji su 14 veći od proizvoda svojih cifara.

37. Odrediti četvorocifreni broj $\overline{abcd}$ koji ispunjava uslove $\overline{cda} - \overline{abc} = 297$ i $a + b + c = 23$.

38. Odrediti sve trocifrene brojeve $\overline{abc}$ koji imaju osobinu $\overline{abc}^2 = \overline{xyzabc}$.

39. Ako je $\overline{cd} = 2 \cdot \overline{ab}$, onda broj $\overline{abcd}$ ne može biti potpun kvadrat.

40. Od cifara $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ sataviti dva broja P i Q koji će zadovoljavati sljedeće uslove:

    a) Prva cifra brojeva P i Q nije nula.
    b) Svaka od navedenih cifara se javlja jedanput i to samo u jednom iod navedenih brojeva P i Q.
    c) Broj Q je devet puta veći od broja P.

41. Naći prirodne brojeve m i n koji zadovoljavaju jednačinu

$$1! + 2! + \cdots + n! = m^2.$$

42. Naći sve dvocifrene brojeve koji su djeljivi proizvodom svojih cifara.

43. Naći sve trocifrene brojeve koji su djeljivi proizvodom svojih cifara.

44. Odrediti sve prirodne brojeve n tako da $5 \mid (n^2 + n - 2)$.

45. Odrediti sve prirodne brojeve n takve da je $n^2 + n + 1$ djeljivo sa 21.

46. Naći sve dvocifrene brojeve kod kojih se zbir cifara ne mijenja množenjem broja sa 2,3,4,5,6,7,8,9. (Uputstvo: Ako je a traženi bro, onda brojevi: $a, 2a, 3a, \ldots, 9a$ imaju isti zbir cifara. Broj $9a$ je djeljiv sa 9, pa mu je i zbir cifara djeljiv sa 9. Dakle, zbir cifara broja a je djeljiv sa 9, pa je i broj a djeljiv sa 9.)

47. Odrediti sve parove (a, b) prirodnih brojeva tako da su brojevi $\frac{a+3}{b} + \frac{b+3}{a}$ i $\frac{a^2}{b} + \frac{b^2}{a}$ prirodni brojevi.

48. Odrediti sve parove (a, b) prirodnih brojeva tako da su brojevi $\frac{4a+p}{b} + \frac{4b+p}{a}$ i $\frac{a^2}{b} + \frac{b^2}{a}$ prirodni brojevi, gdje je p neki prost broj.

49. U skupu prirodnih brojeva riješiti jednačinu $2^x + 3^y = z^2$.

50. Ako je broj $\overline{xyyy}$, $(y \neq 0)$ djeljiv brojem $\overline{xy}$, onda je $x = y$. Dokazati!

51. Odrediti cifre x i y tako da je $4^{\overline{xxy}} + 8^{\overline{yyx}} = 2^{1779}$.

52. Naći sve parove (p, q) prostih brojeva, takvih da je $2p^2 + 1 = q^5$.

53. Naći sve parove prostih brojeva (p, q) takvih da je $2(p^6 - q^2) = (p - q)^2$.

54. Naći sve parove (p, q) prostih brojeva tako da je $p^3 - q^5 = (p + q)^2$.

55. Naći sve parove prostih brojeva p i q tako da je $p^2 + 3pq + q^2$ a) potpun kvadrat: b) potencija broja 5.

56. Naći sve parove prirodnih brojeva (a, b) tako da je $ab = 160 + 90\, nzd(a, b)$.

57. Naći sve parove prirodnih brojeva (a, b) $a \leq b$ tako da je

$$ab = 300 + 7nzs(a, b) + 5nzd(a, b).$$