Osnovne informacije o kolegiju

Predavanja 2022/2023: Andrej Dujella i Filip Najman

Osnovne informacije o kolegiju

Predavanja 2022/2023: Andrej Dujella i Filip Najman

Vježbe 2022/2023: Adrian Beker i Petar Orlić

Osnovne informacije o kolegiju

Predavanja 2022/2023: Andrej Dujella i Filip Najman

Vježbe 2022/2023: Adrian Beker i Petar Orlić

Održavanje kolegija:
Četvrtkom 12-14 u prostoriji A101.

Osnovne informacije o kolegiju

Predavanja 2022/2023: Andrej Dujella i Filip Najman

Vježbe 2022/2023: Adrian Beker i Petar Orlić

Održavanje kolegija:
Četvrtkom 12-14 u prostoriji A101.

Konzultacije: Četvrtkom 10-12 ili po dogovoru.

Osnovne informacije o kolegiju

Predavanja 2022/2023: Andrej Dujella i Filip Najman

Vježbe 2022/2023: Adrian Beker i Petar Orlić

Održavanje kolegija:
Četvrtkom 12-14 u prostoriji A101.

Konzultacije: Četvrtkom 10-12 ili po dogovoru.

e-mail: fnajman@math.hr

Sadržaj:

Literatura:

- `https://web.math.pmf.unizg.hr/~duje/utb.html`;
- Andrej Dujella, *Uvod u teoriju brojeva,* skripta (PMF-MO), `https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`
- A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

Način polaganja predmeta

Kolokviji i završni ispit: Tijekom semestra pišu se dva kolokvija (na svakom će maksimalan broj bodova biti 60).

Način polaganja predmeta

Kolokviji i završni ispit: Tijekom semestra pišu se dva kolokvija (na svakom će maksimalan broj bodova biti 60).

Aktivnost na nastavi: Na vježbama i predavanjima zadavat će se zadatci za samostalno rješavanje. Studenti koji budu najuspješniji u rješavanju tih zadataka, dobit će u pravilu za svaki zadatak po 5 bodova. Maksimalan broj bodova koji će se moći sakupiti u ovoj komponenti je 20. Sa sakupljenih 15 bodova, studenti će se moći osloboditi završnog ispita. Možete maksimalno 15 bodova skupiti na vježbama.

Način polaganja predmeta

Kolokviji i završni ispit: Tijekom semestra pišu se dva kolokvija (na svakom će maksimalan broj bodova biti 60).

Aktivnost na nastavi: Na vježbama i predavanjima zadavat će se zadatci za samostalno rješavanje. Studenti koji budu najuspješniji u rješavanju tih zadataka, dobit će u pravilu za svaki zadatak po 5 bodova. Maksimalan broj bodova koji će se moći sakupiti u ovoj komponenti je 20. Sa sakupljenih 15 bodova, studenti će se moći osloboditi završnog ispita. Možete maksimalno 15 bodova skupiti na vježbama.

Završni ispit: Završni ispit je usmeni; ispituje se sadržaj obrađen na predavanjima. Uvjet za pristup završnom ispitu je ukupno barem 40 bodova prikupljenih na 2 kolokvija i aktivnostima na nastavi. Maksimalan broj bodova koji je moguće dobiti na završnom ispitu je 60. Studenti koji kroz aktivnosti na nastavi sakupe barem 15 bodova ne moraju izaći na završni ispit, već mogu uzeti ocjenu dobivenu na osnovu 2 kolokvija i aktivnosti na nastavi.

Način polaganja predmeta

Popravni ispit: Može se popravljati najviše jedan od kolokvija ili završni ispit. Nakon drugog kolokvija piše se popravak kolokvija na kojem studenti mogu pisati ili popravak prvog ili popravak drugog kolokvija. Nema uvjeta za izlazak na taj popravak. Studenti koji nisu zadovoljni rezultatom završnog ispita i koji nisu pisali popravak kolokvija, mogu izaći na popravni završni ispit. Taj ispit bi bio u istom terminu kad i završni ispit za studente koji su pisali popravak kolokvija.

Način polaganja predmeta

Popravni ispit: Može se popravljati najviše jedan od kolokvija ili završni ispit. Nakon drugog kolokvija piše se popravak kolokvija na kojem studenti mogu pisati ili popravak prvog ili popravak drugog kolokvija. Nema uvjeta za izlazak na taj popravak. Studenti koji nisu zadovoljni rezultatom završnog ispita i koji nisu pisali popravak kolokvija, mogu izaći na popravni završni ispit. Taj ispit bi bio u istom terminu kad i završni ispit za studente koji su pisali popravak kolokvija.

Zaključivanje ocjene: zbrojit će se bodovi iz 1. kolokvija (max. 60), 2. kolokvija (max.60), aktivnosti na nastavi (max.20) i završnog ispita (max.60). Studentima koji budu oslobođeni završnog ispita, zbrojit će se bodovi iz prve 3 komponente.

Način polaganja predmeta

Ocjene:

1. $\geq$ 85% bodova - ocjena 5
2. $70 - 85\%$ bodova - ocjena 4
3. $55 - 70\%$ bodova- ocjena 3
4. $40 - 55\%$ bodova - ocjena 2
5. $<$ 40% bodova - ocjena 1.

Uvod

- Teorija brojeva (klasična) se bavi ponajprije svojstima prirodnih brojeva, te cijelih i racionalnih brojevima.

Neka svojstva skupa prirodnih i skupa cijelih brojeva koja ćemo koristiti:

- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) su definirane operacije zbrajanja i množenja koje zadovoljavaju svojstva komutativnosti, asocijativnosti i distributivnosti;

Uvod

- Teorija brojeva (klasična) se bavi ponajprije svojstima prirodnih brojeva, te cijelih i racionalnih brojevima.

Neka svojstva skupa prirodnih i skupa cijelih brojeva koja ćemo koristiti:

- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) su definirane operacije zbrajanja i množenja koje zadovoljavaju svojstva komutativnosti, asocijativnosti i distributivnosti;
- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) imamo uređaj takav da za svaka dva različita elementa $m, n \in \mathbb{N}$ ($\mathbb{Z}$) vrijedi ili $m < n$ ili $n < m$;

Uvod

- Teorija brojeva (klasična) se bavi ponajprije svojstima prirodnih brojeva, te cijelih i racionalnih brojevima.

Neka svojstva skupa prirodnih i skupa cijelih brojeva koja ćemo koristiti:

- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) su definirane operacije zbrajanja i množenja koje zadovoljavaju svojstva komutativnosti, asocijativnosti i distributivnosti;
- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) imamo uređaj takav da za svaka dva različita elementa $m, n \in \mathbb{N}$ ($\mathbb{Z}$) vrijedi ili $m < n$ ili $n < m$;
- Svaki neprazan podskup skupa $\mathbb{N}$ ima najmanji element i vrijedi princip matematičke indukcije;

Uvod

- Teorija brojeva (klasična) se bavi ponajprije svojstima prirodnih brojeva, te cijelih i racionalnih brojevima.

Neka svojstva skupa prirodnih i skupa cijelih brojeva koja ćemo koristiti:

- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) su definirane operacije zbrajanja i množenja koje zadovoljavaju svojstva komutativnosti, asocijativnosti i distributivnosti;
- Na skupu $\mathbb{N}$ ($\mathbb{Z}$) imamo uređaj takav da za svaka dva različita elementa $m, n \in \mathbb{N}$ ($\mathbb{Z}$) vrijedi ili $m < n$ ili $n < m$;
- Svaki neprazan podskup skupa $\mathbb{N}$ ima najmanji element i vrijedi princip matematičke indukcije;
- Osim svojstava skupa $\mathbb{N}$, proučavat ćemo i svojstva skupa cijelih brojeva $0, \pm 1, \pm 2, \pm 3, \ldots$ kojeg ćemo označavati sa $\mathbb{Z}$, te skupa racionalnih brojeva, tj. brojeva oblika $\frac{p}{q}$ za $p \in \mathbb{Z}$, $q \in \mathbb{N}$, kojeg ćemo označavati s $\mathbb{Q}$.

1. Djeljivost

Definicija (1.1)

Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da a dijeli b, odnosno da je b djeljiv s a, ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo s $a \mid b$. Broj a nazivamo djelitelj broja b, a broj b višekratnik broja a.

1. Djeljivost

Definicija (1.1)

Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da a dijeli b, odnosno da je b djeljiv s a, ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo s $a \mid b$. Broj a nazivamo djelitelj broja b, a broj b višekratnik broja a.
Ako b nije djeljiv s a, onda pišemo $a \nmid b$. Oznaku $a^k \parallel b$, $k \in \mathbb{N}$ ćemo koristiti kada $a^k \mid b$ i $a^{k+1} \nmid b$.

Zadatak (1.1)

Pokažite da je relacija "biti djeljiv" relacija parcijalnog uređaja na skupu $\mathbb{N}$, odnosno da za prirodne brojeve a, b, c vrijedi:

- $a \mid a$ *(refleksivnost)*;
- $a \mid b$ *i* $b \mid c \implies a \mid c$ *(tranzitivnost)*;
- $a \mid b$ *i* $b \mid a \implies a = b$ *(antisimetričnost)*.

Napomena:

- Relacija "biti djeljiv" nije relacija parcijalnog uređaja na skupu $\mathbb{Z} \setminus \{0\}$ jer $a \,|\, b$ i $b \,|\, a$, povlači $a = \pm b$, pa ne vrijedi antisimetričnost;

Napomena:

- Relacija "biti djeljiv" nije relacija parcijalnog uređaja na skupu $\mathbb{Z} \setminus \{0\}$ jer $a \,|\, b$ i $b \,|\, a$, povlači $a = \pm b$, pa ne vrijedi antisimetričnost;
- Za svaki cijeli broj a vrijedi $1 \,|\, a$.

Napomena:

- Relacija "biti djeljiv" nije relacija parcijalnog uređaja na skupu $\mathbb{Z} \setminus \{0\}$ jer $a \,|\, b$ i $b \,|\, a$, povlači $a = \pm b$, pa ne vrijedi antisimetričnost;
- Za svaki cijeli broj a vrijedi $1 \,|\, a$.
- Za svaki cijeli broj $a \neq 0$ vrijedi $a \,|\, 0$.

Napomena:

- Relacija "biti djeljiv" nije relacija parcijalnog uređaja na skupu $\mathbb{Z} \setminus \{0\}$ jer $a \,|\, b$ i $b \,|\, a$, povlači $a = \pm b$, pa ne vrijedi antisimetričnost;
- Za svaki cijeli broj a vrijedi $1 \,|\, a$.
- Za svaki cijeli broj $a \neq 0$ vrijedi $a \,|\, 0$.

Zadatak (1.2)

Ako su $a, b, d, m, n \in \mathbb{Z}$, $d \neq 0$, *onda vrijedi:*

- $d \,|\, a$ *i* $d \,|\, b \implies d \,|\, (an + bm)$;
- $d \,|\, a \implies md \,|\, ma$;
- $md \,|\, ma \implies d \,|\, a$;
- $d \,|\, a \implies \frac{a}{d} \,|\, a$,
  kad god je djelitelj različit od 0.

1.1. Teorem o dijeljenju s ostatkom

Teorem (Teorem o dijeljenju s ostatkom)

Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

$$b = aq + r \text{ i } 0 \leq r < a.$$

1.1. Teorem o dijeljenju s ostatkom

Teorem (Teorem o dijeljenju s ostatkom)

Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

$$b = aq + r \text{ i } 0 \leq r < a.$$

Dokaz: Dokažimo prvo postojanje takvih q i r.

1.1. Teorem o dijeljenju s ostatkom

Teorem (Teorem o dijeljenju s ostatkom)

Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

$$b = aq + r \text{ i } 0 \leq r < a.$$

Dokaz: Dokažimo prvo postojanje takvih q i r.

Promotrimo skup $S = \{b - am : m \in \mathbb{Z}\}$.

1.1. Teorem o dijeljenju s ostatkom

Teorem (Teorem o dijeljenju s ostatkom)

Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

$$b = aq + r \text{ i } 0 \leq r < a.$$

Dokaz: Dokažimo prvo postojanje takvih q i r.

Promotrimo skup $S = \{b - am : m \in \mathbb{Z}\}$.

Definirajmo $r := \min(S \cap \mathbb{N}_0)$.

1.1. Teorem o dijeljenju s ostatkom

Teorem (Teorem o dijeljenju s ostatkom)

Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

$$b = aq + r \text{ i } 0 \leq r < a.$$

Dokaz: Dokažimo prvo postojanje takvih q i r.

Promotrimo skup $S = \{b - am : m \in \mathbb{Z}\}$.

Definirajmo $r := \min(S \cap \mathbb{N}_0)$.

Tada je $0 \leq r < a$, pošto ako nije onda je $r - a \in S$, te $0 \leq r - a < r$, što je kontradikicja s minimalnošću od r.

1.1. Teorem o dijeljenju s ostatkom

Teorem (Teorem o dijeljenju s ostatkom)

Za proizvoljan prirodan broj a i proizvoljan cijeli broj b postoje jedinstveni cijeli brojevi q i r takvi da je

$$b = aq + r \text{ i } 0 \leq r < a.$$

Dokaz: Dokažimo prvo postojanje takvih q i r.

Promotrimo skup $S = \{b - am : m \in \mathbb{Z}\}$.

Definirajmo $r := \min(S \cap \mathbb{N}_0)$.

Tada je $0 \leq r < a$, pošto ako nije onda je $r - a \in S$, te $0 \leq r - a < r$, što je kontradikicja s minimalnošću od r.

Neka je $q \in \mathbb{Z}$ takav da je $b - qa = r$, tj. $b = qa + r$, čime smo završili dokaz postojanja.

Teorem o dijeljenju s ostatkom

Dakle postoje q, r takvi da je

$$b = aq + r \quad \text{i} \quad 0 \leq r < a.$$

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete, tj. $b = aq_1 + r_1$.

Teorem o dijeljenju s ostatkom

Dakle postoje q, r takvi da je

$$b = aq + r \quad \text{i} \quad 0 \leq r < a.$$

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete, tj. $b = aq_1 + r_1$.

Pokažimo najprije da je $r_1 = r$.

Teorem o dijeljenju s ostatkom

Dakle postoje q, r takvi da je

$$b = aq + r \quad \text{i} \quad 0 \leq r < a.$$

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete, tj. $b = aq_1 + r_1$.

Pokažimo najprije da je $r_1 = r$.

Pretpostavimo da je npr. $r < r_1$.

Teorem o dijeljenju s ostatkom

Dakle postoje q, r takvi da je

$$b = aq + r \quad \text{i} \quad 0 \leq r < a.$$

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete, tj. $b = aq_1 + r_1$.

Pokažimo najprije da je $r_1 = r$.

Pretpostavimo da je npr. $r < r_1$.

Tada je $0 < r_1 - r < a$, dok je s druge strane
$r_1 - r = a(q - q_1) \geq a$, što je kontradikcija.

Teorem o dijeljenju s ostatkom

Dakle postoje q, r takvi da je

$$b = aq + r \quad \text{i} \quad 0 \leq r < a.$$

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete, tj. $b = aq_1 + r_1$.

Pokažimo najprije da je $r_1 = r$.

Pretpostavimo da je npr. $r < r_1$.

Tada je $0 < r_1 - r < a$, dok je s druge strane $r_1 - r = a(q - q_1) \geq a$, što je kontradikcija.

Prema tome je $r_1 = r$, pa je stoga i $0 = r_1 - r = a(q_1 - q)$, iz čega zaključujemo da je $q = q_1$. □

Teorem o dijeljenju s ostatkom

Dakle postoje q, r takvi da je

$$b = aq + r \quad \text{i} \quad 0 \leq r < a.$$

Da bi dokazali jedinstvenost od q i r, pretpostavimo da postoji još jedan par q_1, r_1 koji zadovoljava iste uvjete, tj. $b = aq_1 + r_1$.

Pokažimo najprije da je $r_1 = r$.

Pretpostavimo da je npr. $r < r_1$.

Tada je $0 < r_1 - r < a$, dok je s druge strane $r_1 - r = a(q - q_1) \geq a$, što je kontradikcija.

Prema tome je $r_1 = r$, pa je stoga i $0 = r_1 - r = a(q_1 - q)$, iz čega zaključujemo da je $q = q_1$. □

Napomena: Broj r iz Teorema 1.1 nazivamo ostatak, a broj q kvocijent, pri dijeljenju b s a. Uočimo da je u Teoremu 1.1 $r = 0$ ako i samo ako a dijeli b. Dakle, a dijeli b ako i samo ako je ostatak pri dijeljenju b s a jednak 0.

Definicija (1.2)

Broj $d \in \mathbb{Z}$ nazivamo zajednički djelitelj od a i b ako $d \mid a$ i $d \mid b$.

Definicija (1.2)

Broj $d \in \mathbb{Z}$ nazivamo zajednički djelitelj od a i b ako $d \mid a$ i $d \mid b$. Ako je barem jedan od brojeva a i b različit od nule, onda postoji konačno mnogo zajedničikih djeliteja od a i b i najveći među njima nazivamo najveći zajednički djelitelj od a i b i označavamo s

$$\gcd(a, b) \text{ ili } nzd(a, b) \text{ ili samo } (a, b).$$

Definicija (1.2)

Broj $d \in \mathbb{Z}$ nazivamo zajednički djelitelj od a i b ako $d \mid a$ i $d \mid b$. Ako je barem jedan od brojeva a i b različit od nule, onda postoji konačno mnogo zajedničikih djeliteja od a i b i najveći među njima nazivamo najveći zajednički djelitelj od a i b i označavamo s

$$\gcd(a, b) \text{ ili } nzd(a, b) \text{ ili samo } (a, b).$$

Na sličan način definiramo najveći zajednički djelitelj za bilo koji konačan skup cijelih brojeva $a_1, a_2, \ldots, a_n$, a označavamo ga s $(a_1, a_2, \ldots, a_n)$.

Definicija (1.2)

Broj $d \in \mathbb{Z}$ nazivamo zajednički djelitelj od a i b ako $d \mid a$ i $d \mid b$. Ako je barem jedan od brojeva a i b različit od nule, onda postoji konačno mnogo zajedničikih djeliteja od a i b i najveći među njima nazivamo najveći zajednički djelitelj od a i b i označavamo s

$$\gcd(a, b) \text{ ili } nzd(a, b) \text{ ili samo } (a, b).$$

Na sličan način definiramo najveći zajednički djelitelj za bilo koji konačan skup cijelih brojeva $a_1, a_2, \ldots, a_n$, a označavamo ga s $(a_1, a_2, \ldots, a_n)$.

Uočimo:

- Svaki prirodan broj $a > 1$ ima uvijek dva djelitelja 1 i a. Njih nazivamo *trivijalni djelitelji*.
- $(a, b) \geq 1$.
- $(a, 0) = |a|$, za svaki $a \in \mathbb{Z}$, $a \neq 0$.

Teorem (1.2)

Neka su $b, c \in \mathbb{Z}$ *od kojih je barem jedan različit od nule. Neka je*

$$S = \{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je $(b, c) = \min S$.

Teorem (1.2)

Neka su $b, c \in \mathbb{Z}$ od kojih je barem jedan različit od nule. Neka je

$$S = \{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je $(b, c) = \min S$.

Dokaz:
Neka je $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

Teorem (1.2)

Neka su $b, c \in \mathbb{Z}$ *od kojih je barem jedan različit od nule. Neka je*

$$S = \{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je $(b, c) = \min S$.

Dokaz:
Neka je $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

To znači da postoje cijeli brojevi x_0 i y_0 takvi da je $\ell = bx_0 + cy_0$.

Teorem (1.2)

Neka su $b, c \in \mathbb{Z}$ *od kojih je barem jedan različit od nule. Neka je*

$$S = \{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je $(b, c) = \min S$.

Dokaz:
Neka je $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

To znači da postoje cijeli brojevi x_0 i y_0 takvi da je $\ell = bx_0 + cy_0$.

Pokažimo da $\ell | b$ i $\ell | c$. Pretpostavimo da npr. $\ell \nmid b$.

Teorem (1.2)

Neka su $b, c \in \mathbb{Z}$ *od kojih je barem jedan različit od nule. Neka je*

$$S = \{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je $(b, c) = \min S$.

Dokaz:
Neka je $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

To znači da postoje cijeli brojevi x_0 i y_0 takvi da je $\ell = bx_0 + cy_0$.

Pokažimo da $\ell | b$ i $\ell | c$. Pretpostavimo da npr. $\ell \nmid b$.

Tada po Teoremu 1.1. postoje cijeli brojevi q i r takvi da je $b = \ell q + r$ i $0 < r < \ell$.

Teorem (1.2)

Neka su $b, c \in \mathbb{Z}$ od kojih je barem jedan različit od nule. Neka je

$$S = \{bx + cy : x, y \in \mathbb{Z}\} \cap \mathbb{N},$$

tada je $(b, c) = \min S$.

Dokaz:
Neka je $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \ : \ x, y \in \mathbb{Z}\} \cap \mathbb{N}.$$

To znači da postoje cijeli brojevi x_0 i y_0 takvi da je $\ell = bx_0 + cy_0$.

Pokažimo da $\ell | b$ i $\ell | c$. Pretpostavimo da npr. $\ell \nmid b$.

Tada po Teoremu 1.1. postoje cijeli brojevi q i r takvi da je $b = \ell q + r$ i $0 < r < \ell$.

Sada je

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

što je u suprotnosti s minimalnošću od ℓ.

Dakle, $\ell | b$, a na isti način se pokazuje da $\ell | c$. To znači da je $\ell \leq g$.

Dakle, $\ell | b$, a na isti način se pokazuje da $\ell | c$. To znači da je $\ell \leq g$.

Imamo kao i prije $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Dakle, $\ell | b$, a na isti način se pokazuje da $\ell | c$. To znači da je $\ell \leq g$.

Imamo kao i prije $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Dakle do sada smo dokazali da je $\ell \leq g$, dokažimo sada i $\ell \geq g$.

Dakle, $\ell | b$, a na isti način se pokazuje da $\ell | c$. To znači da je $\ell \leq g$.

Imamo kao i prije $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Dakle do sada smo dokazali da je $\ell \leq g$, dokažimo sada i $\ell \geq g$.

Budući da je $g = (b, c)$, postoje $\beta, \gamma \in \mathbb{Z}$ takvi da je $b = g\beta$, $c = g\gamma$, pa je $\ell = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0)$.

Dakle, $\ell | b$, a na isti način se pokazuje da $\ell | c$. To znači da je $\ell \leq g$.

Imamo kao i prije $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Dakle do sada smo dokazali da je $\ell \leq g$, dokažimo sada i $\ell \geq g$.

Budući da je $g = (b, c)$, postoje $\beta, \gamma \in \mathbb{Z}$ takvi da je $b = g\beta$, $c = g\gamma$, pa je $\ell = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0)$.

Odavde slijedi da $g \mid \ell$, pa je onda $g \leq \ell$, te smo dokazali da je $g = \ell$. □

Dakle, $\ell | b$, a na isti način se pokazuje da $\ell | c$. To znači da je $\ell \leq g$.

Imamo kao i prije $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Dakle do sada smo dokazali da je $\ell \leq g$, dokažimo sada i $\ell \geq g$.

Budući da je $g = (b, c)$, postoje $\beta, \gamma \in \mathbb{Z}$ takvi da je $b = g\beta$, $c = g\gamma$, pa je $\ell = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0)$.

Odavde slijedi da $g \mid \ell$, pa je onda $g \leq \ell$, te smo dokazali da je $g = \ell$. □

Ako se cijeli broj d može prikazati u obliku $d = bx + cy$, onda je (b, c) djelitelj od d. Posebno, ako je $bx + cy = 1$, onda je $(b, c) = 1$.

Dakle, $\ell | b$, a na isti način se pokazuje da $\ell | c$. To znači da je $\ell \leq g$.

Imamo kao i prije $g = (b, c)$, te neka je

$$\ell := \min S = \min(\{bx + cy \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}).$$

Dakle do sada smo dokazali da je $\ell \leq g$, dokažimo sada i $\ell \geq g$.

Budući da je $g = (b, c)$, postoje $\beta, \gamma \in \mathbb{Z}$ takvi da je $b = g\beta$, $c = g\gamma$, pa je $\ell = bx_0 + cy_0 = g(\beta x_0 + \gamma y_0)$.

Odavde slijedi da $g \mid \ell$, pa je onda $g \leq \ell$, te smo dokazali da je $g = \ell$. □

Ako se cijeli broj d može prikazati u obliku $d = bx + cy$, onda je (b, c) djelitelj od d. Posebno, ako je $bx + cy = 1$, onda je $(b, c) = 1$.

Ako je d zajednički djeljitelj od b i c, onda $d \mid (b, c)$. Zaista, d dijeli b i c, pa onda dijeli i $bx + cy$, te tvrdnja slijedi iz Teorema 1.2.

Definicija (1.3)

Kažemo da su cijeli brojevi a i b relativno prosti, ako je $(a, b) = 1$.

Definicija (1.3)

Kažemo da su cijeli brojevi a i b relativno prosti, ako je $(a, b) = 1$.

Za cijele brojeve $a_1, a_2, \ldots, a_n$ kažemo da su relativno prosti ako je $(a_1, a_2, \ldots, a_n) = 1$, a da su u parovima relativno prosti ako je $(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.

Definicija (1.3)

Kažemo da su cijeli brojevi a i b relativno prosti, ako je $(a, b) = 1$.

Za cijele brojeve $a_1, a_2, \ldots, a_n$ kažemo da su relativno prosti ako je $(a_1, a_2, \ldots, a_n) = 1$, a da su u parovima relativno prosti ako je $(a_i, a_j) = 1$ za sve $1 \leq i, j \leq n$, $i \neq j$.

Napomena

Biti u parovima relativno prost je jače svojstvo od biti relativno prost, tj. ako su $a_1, a_2, \ldots, a_n$ u parovima relativno prosti, onda su oni relativno prosti, ali obrnuto ne vrijedi!

Zadatak

Nađite kontraprimjer koji dokazuje drugu tvrdnju iz prethodne napomene!

Propozicija (1.1)

Neka su $a, b, m \in \mathbb{Z}$. *Ako je* $(a, m) = (b, m) = 1$, *onda je* $(ab, m) = 1$.

Propozicija (1.1)

Neka su $a, b, m \in \mathbb{Z}$. *Ako je* $(a, m) = (b, m) = 1$, *onda je* $(ab, m) = 1$.

Dokaz:

Po Teoremu 1.2. postoje $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ takvi da je

$$1 = ax_0 + my_0 \quad \text{i} \quad 1 = bx_1 + my_1.$$

Propozicija (1.1)

Neka su $a, b, m \in \mathbb{Z}$. *Ako je* $(a, m) = (b, m) = 1$, *onda je* $(ab, m) = 1$.

Dokaz:

Po Teoremu 1.2. postoje $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ takvi da je

$$1 = ax_0 + my_0 \quad \text{i} \quad 1 = bx_1 + my_1.$$

Odavde je

$$ax_0 bx_1 = (1 - my_0)(1 - my_1) = 1 - m(y_0 + y_1 - my_0 y_1) = 1 - my_2,$$

gdje je $y_2 = y_0 + y_1 - my_0 y_1$.

Propozicija (1.1)

Neka su $a, b, m \in \mathbb{Z}$. *Ako je* $(a, m) = (b, m) = 1$, *onda je* $(ab, m) = 1$.

Dokaz:

Po Teoremu 1.2. postoje $x_0, y_0, x_1, y_1 \in \mathbb{Z}$ takvi da je

$$1 = ax_0 + my_0 \quad \text{i} \quad 1 = bx_1 + my_1.$$

Odavde je

$$ax_0 bx_1 = (1 - my_0)(1 - my_1) = 1 - m(y_0 + y_1 - my_0 y_1) = 1 - my_2,$$

gdje je $y_2 = y_0 + y_1 - my_0 y_1$.

Sada iz $ab(x_0 x_1) + m(y_2) = 1$ zaključujemo da je $(ab, m) = 1$. $\square$

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Dokaz:

Označimo $(a, b) = d$, $(a, b + ax) = g$.

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Dokaz:

Označimo $(a, b) = d$, $(a, b + ax) = g$.

Po Teoremu 1.2. postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$, odnosno dodavanjem i oduzimanjem axy_0,

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Dokaz:

Označimo $(a, b) = d$, $(a, b + ax) = g$.

Po Teoremu 1.2. postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$, odnosno dodavanjem i oduzimanjem axy_0,

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Odavdje slijedi da $g|d$, pošto je $(a, b + ax) = g$. Pokažimo sada da $d|g$.

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Dokaz:

Označimo $(a, b) = d$, $(a, b + ax) = g$.

Po Teoremu 1.2. postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$, odnosno dodavanjem i oduzimanjem axy_0,

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Odavdje slijedi da $g|d$, pošto je $(a, b + ax) = g$. Pokažimo sada da $d|g$.

Budući $d|a$ i $d|b$, imamo da $d|(b + ax)$.

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Dokaz:

Označimo $(a, b) = d$, $(a, b + ax) = g$.

Po Teoremu 1.2. postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$, odnosno dodavanjem i oduzimanjem axy_0,

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Odavdje slijedi da $g|d$, pošto je $(a, b + ax) = g$. Pokažimo sada da $d|g$.

Budući $d|a$ i $d|b$, imamo da $d|(b + ax)$.

Dakle, d je zajednički djelitelj od a i $b + ax$, pa po Teoremu 1.2. imamo da $d|g$.

Propozicija (1.2)

Neka su $a, b \in \mathbb{Z}$, *tada je* $(a, b) = (a, b + ax)$ *za svaki* $x \in \mathbb{Z}$.

Dokaz:

Označimo $(a, b) = d$, $(a, b + ax) = g$.

Po Teoremu 1.2. postoje $x_0, y_0 \in \mathbb{Z}$ takvi da je $d = ax_0 + by_0$, odnosno dodavanjem i oduzimanjem axy_0,

$$d = a(x_0 - xy_0) + (b + ax)y_0.$$

Odavdje slijedi da $g|d$, pošto je $(a, b + ax) = g$. Pokažimo sada da $d|g$.

Budući $d|a$ i $d|b$, imamo da $d|(b + ax)$.

Dakle, d je zajednički djelitelj od a i $b + ax$, pa po Teoremu 1.2. imamo da $d|g$.

Pošto su brojevi d i g pozitivni po definiciji, iz $d|g$ i $g|d$ slijedi da je $d = g$.

Teorem (1.3 Euklidov algoritam)

Neka su dani $b \in \mathbb{Z}$ i $c \in \mathbb{N}$. Pretpostavimo da je uzastopnom primjenom Teorema 1.1 dobiven niz jednakosti

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Tada je $(b, c) = r_j$, tj. (b, c) je jednak posljednjem ostatku različitom od 0.

Teorem (1.3 Euklidov algoritam)

Neka su dani $b \in \mathbb{Z}$ i $c \in \mathbb{N}$. Pretpostavimo da je uzastopnom primjenom Teorema 1.1 dobiven niz jednakosti

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Tada je $(b, c) = r_j$, tj. (b, c) je jednak posljednjem ostatku različitom od 0.
Brojevi $x_0, y_0 \in \mathbb{Z}$ takvi da je

$$(b, c) = r_j = bx_0 + cy_0, \qquad (**)$$

mogu se dobiti izražavanjem svakog r_i kao lin. kombinacije od a i b.

Dokaz: Prepišimo:

$$
\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}
$$

Dokazujemo prvo da je $(b, c) = r_j$.

Dokaz: Prepišimo:

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Dokazujemo prvo da je $(b, c) = r_j$.

Po Propoziciji 1.2 imamo

$$(b, c) = (b - cq_1, c) = (r_1, c) = (r_1, c - r_1 q_2) = (r_1, r_2)$$

$$= (r_1 - r_2 q_3, r_2) = (r_3, r_2).$$

Dokaz: Prepišimo:

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Dokazujemo prvo da je $(b, c) = r_j$.

Po Propoziciji 1.2 imamo

$$(b, c) = (b - cq_1, c) = (r_1, c) = (r_1, c - r_1 q_2) = (r_1, r_2)$$

$$= (r_1 - r_2 q_3, r_2) = (r_3, r_2).$$

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

Prepišimo opet:

$$\begin{aligned}
b &= cq_1 + r_1, \quad 0 < r_1 < c, \\
c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\
&\dots \\
r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\
r_{j-1} &= r_j q_{j+1}.
\end{aligned}$$

Sada indukcijom dokazujemo da je svaki r_i linearna kombinacija od b i c.

Prepišimo opet:

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_j q_{j+1}. \end{aligned}$$

Sada indukcijom dokazujemo da je svaki r_i linearna kombinacija od b i c.

To je točno za

$$r_1 = b - cq_1 \qquad \text{i}$$

$$r_2 = c - r_1 q_2 = c - (b - cq_1)q_2 = -bq_1 + c(1 + q_1 q_2),$$

pa pretpostavimo da vrijedi za r_{i-1} i r_{i-2}.

Prepišimo opet:

$$\begin{aligned} b &= cq_1 + r_1, \quad 0 < r_1 < c, \\ c &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2, \\ &\dots \\ r_{j-2} &= r_{j-1} q_j + r_j, \quad 0 < r_j < r_{j-1}, \\ r_{j-1} &= r_j q_{j+1}. \end{aligned}$$

Sada indukcijom dokazujemo da je svaki r_i linearna kombinacija od b i c.

To je točno za

$$r_1 = b - cq_1 \qquad \text{i}$$

$$r_2 = c - r_1 q_2 = c - (b - cq_1)q_2 = -bq_1 + c(1 + q_1 q_2),$$

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.

Napomena

- *U Euklidovom algoritmu smo pretpostavili da je* $c > 0$ *što nije bitno ograničenje jer je* $(b, c) = (|b|, |c|)$;

Napomena

- *U Euklidovom algoritmu smo pretpostavili da je* $c > 0$ *što nije bitno ograničenje jer je* $(b, c) = (|b|, |c|)$;
- *Ako su* $b, c \in \mathbb{N}$ *i* $b < c$, *onda u prvom koraku imamo* $b = c \cdot 0 + a$, *pa* b *i* c *zamijene mjesta;*

Napomena

- *U Euklidovom algoritmu smo pretpostavili da je* $c > 0$ *što nije bitno ograničenje jer je* $(b, c) = (|b|, |c|)$;
- *Ako su* $b, c \in \mathbb{N}$ *i* $b < c$, *onda u prvom koraku imamo* $b = c \cdot 0 + a$, *pa* b *i* c *zamijene mjesta;*
- *Primijetimo da je (konačan) niz ostataka u (*)* $r_0 = c$, $r_1, r_2, \ldots, r_k$ *strogo padajući niz;*

Napomena

- *U Euklidovom algoritmu smo pretpostavili da je* $c > 0$ *što nije bitno ograničenje jer je* $(b, c) = (|b|, |c|)$;
- *Ako su* $b, c \in \mathbb{N}$ *i* $b < c$, *onda u prvom koraku imamo* $b = c \cdot 0 + a$, *pa* b *i* c *zamijene mjesta;*
- *Primijetimo da je (konačan) niz ostataka u (*)* $r_0 = c$, $r_1, r_2, \ldots, r_k$ *strogo padajući niz;*
- *Primijetimo da je*

$$\left\lfloor \frac{b}{c} \right\rfloor = q_1, \qquad \left\lfloor \frac{c}{r_1} \right\rfloor = q_2, \qquad \left\lfloor \frac{r_1}{r_2} \right\rfloor = q_3 \quad \ldots,$$

gdje je $\lfloor x \rfloor$ *najveći cijeli dio od* x, *tj.* $\lfloor x \rfloor = q$, *gdje je* q *najveći cijeli broj* $\leq x$.

Napomena

- *U Euklidovom algoritmu smo pretpostavili da je* $c > 0$ *što nije bitno ograničenje jer je* $(b, c) = (|b|, |c|)$;
- *Ako su* $b, c \in \mathbb{N}$ *i* $b < c$, *onda u prvom koraku imamo* $b = c \cdot 0 + a$, *pa* b *i* c *zamijene mjesta;*
- *Primijetimo da je (konačan) niz ostataka u (*)* $r_0 = c$, $r_1, r_2, \ldots, r_k$ *strogo padajući niz;*
- *Primijetimo da je*

$$\left\lfloor \frac{b}{c} \right\rfloor = q_1, \qquad \left\lfloor \frac{c}{r_1} \right\rfloor = q_2, \qquad \left\lfloor \frac{r_1}{r_2} \right\rfloor = q_3 \quad \ldots,$$

  gdje je $\lfloor x \rfloor$ *najveći cijeli dio od* x, *tj.* $\lfloor x \rfloor = q$, *gdje je* q *najveći cijeli broj* $\leq x$.
- *Brojevi* $x_0, y_0 \in \mathbb{Z}$ *u (**) nisu jednoznačno određeni, jer je npr.*

$$(b, c) = bx_0 + cy_0 = (x_0 + c)\, b + (y_0 - b)\, c.$$

Rješenja jednadžbe $bx + cy = (b, c)$ mogu se efikasno dobiti na slijedeći način: ako je

$$\begin{aligned} r_{-1} &= b, \quad r_0 = c; \quad r_i = r_{i-2} - q_i r_{i-1}; \\ x_{-1} &= 1, \quad x_0 = 0; \quad x_i = x_{i-2} - q_i x_{i-1}; \\ y_{-1} &= 0, \quad y_0 = 1; \quad y_i = y_{i-2} - q_i y_{i-1}, \end{aligned}$$

onda je

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

Rješenja jednadžbe $bx + cy = (b, c)$ mogu se efikasno dobiti na slijedeći način: ako je

$$\begin{aligned} r_{-1} &= b, \quad r_0 = c; \quad r_i = r_{i-2} - q_i r_{i-1}; \\ x_{-1} &= 1, \quad x_0 = 0; \quad x_i = x_{i-2} - q_i x_{i-1}; \\ y_{-1} &= 0, \quad y_0 = 1; \quad y_i = y_{i-2} - q_i y_{i-1}, \end{aligned}$$

onda je

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

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

$$bx_j + cy_j = (b, c).$$

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

$$252 = 198 \cdot 1 + 54$$

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

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

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

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

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

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

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

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

Nadalje, imamo:

$$\begin{aligned} 18 &= 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) \cdot 1 = 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 198 \cdot 1) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198. \end{aligned}$$

Primjer (1.1)

Odredimo $d = (252, 198)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 252 *i* 198.

Rješenje:

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

Nadalje, imamo:

$$\begin{aligned} 18 &= 54 - 36 \cdot 1 = 54 - (198 - 54 \cdot 3) \cdot 1 = 4 \cdot 54 - 1 \cdot 198 \\ &= 4 \cdot (252 - 198 \cdot 1) - 1 \cdot 198 = 4 \cdot 252 - 5 \cdot 198. \end{aligned}$$

Zadatak

Odredite $g = (423, 198)$ *i nađite cijele brojeve* x, y *takve da je* $423x + 198y = g$.

Zadatak

Odredite cijele brojeve x, y *takve da je*

a) $71x + 50y = 1$, *b)* $93x + 81y = 3$.

Primjer (1.2)

Odredimo $d = (3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Primjer (1.2)

Odredimo $d = (3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Primjer (1.2)

Odredimo $d = (3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$3587 = 1819 \cdot 1 + 1768$$

Primjer (1.2)

Odredimo $d = (3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \end{aligned}$$

Primjer (1.2)

Odredimo $d = (3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \end{aligned}$$

Primjer (1.2)

Odredimo $d = (3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \\ 51 &= 34 \cdot 1 + 17 \end{aligned}$$

Primjer (1.2)

Odredimo $d = (3587, 1819)$ *i prikažimo* d *kao linearnu kombinaciju brojeva* 3587 *i* 1819.

Rješenje:

$$\begin{aligned} 3587 &= 1819 \cdot 1 + 1768 \\ 1819 &= 1768 \cdot 1 + 51 \\ 1768 &= 51 \cdot 34 + 34 \\ 51 &= 34 \cdot 1 + 17 \\ 34 &= 17 \cdot 2 \end{aligned}$$

Sjetimo se rekurzije:

$$\begin{aligned} r_{-1} &= b, \quad r_0 = c; \quad r_i = r_{i-2} - q_i r_{i-1}; \\ x_{-1} &= 1, \quad x_0 = 0; \quad x_i = x_{i-2} - q_i x_{i-1}; \\ y_{-1} &= 0, \quad y_0 = 1; \quad y_i = y_{i-2} - q_i y_{i-1}, \end{aligned}$$

Rješenje rekurzijom:

i	-1	0	1	2	3	4
q_i			1	1	34	1
x_i	1	0	1	-1	35	-36
y_i	0	1	-1	2	-69	71

Dakle, $d = 17$, te $3587 \cdot (-36) + 1819 \cdot 71 = 17$.

Definicija

Prirodan broj $p > 1$ *se zove 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.*

Definicija

Prirodan broj $p > 1$ se zove 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.

Teorem

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

Definicija

Prirodan broj $p > 1$ se zove 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.

Teorem

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

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Definicija

Prirodan broj $p > 1$ se zove 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.

Teorem

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

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. Pretpostavimo da je $n > 2$, te da tvrdnja teorema vrijedi za sve m, $2 \leq m < n$.

Definicija

Prirodan broj $p > 1$ se zove 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.

Teorem

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

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. 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.

Definicija

Prirodan broj $p > 1$ se zove 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.

Teorem

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

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. 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, nemamo što dokazivati.

Definicija

Prirodan broj $p > 1$ se zove 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.

Teorem

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

Dokaz: Dokazat ćemo teorem matematičkom indukcijom.

Broj 2 je prost. 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, 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.

Iz prošlog Teorema slijedi da svaki prirodan broj n možemo prikazati 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.

Iz prošlog Teorema slijedi da svaki prirodan broj n možemo prikazati 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.

Ovakav prikaz broja n zvat ćemo *kanonski rastav* broja n na proste faktore.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Sada je $abx + pby = b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Sada je $abx + pby = b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Sada je $abx + pby = b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora.

Sada ako $p|a_1(a_2 \cdots a_n)$, onda $p|a_1$ ili $p|a_2 a_3 \cdots a_n$.

Propozicija

Ako je p prost broj i $p|ab$, onda $p|a$ ili $p|b$. Općenitije, ako $p|a_1 a_2 \cdots a_n$, onda p dijeli barem jedan faktor a_i.

Dokaz:

Ako $p \nmid a$, onda je $(p, a) = 1$, pa postoje cijeli brojevi x i y takvi da je $ax + py = 1$.

Sada je $abx + pby = b$, pa pošto p dijeli ab, slijedi da p dijeli lijevu stranu, pa dijeli i b.

Općenitiju tvrdnju dokazujemo indukcijom. Pretpostavimo da tvrdnja vrijedi za produkte s manje od n faktora.

Sada ako $p|a_1(a_2 \cdots a_n)$, onda $p|a_1$ ili $p|a_2 a_3 \cdots a_n$.

Ako $p|a_2 a_3 \cdots a_n$, onda po induktivnoj pretpostavci $p|a_i$ za neki $i = 2, \ldots, n$. □

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobit ćemo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i,j.

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobit ćemo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i,j.

Međutim, to je nemoguće jer iz $p_1 | q_1 q_2 \cdots q_s$, po prethodnoj Propoziciji, slijedi pa p_1 dijeli barem jedan q_j.

Teorem (Osnovni teorem aritmetike)

Faktorizacija svakog prirodnog broja $n > 1$ na proste faktore je jedinstvena do na poredak prostih faktora.

Dokaz:

Pretpostavimo da n ima dvije različite faktorizacije.

Dijeleći s prostim brojevima koji su zajednički objema reprezentacijama, dobit ćemo jednakost oblika

$$p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s,$$

gdje su p_i, q_j prosti brojevi, ne nužno različiti, ali takvi da se niti jedan prost broj s lijeve strane ne pojavljuje na desnoj strani, tj. $p_i \neq q_j$ za sve i,j.

Međutim, to je nemoguće jer iz $p_1 | q_1 q_2 \cdots q_s$, po prethodnoj Propoziciji, slijedi pa p_1 dijeli barem jedan q_j.

No, to znači da je $p_1 = q_j$, kontradikcija. □

Napomena

Kasnije na kolegiju ćemo vidjeti da analogon Osnovnog teorema aritmetike ne vrijedi za cijele brojeve u (nekim) općenitijim poljima.

Napomena

Kasnije na kolegiju ćemo vidjeti da analogon Osnovnog teorema aritmetike ne vrijedi za cijele brojeve u (nekim) općenitijim poljima.

Za sada, kao primjer nejednoznačne faktorizacije na proste faktore u prstenu $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ *navedimo ove dvije faktorizacije broja* 10*:*

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

Napomena

Kasnije na kolegiju ćemo vidjeti da analogon Osnovnog teorema aritmetike ne vrijedi za cijele brojeve u (nekim) općenitijim poljima.

Za sada, kao primjer nejednoznačne faktorizacije na proste faktore u prstenu $\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} : a, b \in \mathbb{Z}\}$ *navedimo ove dvije faktorizacije broja* 10*:*

$$10 = 2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6}).$$

U primjenama Osnovnog teorema aritmetike često ćemo prirodan broj a pisati u obliku $a = \prod_p p^{\alpha(p)}$, gdje je $\alpha(p) \geq 0$ i podrazumijevamo da je $\alpha(p) = 0$ za skoro sve proste brojeve p. Ako je $a = 1$, onda je $\alpha(p) = 0$ za sve p.

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Dakle, ako $a|c$, onda je $\alpha(p) \leq \gamma(p)$.

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Dakle, ako $a|c$, onda je $\alpha(p) \leq \gamma(p)$.

Obratno, ako je $\alpha(p) \leq \gamma(p)$, onda možemo definirati prirodan broj $b = \prod_p p^{\beta(p)}$ sa $\beta(p) = \gamma(p) - \alpha(p)$. Tada je $ab = c$, pa $a|c$.

Ako je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$, $c = \prod_p p^{\gamma(p)}$ i $ab = c$, onda je

$$\alpha(p) + \beta(p) = \gamma(p) \text{ za sve } p.$$

Dakle, ako $a|c$, onda je $\alpha(p) \leq \gamma(p)$.

Obratno, ako je $\alpha(p) \leq \gamma(p)$, onda možemo definirati prirodan broj $b = \prod_p p^{\beta(p)}$ sa $\beta(p) = \gamma(p) - \alpha(p)$. Tada je $ab = c$, pa $a|c$.

Prema tome, dobili smo da vrijedi

$$a|c \iff \alpha(p) \leq \gamma(p), \quad \forall p. \tag{1}$$

Kao posljedicu formule (1) dobivamo formulu

$$(a, b) = \prod_p p^{\min(\alpha(p), \beta(p))}. \tag{2}$$

Definicija

Neka su $a_1, a_2, \ldots, a_n$ *cijeli brojevi različiti od nule. Najmanji prirodan broj* c *za koji vrijedi da* $a_i | c$ *za sve* $i = 1, 2, \ldots, n$ *zove se najmanji zajednički višekratnik i označava s* $[a_1, a_2, \ldots, a_n]$.

Slijedi da je

$$[a, b] = \prod_p p^{\max(\alpha(p),\beta(p))}. \tag{3}$$

Slijedi da je

$$[a, b] = \prod_p p^{\max(\alpha(p),\beta(p))}. \tag{3}$$

Propozicija

$$(a, b) \cdot [a, b] = |ab|$$

Slijedi da je

$$[a, b] = \prod_p p^{\max(\alpha(p),\beta(p))}. \tag{3}$$

Propozicija

$$(a, b) \cdot [a, b] = |ab|$$

Dokaz:

Po Osnovnom teoremu aritmetike i ranije dokazanom, dovoljno je provjeriti da za sve realne brojeve x, y vrijedi:

$$\min(x, y) + \max(x, y) = x + y.$$

Slijedi da je

$$[a, b] = \prod_p p^{\max(\alpha(p),\beta(p))}. \tag{3}$$

Propozicija

$$(a, b) \cdot [a, b] = |ab|$$

Dokaz:

Po Osnovnom teoremu aritmetike i ranije dokazanom, dovoljno je provjeriti da za sve realne brojeve x, y vrijedi:

$$\min(x, y) + \max(x, y) = x + y.$$

Zaista, ako je $x \leq y$, onda je $\min(x, y) + \max(x, y) = x + y$, a ako je $x > y$, onda je $\min(x, y) + \max(x, y) = y + x = x + y$. □

Zadatak

Odredite $[482, 1687]$.

Reći ćemo da je prirodan broj *a (potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Reći ćemo da je prirodan broj a *(potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Reći ćemo da je prirodan broj a *(potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Kažemo da je a *kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a.

Reći ćemo da je prirodan broj a *(potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Kažemo da je a *kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a.

Stoga je a kvadratno slobodan ako i samo ako su svi eksponenti $\alpha(p)$ jednaki 0 ili 1.

Reći ćemo da je prirodan broj a *(potpun) kvadrat* ako se može zapisati u obliku n^2, $n \in \mathbb{N}$.

Odmah vidimo da je a potpun kvadrat ako i samo ako su svi eksponenti $\alpha(p)$ parni.

Kažemo da je a *kvadratno slobodan* ako je 1 najveći kvadrat koji dijeli a.

Stoga je a kvadratno slobodan ako i samo ako su svi eksponenti $\alpha(p)$ jednaki 0 ili 1.

Ako je p prost, onda je $p^k \| a \iff k = \alpha(p)$.

Primjer

Neka su a i b prirodni brojevi takvi da je $(a, b) = 1$, te da je ab potpun kvadrat. Dokažite da su tada a i b potpuni kvadrati.

Primjer

Neka su a i b prirodni brojevi takvi da je $(a, b) = 1$, te da je ab potpun kvadrat. Dokažite da su tada a i b potpuni kvadrati.

Neka je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$.

Primjer

Neka su a i b prirodni brojevi takvi da je $(a, b) = 1$, te da je ab potpun kvadrat. Dokažite da su tada a i b potpuni kvadrati.

Neka je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$.

Budući da je ab potpun kvadrat, broj $\alpha(p) + \beta(p)$ je paran za sve p.

Primjer

Neka su a i b prirodni brojevi takvi da je $(a, b) = 1$, te da je ab potpun kvadrat. Dokažite da su tada a i b potpuni kvadrati.

Neka je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$.

Budući da je ab potpun kvadrat, broj $\alpha(p) + \beta(p)$ je paran za sve p.

S druge strane, $(a, b) = 1$ povlači da je za sve p barem jedan od brojeva $\alpha(p)$, $\beta(p)$ jednak 0.

Primjer

Neka su a i b prirodni brojevi takvi da je $(a, b) = 1$, te da je ab potpun kvadrat. Dokažite da su tada a i b potpuni kvadrati.

Neka je $a = \prod_p p^{\alpha(p)}$, $b = \prod_p p^{\beta(p)}$.

Budući da je ab potpun kvadrat, broj $\alpha(p) + \beta(p)$ je paran za sve p.

S druge strane, $(a, b) = 1$ povlači da je za sve p barem jedan od brojeva $\alpha(p)$, $\beta(p)$ jednak 0.

Zo znači da su brojevi $\alpha(p)$ i $\beta(p)$ parni za sve p, pa su a i b potpuni kvadrati.

Zadatak

Nađite prirodan broj n sa svojstvom da je $\frac{n}{2}$ kvadrat, $\frac{n}{3}$ kub, a $\frac{n}{5}$ peta potencija nekog prirodnog broja.

Primjer

Dokažite da svaki složen broj n ima prosti faktor $p \leq \sqrt{n}$.

Neka je p najmanji djelitelj od n koji je veći od 1.

Primjer

Dokažite da svaki složen broj n ima prosti faktor $p \leq \sqrt{n}$.

Neka je p najmanji djelitelj od n koji je veći od 1.

Tada je p očito prost i postoji $m \in \mathbb{N}$ takav da je $n = p \cdot m$.

Primjer

Dokažite da svaki složen broj n ima prosti faktor $p \leq \sqrt{n}$.

Neka je p najmanji djelitelj od n koji je veći od 1.

Tada je p očito prost i postoji $m \in \mathbb{N}$ takav da je $n = p \cdot m$.

Budući da je $m \geq p$, dobivamo da je $n \geq p^2$, pa je $p \leq \sqrt{n}$.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5.

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5.

U svakom koraku, prvi neprekriženi broj je prost, te u idućem koraku križamo njegove prave višekratnike (prvi novoprekriženi broj će biti njegov kvadrat, jer su svi manji višekratnici već ranije prekriženi).

Prethodni primjer možemo iskoristiti za generiranje tablice prostih brojeva tzv. *Eratostenovim sitom*.

Recimo, na primjer, da želimo napraviti tablicu prostih brojeva ≤ 200.

Napišemo sve prirodne brojeve od 2 do 200.

Prekrižimo sve prave višekratnike broja 2, pa broja 3, pa broja 5.

U svakom koraku, prvi neprekriženi broj je prost, te u idućem koraku križamo njegove prave višekratnike (prvi novoprekriženi broj će biti njegov kvadrat, jer su svi manji višekratnici već ranije prekriženi).

U našem slučaju, nakon križanja višekratnika od 7, 11 i 13, tablica je gotova (jer je $17 > \sqrt{200}$).

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi.

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi.

Promotrimo broj

$$n = 1 + p_1 p_2 \cdots p_k.$$

Uočimo da n nije djeljiv ni sa p_1, ni sa p_2, $\ldots$, ni sa p_k.

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi.

Promotrimo broj

$$n = 1 + p_1 p_2 \cdots p_k.$$

Uočimo da n nije djeljiv ni sa p_1, ni sa p_2, $\ldots$, ni sa p_k.

Dakle, svaki prosti faktor p od n je različit od $p_1, \ldots, p_k$.

Teorem (Euklid)

Skup svih prostih brojeva je beskonačan.

Dokaz:

Pretpostavimo da su $p_1, p_2, \ldots, p_k$ svi prosti brojevi.

Promotrimo broj

$$n = 1 + p_1 p_2 \cdots p_k.$$

Uočimo da n nije djeljiv ni sa p_1, ni sa p_2, $\ldots$, ni sa p_k.

Dakle, svaki prosti faktor p od n je različit od $p_1, \ldots, p_k$.

Budući da je n ili prost ili ima prosti faktor, dobili smo prost broj različit od $p_1, \ldots, p_k$, što je kontradikcija. $\square$