1.

Djeljivost brojeva

1.1. Dokaži da je broj $p^2 - 1$ djeljiv s 24 ako je $p \geqslant 5$ prost broj.

1.2. Nađi sve proste brojeve p takve da je $14p^2 + 1$ također prost broj.

1.3. Dokaži da broj djelitelja proizvoljnog prirodnog broja n nije veći od $2\sqrt{n}$.

1.4. Koliki se ostatak dobije pri dijeljenju broja 2^{100} s 3, a koliki pri dijeljenju istog broja s 5?

1.5. a) Za koje je cijele pozitivne brojeve n broj $2^n - 1$ kvadrat cijelog broja?

b) Isto pitanje za $2^n + 1$.

1.6. Koliki mogu biti ostaci pri dijeljenju kubova cijelih brojeva s 9?

1.7. Dokaži da postoji beskonačno mnogo cijelih brojeva koji se ne mogu prikazati u obliku zbroja kubova tri cijela broja.

1.8. Neka je $2^p - 1$ prost broj. Dokaži da je tada p također prost broj.

1.9. Neka je $2^n + 1$ prost broj. Dokaži da je tada n potencija broja 2 ($n = 2^k$).

1.10. Dokaži da je broj $7^{2n} - 4^{2n}$ djeljiv s 33.

1.11. Za koje je prirodne brojeve n broj $20^n + 16^n - 3^n - 1$ djeljiv s 323?

1.12. Dokaži da je za proizvoljan cijeli broj n broj $n^5 - 5n^3 + 4n$ djeljiv sa 120.

1.13. 15 prostih cijelih brojeva čine aritmetički niz. Dokaži da je razlika niza veća od 30 000.

1.14. Dokaži da je za proizvoljan $n \in \mathbf{N}$ broj $5^{2n+1} + 3^{n+2} \cdot 2^{n-1}$ djeljiv s 19.

1.15. Dokaži da je produkt dvije posljednje znamenke kvadrata cijelog broja paran.

1.16. Može li kvadrat cijelog broja završavati s četiri jednake znamenke različite od 0?

1.17. Dokaži da je za proizvoljan $n \in \mathbf{N}$ broj $n^4 + 4$ složen.

1.18. Dokaži ako je zbroj tri cijela broja djeljiv sa 6, tada je i zbroj njihovih kubova djeljiv sa 6.

1.19. Dokaži da je za proizvoljan $m \in \mathbf{N}$ broj $\dfrac{m}{3} + \dfrac{m^2}{2} + \dfrac{m^3}{6}$ cijeli broj.

1.20. Neki cijeli broj zapisan je u dekadskom sustavu s 300 jedinica i određenim brojem nula. Može li on biti potpuni kvadrat?

1.21. Neka je b posljednja znamenka broja 2^n; tada je $2^n = 10a + b$. Dokaži da je broj ab djeljiv sa 6.

1.22. Od 15 listova papira je nekoliko listova izrezano na po 10 dijelova, zatim se od dobivenih listova još neki izrežu na po 10 dijelova itd. Kad su prebrojani dobiveni listovi papira, pokazalo se da ih ima 1963. Dokaži da su listovi pogrešno prebrojani.

1.23. Nađi najmanji prirodan broj koji pri dijeljenju s 2, 3, 5, 7 i 11 daje ostatak 1.

1.24. Nađi najmanji cijeli broj koji pri djeljenju s $2, 3, 5, \dots, p_i, \dots, p_n$ (p_i je proizvoljan broj između prvih n prostih brojeva) daje ostatak 1.

1.25. Dokaži da postoji beskonačno mnogo prostih brojeva.

1.26. Dokaži da za proizvoljni n postoji n uzastopnih cijelih brojeva koji su svi složeni (tj. bez obzira na to što je skup prostih brojeva beskonačan, u nizu prirodnih brojeva postoje intervali proizvoljne dužine koji uopće ne sadrže proste brojeve).

1.27. Dokaži da postoji beskonačno mnogo prostih brojeva koji pri dijeljenju sa 4 daju ostatak 3, tj. prostih brojeva oblika $4n + 3$. To isto vrijedi za brojeve oblika $6n + 5$.

1.28. Dokaži da postoji beskonačno mnogo cijelih brojeva koji nisu oblika $p + n^2$ niti za jedan p i $n > 1$, gdje je p prost, a n cijeli broj.

1.29. Dokaži jednakost $(2+1)(2^2+1)\ldots(2^{2^n}+1) = 2^{2^{n+1}} - 1$.

1.30. Dokaži da su dva proizvoljna broja niza $2^{2^0}+1 = 3, 2^{2^1}+1 = 5, 2^{2^2}+1 = 17, \ldots 2^{2^n}+1$ relativno prosti. Iz toga izvedi dokaz u Zadatku 1.25.

1.31. Najmanje cijelo broja x naziva se najveći cijeli broj ne veći od x i označava se simbolom $\lfloor x \rfloor$.

a) Nađi cjelobrojni dio sljedećih brojeva: -1.5, $-\dfrac{1}{2}$, 0, 1, $2\dfrac{1}{2}$, 3.99.

b) Dokaži sljedeća svojstva cjelobrojnog dijela:

1) $\lfloor n+x \rfloor = n + \lfloor x \rfloor$ za cijeli n;

2) $\lfloor ka/b \rfloor \geqslant k \cdot \lfloor a/b \rfloor$ za cijeli k.

1.32. Dokaži da postoji točno $\lfloor N/q \rfloor$ prirodnih brojeva koji nisu veći od zadanog broja $N > 0$ i koji su djeljivi zadanim prirodnim brojem q, ($q < N$).

1.33. Dokaži da, ako je $b > 0$ cijeli broj, tada je $\lfloor a/b \rfloor = \lfloor \lfloor a \rfloor / b \rfloor$ za $a \geqslant 0$.

1.34. Sa $n!$ se označava produkt prvih n prirodnih brojeva ($n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$). Dokaži da je najveća potencija prostog broja p kojim je djeljiv broj $n!$ jednaka $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor \ldots + \lfloor n/p^m \rfloor$, gdje je $p^m \leqslant n$, $p^{m+1} > n$.

1.35. Dokaži da $n!$ niti za jedan n nije djeljiv s p^n, gdje je p prost broj.

1.36. Dokaži da je broj $(n!)!$ djeljiv s $(n!)^{(n-1)!}$.

1.37. Zadana su dva prirodna broja a i b. Pri dijeljenju a s b dobijamo ostatak r_1. Podijelimo b sa r_1 (očigledno je $r_1 < b$); dobijamo ostatak r_2; dalje r_1 podijelimo s r_2, dobijemo ostatak r_3, itd. Treba dokazati da se nakon nekog koraka ovaj postupak prekida (tj. da će neki ostatak r_{n-1} biti djeljiv s r_n) i da će posljednji ostatak koji nije jednak nuli biti najveći zajednički djelitelj brojeva a i b.

1.38. Dokaži da se za proizvoljne cijele brojeve a i b mogu naći takvi cijeli brojevi m i n da vrijedi $ma + nb = d$ gdje je d najveći zajednički djelitelj brojeva a i b. (Posebno, ako su a i b relativno prosti brojevi tada iz rezultata zadatka slijedi da postoje takvi cijeli brojevi m i n da je $ma + nb = 1$.)

1.39. Dokaži: brojevi $2^p - 1$ i $2^q - 1$ relativno su prosti ako i samo ako su p i q relativno prosti brojevi. Nađi najveću zajedničku mjeru brojeva $2^p - 1$ i $2^q - 1$, ako p i q nisu relativno prosti.

1.40. Dokaži da su sva cjelobrojna rješenja jednadžbe $x^m = y^n$, gdje su m i n relativno prosti brojevi, dana formulom $x = t^n$ i $y = t^m$, gdje je t proizvoljan cijeli broj.

1.41. Dokaži da je $\log 2$ iracionalan broj.

1.42. Kakvi bi trebali biti cijeli brojevi a i b da bi $\log_a b$ bio racionalan broj?

Rješenja

1.1. *Prvo rješenje.* Dokažimo najprije da se dijeljenjem prostog broja p, $p \geqslant 5$ sa 6 dobije ostatak 1 ili 5, tj. da se svaki prosti broj veći od 5 može napisati u obliku $6k+1$ ili $6k+5$ gdje je k cijeli broj.

Zaista, ako se dijeljenjem broja $p \geqslant 5$ sa 6 dobiju ostaci 2, 3 ili 4, tada je taj broj ili paran ili djeljiv s 3 pa ne može biti prost broj. Koristeći dokazano u slučaju $p = 6k+1$ odmah dobijemo $(6k+1)^2 - 1 = 12k(3k+1)$, dalje je lako vidjeti da je jedan od brojeva k i $3k+1$ paran, a ovo znači da je $p^2 - 1$ djeljiv s 24. Slučaj $p = 6k+5$ promatramo analogno.

Drugo rješenje. Razmatrajmo brojeve $p-1, p, p+1$. Kako je $p \geqslant 5$ prost broj, tada su $p-1$ i $p+1$ parni brojevi, pa je jedan od njih djeljiv sa 4, tj. $p^2 - 1$ djeljiv je s 8. Dalje je jedan od brojeva $p-1, p, p+1$ djeljiv s 3, a kako je $p \geqslant 5$ prost broj onda je ili $p-1$ ili $p+1$ djeljiv s 3.

1.2. $p = 3$. Ako je $p \neq 3$ tada je $14p^2 + 1$ djeljiv s 3. Naime, kvadriranjem brojeva $p = 3k+1$ ili $p = 3k-1$ dobivamo $p^2 = 9k^2 - 6k + 1$, tj. $p^2 = 9k^2 + 6k + 1$ a oba broja pri dijeljenju s 3 daju ostatak 1. Znači da je broj $14p^2 + 1$ djeljiv s 3. Ako je $p = 3$, tada je $14p^2 + 1 = 127$ prost broj.

1.3. Ako je $ab = N$, tada je ili $a \leqslant \sqrt{N}$ ili $b \leqslant \sqrt{N}$. Djelitelji broja dolaze dakle u parovima od kojih je jedan uvijek manji od $\sqrt{N}$, pa je njihov broj najviše $2\sqrt{N}$.

1.4. Razmotrimo koliki se ostaci dobivaju dijeljenjem brojeva $2, 2^2, 2^3, \ldots, 2^n, \ldots$, s 3 ili s 5. Dobivamo:

a) $2, 1, 2, 1, \ldots$,

b) $2, 4, 3, 1, 2, 4, 3, 1, \ldots$.

Sada primjećujemo da za n koji je djeljiv sa 4 pri dijeljenju broja 2^n

s 5 dobivamo ostatak 1. Pri dijeljenju 2^n s 3 za paran n ostatak je također 1. Odatle izlazi da su oba tražena ostatka jednaka 1.

1.5. a) Broj $2^n - 1$ za $n > 1$ pri dijeljenju sa 4 daje ostatak 3. Dokaži da kvadrat cijelog broja djeljenjem sa 4 daje ostatak 0 ili 1. Za $n = 1$ $2^1 - 1 = 1$ je kvadrat.

b) Ako je 2^n+1 kvadrat, tada je $2^n+1 = k^2$ i zato $2^n = (k+1)(k-1)$ tj. $k+1 = 2^l$, $k-1 = 2^m$. Odatle, oduzimanjem drugog broja od prvog dobivamo $2 = 2^l - 2^m$ pa je očito da je $m = 1$, $l - m = 1$, tj. $m = 1$, $l = 2$ odakle slijedi $n = 3$.

1.6. *Odgovor.* 0, 1, 8. Ako je broj n djeljiv s 3, tada je n^3 djeljiv s 9. Ako n nije djeljiv s 3, tada je $n = 3k+1$ ili $n = 3k+2$. Ostalo je očito.

1.7. Koristeći rezultat prethodnog zadatka dokaži da se brojevi $9k+4$ i $9k+5$ ne mogu predstaviti u obliku zbroja tri kuba ni za kakve cijele brojeve k.

1.8. Ako p nije prost broj tada se $p = k \cdot l$ i broj $2^{kl} - 1$ lako rastavljaju na faktore $2^{kl} - 1 = (2^k - 1)[2^{k(l-1)} + 2^{k(l-2)} + \ldots + 2^k + 1]$.

1.9. Ako n nije potencija broja 2 tada je $n = 2^l \cdot n'$ gdje je $n' > 1$ neparan broj, $l \geqslant 0$; u tom slučaju $2^n + 1 = \left(2^{2^l}\right)^{n'} + 1$ djeljiv s $2^{2^l} + 1$.

(Koristi činjenicu da je $x^k + y^k$ za neparan broj k djeljiv s $x + y$).

1.10. $7^{2n} - 4^{2n} = \left(7^2\right)^n - \left(4^2\right)^n$. Sada koristi činjenicu da je $x^k - y^k$ djeljiv s $x - y$ za proizvoljan prirodan broj k.

1.11. Za paran broj n. Treba napomenuti da je $323 = 17 \cdot 19$.

Odredimo koliki se ostatak dobiva dijeljenjem broja $20^n+16^n-3^n-1$ sa 17 i 19, i dokažimo da su za parne brojeve n oba ostatka jednaka nuli, a za neparne n su različita od nule. Na primjer, nađimo koliki je ostatak kad se navedeni broj podijeli s 19. Dobijemo: 20 daje ostatak 1, 16 daje ostatak -3, što znači da $20^n + 16^n - 3^n - 1$ daje isti ostatak kao i

$$1^n + (-3)^n - 3^n - 1 = 3^n[(-1)^n - 1].$$

Razmatrajući analogno ostatak dijeljenja zadanog broja sa 17, lako dobijemo da je za paran broj n on djeljiv sa 17 i s 19, a za neparan broj nije.

1.12. $n^5 - 5n^3 + 4n = (n-2)(n-1)n(n+1)(n+2)$. Između pet uzastopnih cijelih brojeva naći će se dva parna broja od kojih je jedan sigurno djeljiv s 4, što znači da je njihov produkt djeljiv s 8. Između 3 proizvoljna uzastopna cijela broja naći će se broj koji je djeljiv s 3, a između pet proizvoljnih uzastopnih cijelih brojeva naći će se broj djeljiv s 5. Dakle je broj djeljiv sa 120 ($120 = 8 \cdot 5 \cdot 3$).

1.13. Prije svega primijetimo da se u zadanom nizu ne nalazi niti jedan iz prostih brojeva 2, 3, 5, 7, 11, 13. Kad bi se bilo koji od ovih brojeva (npr. 13) nalazio među zadanima, tada bi prvi član niza p_1 bio jednak jednom od brojeva 2, 3, 5, 7, 11, 13. Tada bi i broj $p_1 + p_1 d$ također bio član niza što znači da bi trebao biti prost broj, što nije.

Dalje dokažimo da razlika niza d mora biti djeljiva sa 2, 3, 5, 7, 11, 13. Npr. pokažimo da je d djeljiv sa 13. Neka je p_1 prvi član niza. Tada su svi brojevi $p_1, p_1 + d, \ldots, p_1 + 12d$ prosti. Pretpostavimo da d nije djeljiv s 13. Tada svi brojevi $p_1, p_1 + d, \ldots, p_1 + 12d$ daju pri djeljenju s 13 različite ostatke pa je jedan između njih djeljiv sa 13, što je u suprotnosti s uvjetom zadatka da su svi brojevi prosti. Analogno dokazujemo da je d djeljiv sa 2, 3, 5, 7, 11. Kako je d djeljiv sa svim prostim brojevima 2, 3, 5, 7, 11, 13, tada on nije manji od $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 = 30030$.

1.14. $5^{2n+1} + 3^{n+2} \cdot 2^{n-1} = 5 \cdot 25^n + 27 \cdot 6^{n-1}$. Broj 25 pri djeljenju s 19 daje ostatak 6, što znači da zadani broj pri djeljenju s 19 daje isti ostatak kao i broj $5 \cdot 6^n + 27 \cdot 6^{n-1} = 57 \cdot 6^{n-1}$. Zadnji je broj uvijek djeljiv s 19.

1.15. Napiši broj u obliku $10a + b$, gdje je b posljednja znamenka, i kvadriraj.

1.16. Ne može. Koristi rezultat prethodnog zadatka.

1.17. Rastavi polinom $n^4 + 4 = (n^2 + 2)^2 - (2n)^2$ na faktore.

1.18. Broj

$$\begin{aligned} &a^3 + b^3 + c^3 - a - b - c \\ &\qquad = a(a-1)(a+1) + b(b-1)(b+1) + c(c-1)(c+1) \end{aligned}$$

uvijek je djeljiv sa 6 (tri uzastopna cijela broja sadrže jedan koji je djeljiv s 3 i bar jedan koji je djeljiv s 2). Znači da su $a + b + c$ i $a^3 + b^3 + c^3$ istovremeno ili djeljivi sa 6 ili nisu djeljivi sa 6.

1.19. $\dfrac{m}{3} + \dfrac{m^2}{2} + \dfrac{m^3}{6} = \dfrac{m(m+1)(m+2)}{6}$.

1.20. Odredi zbroj znamenki zadanog broja i uvjeri se da je djeljiv s 3 a da nije djeljiv s 9, što znači da ne može biti potpuni kvadrat.

1.21. Usporedi ostatke pri djeljenju broja 2^n s 3 i njegove posljednje znamenke b. Svi ostaci u slučaju kada je posljednja znamenka broja 2^n različita od 6 su jednaki pa je $10a = 2^n - b$ djeljiv s 3, odakle slijedi da je i a djeljiv s 3.

1.22. Odredi koliki je ostatak pri dijeljenju ukupnog broja listova papira s 9 i koristi sljedeće: rezanje na 10 dijelova jednog lista papira povećava ukupan broj listova za 9 i prema tome ostatak dijeljenja ukupnog broja listova s 9 se ne mijenja. Međutim, 15 i 1963 dijeljenjem s 9 daju različite ostatke.

1.23. $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$.

1.24. $2 \cdot 3 \cdot 5 \cdot 7 \cdot \ldots \cdot p_n + 1$.

1.25. Ako bi skup prostih brojeva bio konačan, broj $p_1 p_2 \ldots p_n + 1$ (gdje je $p_1 p_2 \ldots p_n$ umnožak svih prostih brojeva), bio bi složen i djeljiv s jednim od njih. Kako broj $p_1 p_2 p_2 \ldots p_n + 1$ pri dijeljenju sa bilo kojim od prostih brojeva $p_1, p_2, \ldots, p_n$ daje ostatak 1, dolazimo do kontradikcije.

1.26. Razmotri $1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n+1) = (n+1)!$. Tada su svi brojevi oblika $(n+1)! + 2$, $(n+1)! + 3, \ldots,$ $(n+1)! + n + 1$ složeni.

1.27. Neka postoji konačan skup takvih brojeva. Razmotri broj $4p_1 p_2 \ldots p_n - 1$, gdje je $p_1 p_2 \ldots p_n$ umnožak svih prostih brojeva oblika $4k+3$. Dokaži da ovaj broj ili ima prost faktor oblika $4k+3$ koji je različit od $p_1, p_2, \ldots, p_n$ ili je sam prost broj.

1.28. Razmotrimo sve brojeve oblika N^2 gdje je N cijeli broj i dokažimo da postoji beskonačno mnogo cijelih brojeva koji se ne mogu zapisati u obliku $p + n^2$ niti za jedan p i $n > 1$. Neka je $N^2 = p + n^2$, tada je $(N-n)(N+n) = p$; kako je p prost broj tada je $N - n = 1$, tj. $p = 2N - 1$. Da bi se, dakle, broj N^2 zapisao u zadanom obliku, nužno je da broj $2N - 1$ bude prost broj. Jasno je da postoji beskonačno mnogo cijelih brojeva N za koje je broj $2N - 1$ složen.

1.29.

$$\begin{aligned}
(2+1)(2^2+1)(2^{2^2}+1)\ldots(2^{2^n}+1)& \\
&= (2-1)(2+1)(2^2+1)\ldots(2^{2^n}+1) \\
&= (2^2-1)(2^2+1)\ldots(2^{2^n}+1) \\
&= (2^{2^2}-1)\ldots(2^{2^n}+1) \\
&= \ldots = 2^{2^{n+1}} - 1.
\end{aligned}$$

1.30. Koristeći se rezultatom prethodnog zadatka, dobijemo

$$\big(2^{2^n}+1\big) - 2 = 2^{2^n} - 1 = \big(2+1\big)\big(2^{2^1}+1\big)\ldots\big(2^{2^{n-1}}+1\big)$$

tj.

$$\big(2^{2^n}+1\big) = \big(2+1\big)\big(2^{2^1}+1\big)\ldots\big(2^{2^{n-1}}+1\big) + 2,$$

odakle i slijedi dokaz zadatka. Kako su svaka dva broja oblika $2^{2^n}+1$ relativno prosta, tada je ili broj $2^{2^n}+1$ prost ili ima prost faktor kojim nije djeljiv niti jedan drugi broj niza $2^{2^n}+1$. Odatle lako izlazi dokaz Zadatka 1.26.

1.31. a) $\lfloor -1.5 \rfloor = 2$; $\left\lfloor -\frac{1}{2} \right\rfloor = -1$; $\lfloor 0 \rfloor = 0$; $\lfloor 1 \rfloor = 1$; $\left\lfloor 2\frac{1}{2} \right\rfloor = 2$; $\lfloor 3.99 = 3 \rfloor$.

b) 1. Očigledno je. 2. Primijetimo da je $\frac{ka}{b} = \left\lfloor \frac{ka}{b} \right\rfloor + 1$, gdje je $0 \leqslant \alpha < 1$; $\frac{a}{b} = \left\lfloor \frac{a}{b} \right\rfloor + \beta$, gdje je $0 \leqslant \beta < 1$, tj. $\frac{ka}{b} = k\left\lfloor \frac{a}{b} \right\rfloor + k\beta$; odavde neposredno slijedi da je $\left\lfloor \frac{ka}{b} \right\rfloor = k\left\lfloor \frac{a}{b} \right\rfloor$.

1.32. Svi cijeli brojevi $q, 2q, \ldots, \lfloor N/q \rfloor q$ nisu veći od N i djeljivi su s q; $\big(\lfloor N/q \rfloor + 1\big)q > N$.

1.33. Ako je $\frac{a}{b} \geqslant m$, gdje su m i b cijeli brojevi, ($b > 0$, $m \geqslant 0$), tada je i $\lfloor a \rfloor / b \geqslant m$.

1.34. S obzirom na rezultat Zadatka 1.32 ima točno $\lfloor n/p \rfloor$ brojeva koji nisu veći od n i djeljivi su s p, $\lfloor n/p^2 \rfloor$ djeljivih s p^2, $\lfloor n/p^3 \rfloor$ djeljivih s p^3 itd. a za određivanje potencije s bazom p kojom je djeljivo $n!$ potrebno je zbrojiti sve te brojeve. Dobivamo tako

$$\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \ldots + \lfloor n/p^k \rfloor.$$

Odavde je k broj za koji vrijedi $p^k \leqslant n$, $p^{k+1} > n$, tj. $\lfloor n/p^{k+1} \rfloor = 0$.

1.35. Najveća potencija broja p kojim je djeljiv $n!$ jednaka je $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \lfloor n/p^3 \rfloor + \ldots + \lfloor n/p^k \rfloor$. Dokažimo da je taj broj manji od n. Stvarno,

$$\begin{aligned}\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor &+ \lfloor n/p^3 \rfloor + \ldots + \lfloor n/p^k \rfloor \\ &< n/p + n/p^2 + \ldots + n/p^k + \ldots = \frac{n}{p-1} \leqslant n.\end{aligned}$$

1.36. Neka je p bilo koji prost broj. Prema Zadatku 1.34, najveća potencija broja p kojom je djeljiv $n!$ je $\lfloor n!/p \rfloor + \lfloor n!/p^2 \rfloor + \lfloor n!/p^3 \rfloor + \ldots$. Koristeći formulu iz Zadatka 1.31 dobijemo:

$$\lfloor n!/p \rfloor + \lfloor n!/p^2 \rfloor + \lfloor n!/p^3 \rfloor + \ldots \geqslant (n-1)!\big(\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor + \ldots\big).$$

1.37. Prema uvjetu zadatka vrijedi

$$\begin{aligned} a &= q_1 b + r_1, \quad \text{gdje je } 0 < r_1 < b; \\ b &= q_2 r_1 + r_2, \quad \text{gdje je } 0 < r_2 < r_1; \\ r_1 &= q_3 r_2 + r_3, \quad \text{gdje je } 0 < r_3 < r_2; \\ &\vdots \\ r_{m-2} &= q_m r_{m-1} + r_m, \quad \text{gdje je } 0 < r_m < r_{m-1}, \end{aligned}$$

pa je niz prirodnih brojeva $b, r_1, r_2, \ldots, r_m$ je padajući što znači da se postupak uzastopnog dijeljenja na kraju prekida tj. jedan od ostataka r_{m-1} će biti djeljiv s r_m, dakle $r_{m-1} = q_{m+1} r_m$.

Sada postupak izgleda ovako:

$$\begin{aligned} a &= q_1 b + r_1, \\ b &= q_2 r_1 + r_2, \\ r_1 &= q_3 r_2 + r_3, \\ &\vdots \\ r_{m-2} &= q_m r_{m-1} + r_m, \\ r_{m-1} &= q_{m+1} r_m. \end{aligned}$$

Dokaži sada da je r_m djeljiv proizvoljnim zajedničkim faktorom brojeva a i b i obratno, r_m je zajednički faktor brojeva a i b. To znači da je r_m najveći zajednički djelitelj dvaju brojeva. Ovaj postupak naziva se Euklidov algoritam.

1.38. Izrazi r_m pomoću a i b koristeći postupak iz prethodnog zadatka.

1.39. Koristeći Euklidov algoritam, dokaži da je najveći zajednički djelitelj brojeva $2^p - 1$ i $2^q - 1$ jednak $2^d - 1$, gdje je d najveći zajednički djelitelj brojeva p i q.

1.40. Zamijeni u $x^m = y^n$ x i y umnoškom njihovih prostih faktora: $x = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_r^{k_r}$; $y = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}$. Dobivamo:

$$p_1^{k_1 m} \cdot p_2^{k_2 m} \cdot \ldots \cdot p_r^{k_r m} = p_1^{l_1 n} \cdot p_2^{l_2 n} \cdot \ldots \cdot p_r^{l_r n}.$$

Izjednačavanjem eksponenata broja p_1 na obje strane jednakosti dobivamo $k_1 m = l_1 n$, tj $\dfrac{k_1}{l_1} = \dfrac{n}{m}$; kako su m i n relativno prosti i razlomak $\dfrac{n}{m}$ se ne može skratiti, pa je $k_1 = d_1 n$, $l_1 = d_1 m$, pri čemu je d_1 cijeli broj.

Analogno se dokazuje da vrijedi

$$\begin{aligned} k_2 &= d_2 n, \quad l_2 = d_2 m, \\ &\vdots \\ k_r &= d_r n, \quad l_r = d_r m, \end{aligned}$$

gdje su $d_2, \ldots, d_r$ cijeli brojevi.

Označimo s t broj $p_1^{d_1} p_2^{d_2} \ldots p_r^{d_r}$, tada iz dobivenih jednakosti izlazi $x = t^n$, $y = t^m$.

Očito je da su za proizvoljan cijeli broj t izrazi $x = t^n$ i $y = t^m$ rješenja jednadžbe $x^m = y^n$; ranije smo dokazali da je svako rješenje predstavljeno u tom obliku, tj. ovi su izrazi sva rješenja dane jednadžbe.

1.41. Neka je $\log 2 = \dfrac{m}{n}$. Tada je $10^m = 2^n$, što je nemoguće za cijele brojeve m i n.

1.42. Ako su $\log_a b = \dfrac{p}{q}$ cijeli međusobno prosti brojevi, tada je $a^p = b^q$.

Iz Zadatka 1.40 proizlazi da postoji cijeli broj t takav da je $a = t^q$, $b = t^p$.