3. Relacije

**1.** Pojam relacije. Osnovni pojmovi. Binarna relacija i binarna relacija na skupu.

Relacija je bilo koji podskup Kartezijevog produkta skupova tj.

gdje su skupovi.

Binarna relacija "iz " je bilo koji podskup Kartezijeva produkta .

Domena relacije se definira kao .

Slika (područje vrijednosti) relacije se definira kao .

Binarna relacija na skupu je bilo koji neprazan podskup .

**Napomena:** Ovdje je problematična podcrtana riječ neprazna. Na većini internet stranica se riječ neprazan ne spominje, ali u knjizi jest. Navodno prof. Matić želi da mu se neprazna piše samo u definiciji relacije na skupu, a u ostalima ne i tako je gore učinjeno.

**2.** Predočavanje binarnih relacija. Koliko imamo različitih binarnih relacija na skupu X od n elemenata?

Relacije možemo predočavati nabrajanjem elemenata relacije ako je relacija konačna, kao podskup Kartezijeva produkta (Vennov dijagram), definicijskim dijagramom, Cayleyevom tablicom, matrično i usmjerenim grafom. Primjer Cayleyeve tablice:

|  |  |  |  |
| --- | --- | --- | --- |
|  | a | b | c  Primjer matrice: |
| a | T | **⊥** | **⊥** |
| b | **⊥** | T | T |
| c | **⊥** | **⊥** | **⊥** |

Relaciju predočavamo usmjerenim grafom na sljedeći način: svaki element skupa reprezentira (označena) točka koju nazivamo čvor ili vrh. Ako je tada dva čvora označena sa povežemo strelicom od . Tu strelicu nazivamo usmjereni brid. Ako je i onda imamo dva usmjerena brida između , pa, zbog jednostavnosti, povezujemo jednom dvostranom strelicom. Ako je , usmjereni brid između se zove petlja.

Na skupu od **n** elemenata imamo različitih binarnih relacija.

**Napomena:** Ovdje je, kao i u prvom pitanju, problem nepraznog skupa. Gore je uzeta opcija da je dopušten prazni skup, ali ako se traži da se prazan skup ne smije uzeti tada je rješenje .

**3.** Osnovna svojstva binarnih relacija na skupu: refleksivnost, simetričnost, antisimetričnost, tranzitivnost, potpunost. Dati primjere binarnih relacija koje imaju (nemaju) pojedino svojstvo.

Za binarnu relaciju na kažemo da je:

refleksivna ako vrijedi

simetrična ako vrijedi

antisimetrična ako vrijedi

tranzitivna ako vrijedi

potpuna ako je refleksivna, simetrična, antisimetrična i tranzitivna.

Primjeri: Promatrajmo binarne relacije na skupu . Dajmo primjere **nekih** relacija na ovom skupu.

Binarna relacija je refleksivna dok binarna relacija nije refleksivna.

Binarna relacija je simetrična dok binarna relacija nije simetrična.

Binarna relacija je antisimetrična, a binarna relacija nije antisimetrična.

Binarna relacija je tranzitivna, a binarna relacija nije tranzitivna.

**4.** Operacije s binarnim relacijama: kompozicija relacija, inverzna relacija. Karakterizacija pojmova refleksivnost, simetričnost, antisimetričnost, tranzitivnost, potpunost pomoću operacija s relacijama (citirati i dokazati).

Za dvije zadane relacije i na skupu definiramo novu relaciju - kompoziciju relacija kao skup svih za koje postoji tako da je i . U sažetijem zapisu:

.

Za relaciju na definiramo inverznu relaciju tako da pišemo onda i samo onda ako je . Pišemo:

Propozicija: neka je relacija na skupu , tj. .

Relacija je refleksivna onda i samo onda ako je .

Relacija je simetrična onda i samo onda ako je .

Relacija je antisimetrična onda i samo onda ako je .

Relacija je tranzitivna onda i samo onda ako je .

Relacija je potpuna onda i samo onda ako je , i .

Dokaz:

Ako je refleksivna tada je očito za svaki iz iz čega slijedi . Obratno, ako je onda je za svaki iz pa je refleksivna relacija.

Neka je simetrična relacija. Ako je onda je zbog simetričnosti . Iz definicije inverzne relacije slijedi da je . Dakle, ako je onda je . Time je dokazano da je . Obratna inkluzija se dokazuje na analogan način pa je konačno . Obratno, pretpostavimo da je . Dakle ako je . Po definiciji inverzne relacije je . Iz jednakosti konačno slijedi pa je simetrična relacija.

Neka je relacija tranzitivna. Da bi dokazali inkluziju, uzimamo . Po definiciji kompozicije relacije postoji tako da je i , pa iz tranzitivnosti slijedi , tj. . Time je dokazano da vrijedi . Obratno, neka vrijedi . Da bi dokazali tranzitivnost relacije, neka je i . Onda po definiciji kompozicije vrijedi . Kako je , onda vrijedi i , tj. .

**5.** Pojam relacija ekvivalencije i razreda (klase) ekvivalencije. Svojstva razreda ekvivalencije (citirati teorem i dokazati).

Binarna relacija zove se relacija ekvivalencije ako je refleksivna, simetrična i tranzitivna, tj. ako za sve vrijedi:

Neka je relacija ekvivalencije na skupu . Razred (klasa) ekvivalencije elementa je skup svih elemenata iz koji su u relaciji s . Dakle, je podskup od definiran sa

Teorem: Neka je relacija ekvivalencije na . Onda za sve vrijedi ili ili . Pritom je

onda i samo onda ako je

Dokaz: Pretpostavimo da je . Trebamo dokazati da je Ako postoji , , onda je . Zbog tranzitivnosti dobivamo da je , tj. . Prema tome je opet zbog tranzitivnosti . Na isti način se pokazuje i , tj. . Dakle .

**6.** Particija skupa i pridružena relacija ekvivalencije na tom skupu (citirati teorem i dokazati)

Kažemo da familija podskupova od čini particiju (disjunktni rastav) skupa ako vrijedi:

za sve , tj. familija podskupova je disjunktna.

Teorem: Neka je particija skupa . Definirajmo relaciju na skupu tako da je onda i samo onda ako pripadaju istom skupu iz particije tj. postoji tako da je . Onda je relacija ekvivalencije. Pripadni razredi ekvivalencije podudaraju se sa skupovima .

Dokaz: Tvrdnja je očevidna.

**7.** Što je kvocjentni skup nekog skupa po zadanoj relaciji ekvivalencije na tom skupu? Ilustriraj primjerom kvocjentnog skupa od po relaciji kongruencije po modulu n. Dokazati da je relacija kongruencije po modulu n relacija ekvivalencije na .

Ako je relacija ekvivalencije na skupu , onda skup svih pripadnih razreda ekvivalencije zovemo kvocijentni skup od s obzirom na relaciju i označavamo:

Propozicija: Kvocijentni skup od po relaciji jednak je sljedećem n-članom skupu: Taj skup se naziva kvocijentni skup ostataka po modulu, ili skup ostataka pri dijeljenju sa . Razredi ekvivalencije izgledaju ovako:

Razred gdje je , sadrži skup svih onih cijelih brojeva koji dijeljenjem sa daju ostatak .

Dokaz: Da bi dokazali da je kongruencija po modulu relacija ekvivalencije na moramo dokazati da je refleksivna, simetrična i tranzitivna.

Refleksivnost: Broj dijeli . Simetričnost: Ako dijeli , onda n dijeli i . Tranzitivnost: Ako dijeli , onda dijeli i .

**Napomena:** Prethodna propozicija je u potpunosti ista kao i propozicija iz pitanja broj 12 iz cjeline “Cijeli brojevi” tj. radi se o dvije potpuno iste propozicije koje su preformulirane (zakamuflirane) tako da izgledaju različito.

**8.** Dokažite da je relacija ekvipotentnosti skupova () relacija ekvivalencije. Što su u tom slučaju klase ekvivalencje, a što kvocijentni skup?

Teorem: Ekvipotentnost skupova ima ova temeljna svojstva:

refleksivnost: za svaki skup ,

simetričnost: ako je , onda je

tranzitivnost: ako je i , onda je .

Dokaz:

Identiteta , , je bijekcija.

Ako je bijekcija, onda je i inverzna funkcija također bijekcija.

Ako su funkcije bijekcije, onda je i njihova kompozicija također bijekcija.

U tom slučaju su klase ekvivalencije skupovi onih skupova koji imaju isti kardinalni broj. Naime, u **istu** klasu ekvivalencije spadaju **svi** skupovi koji imaju isti kardinalni broj, npr. jedna klasa ekvivalencije je tj. skup svih skupova koji imaju jedan element (u tu klasu spadaju još i skupovi ). Još jedan primjer klase ekvivalencije je tj. skup svih skupova koji su ekvipotentni sa skupom prirodnih brojeva (u tu klasu spadaju još skupovi ). Kvocjentni skup je skup svih klasa ekvivalencije tj. .

**Napomena:** Slično kao i u prethodnom pitanju, ovaj teorem se već spominje ranije (pitanje broj 7, cjelina „Skupovi“).

**9.** Što je to relacija parcijalnog poretka, a što relacija potpunog poretka. Primjerima pokaži da parcijalno poredani skup ne mora biti i potpuno poredan.

Binarna relacija zove se relacija parcijalnog poretka ako je refleksivna, antisimetrična i tranzitivna tj.

,

,

.

Za parcijalno poredan skup kažemo da je potpuno (totalno) poredanako za za svaki vrijedi ili ,tj. svaka dva elementa su usporediva.

Primjer: Skup je parcijalno poredan skup. Ako partitivni skup ima barem dva elementa, onda skup nije potpuno poredan skup, jer disjunktni podskupovi i iz nisu usporedivi, tj. nisu u relaciji .

Prmjer: Skup je parcijalno poredan skup, ali nije potpuno poredan skup jer npr. ne dijeli niti dijeli .

**10.** Što je to dobro uređen skup? Primjer potpuno uređenog skupa koji nije dobro uređen skup.

Ako je totalno poredani skup takav da svaki njegov neprazni podskup ima minimalni element, onda kažemo da je dobro poredan skup.

Primjer: Skup je totalno poredan skup, ali nije dobro poredan skup jer njegov beskonačni podskup (skup svih negativnih cijelih brojeva) nema minimalni element. Isto vrijedi za skupove i .

**11.** Definiraj pojmove donje (gornje) međe, odozdol (odozgor) omeđenog podskupa, infimuma (supremuma), minimuma (maksimuma) i ilustriraj primjerima.

Neka je parcijalno poredan skup i . Kažemo da je donja (gornja) međa skupa , ako je za sve . Za skup kažemo da je omeđen odzdol (odozgor) ako ima barem jednu donju (gornju) među u .

Element (ako postoji) zovemo infimumom (supremumom) skupa , i označavamo sa (), ako vrijedi:

je donja (gornja) međa od ,

za svaku donju (gornju) među vrijedi .

Ako vrijedi da je onda nazivamo minimumom (maksimumom) skupa i označavamo

Primjer (Infimum, supremum, minimum, maksimum):

Neka je zadan skup i ne postoje.

.

Za skup i relaciju | (relacija “biti dijelitelj od”) ne postoje , ali je zatos obzirom na relaciju |.

**12.** Kartezijev produkt parcijalno poredanih skupova. Primjerom pokaži da Kartezijev produkt totalno poredanih skupova ne mora biti totalno poredan. Što je to leksikografski poredak?

Neka su zadana dva parcijalno poredana skupa Kartezijev produkt parcijalno poredanih skupova definiramo kao . Pritom za elemente kažemo da je ako je nejednakost ispunjena po komponentama, dotično u skupu i u skupu .

Primjer (Kartezijev produkt totalno poredanih skupova ne mora biti totalno poredan): Npr. neka je , i . Elementi nisu usporedivi u .

Neka su zadani parcijalno poredani skupovi svaki sa svojom relacijom poretka. Onda na Kartezijevom produktu definiramo drugu relaciju poretka, tzv. relaciju leksikografskog poretka. Za kažemo da je ako je ispunjen jedan od sljedeća dva uvjeta:

( i bilo kakvi),

i .

**13.** Jednostavnim primjerima objasni što je to Hasseov dijagram relacije poretka na nekom skupu.

Neka je konačan skup i relacija parcijalnog poretka na . Tada relaciju možemo predočiti pomoću Hasseovog dijagama.

* Svaki element skupa reprezentira točka u ravnini koju nazivamo čvor ili vrh.
* Ne crtaju se petlje, jer je relacija refleksivna.
* Ako je i između njih ne postoji niti jedan , tj. iz slijedi , onda čvor koji pripada stavljamo iznad čvora koji pripada i spajamo ih crtom.
* Usmjereni brid koji je impliciran tranzitivnošću ne crtamo.

Primjer: U ovom primjeru je , a relacija poretka je "biti djelitelj od", tj. znači .

**Napomena:** Potrebno je Hasseove dijagrame (vidi Žubrinić, str. 74.).

**14.** Kako definiramo izomorfizam parcijalno poredanih skupova? Dajte primjer.

Za parcijalno poredan skup kažemo da je izomorfan parcijalno poredanom skupu ako postoji bijekcija koja čuva poredak, dotično vrijedi:

Primjer: su izomorfni. Vrijedi: , , Dakle postoji funkcija koja čuva poredak.

**15.** Što je to mreža, a što potpuna mreža? Kako definiramo operacije zbrajanja i množenja u mreži? Pojam nule i jedinice. Sve ilustrirajte jednostavnim primjerima.

Parcijalno poredan skup zove se mreža ako za svaki par elemenata postoji i Na taj način možemo uvesti dvije binarne operacije u parcijalno poredan skup : i .

Parcijalno poredan skup je potpuna mreža ako svaki njegov podskup (konačan ili beskonačan) posjeduje infimum i supremum. Svaka potpuna mreža onda ima element koji se zove **nula** i koji se zove **jedinica**.

Primjer: Partitivni skup je potpuna mreža, a pripadna operacija zbrajanja je unija, a operacija produkta presjek. Nula mreže je prazan skup, a jedinica mreže je .

Primjer. Skup cijelih brojeva je mreža, ali nije potpuna mreža. Operacije zbrajanja i množenja dvaju elemenata su minimum i maksimum. Nema nule ni jedinice.

**16.** Teorem o operacijama i na potpunoj mreži.

Teorem: Za operacije i na mreži vrijede svojstva:

Apsortivnost ili svojstvo upijanja:

**17.** Što je to distributivna a što komplementirana mreža? Primjeri.

Za potpunu mrežu kažemo da je distributivna mreža ako u njoj vrijede zakoni distribucije:

Za element u potpunoj mreži kažemo da je komplement elementa ako je i . Ako svaki element ima komplement, onda mrežu zovemo komplementiranom mrežom.

Primjer: Mreža svih djelitelja broja , s relacijom djeljivosti kao relacijom poretka, je potpuna mreža u kojoj je nula , a jedinica . To je distributivna mreža. Mreža nije komplementirana jer npr. nema komplement.

Primjer: Mreža svih djelitelja broja , s relacijom djeljivosti kao relacijom poretka, je potpuna mreža u kojoj je nula , a jedinica . To je distributivna mreža. Mreža Mreža nije komplementirana.

Primjer: Distributivna i komplementirana potpuna mreža je očevidno Booleova algebra.

4. Cijeli brojevi

**1.** Definirajte relaciju ' biti djelitelj ' i ispitajte strukture .

Neka su cijeli brojevi. Kažemo da **a** dijeli ako je i je višekratnik od (tj. postoji tako da je ). U tom slučaju pišemo i čitamo “a dijeli b”. Broj zovemo dijeliteljem broja .

Propozicija: Struktura (, |) je parcijalno poredani skup. Relacija "dijeliti" na skupu ima sljedeća tri osnovna svojstva:

refleksivnost: za svaki prirodni broj vrijedi

antisimetričnost: za svaka dva prirodna broja iz slijedi

tranzitivnost: ako i , onda .

Dokaz:

trivijalno .

Budući da je i za neke , slijedi . Zbog je , dakle nakon skraćivanja. Brojevi su prirodni, odakle slijedi da je .

Zbog je , dotično .

Struktura nije parcijalno poredan skup jer ne vrijedi svojstvo antisimetričnosti. Na primjer iz i bi po antisimetričnosti slijedilo da je što je netočno.

**2.** Citiraj i dokaži teorem o svojstvima relacije "biti djelitelj"( | ).

Propozicija: Relacija "dijeliti" ima sljedeća tri osnovna svojstva:

refleksivnost: za svaki cijeli broj vrijedi ,

za svaka dva cijela broja iz slijedi . Ako su a i b prirodni brojevi , onda slijedi (antisimetričnost) ,

tranzitivnost:

Dokaz:

trivijalno.

Budući da je i za neke , slijedi . Zbog je , dakle nakon skraćivanja. Brojevi su cijeli, odakle slijedi da je .

Zbog

**Napomena:** U propoziciji pod (2) upravo vidimo ono što smo ustanovili u prethodnom pitanju tj. da struktura nije parcijalno poredan skup te napomenu da je struktura parcijalno poredani skup.

**3.** Najveća zajednička mjera i najmanji zajednički višekratnik dvaju (ili više) cijelih brojeva, Osnovna svojstva (citirati i dokazati pojedine propozicije).

Ako su takvi da , onda zovemo zajedničkim djeljiteljem od i. Ako je barem jedan od brojeva ili različit od , onda postoji i najveći zajdnički djeljitelj , kojeg zovemo najvećom zajedničkom mjerom od i i označavamo ga da Najveća zajednička mjera može se na sličan način definirati i za bilo koji konačan skup cijelih brojeva .

Najmanji zajednički višekratnik cijelih brojeva, definiramo kao najmanji prirodni broj čiji su djelitelji . Označavamo ga sa Najmanji zajednički višekratnik može se na sličan način definirati i za bilo koji konačan skup cijelih brojeva .

Neka svojstva:

Ako su

**.**

.

.

.

Ako je i onda .

Dokazi:

Vrijedi . Zbrojimo dvije jednakosti. Imamo odakle odmah slijedi tvrdnja.

Provjerimo tvrdnju za a: Također, očito je da niti jedan broj veći od nije djelitelj od tj. .

i su očite tvrdnje. Dokazi se izvode pomoću matematičke logike. Evo par dokaza

Tvrdnja se lako dokazuje. Imamo dva slučaja:

. Tada je .

. Dokazivat ćemo svaku od nejednakosti posebno.

Dokažimo kontradikcijom . Neka je . To znači da je ili . No tada ne vrijedi d|a, odnosno d|b (vidi dokaz svojstva ). Dolazimo do kontradikcije.

Jasno je da vrijedi sljedeća tvrdnja zbog početne pretpostavke ().

Nejednakost se također lako dokazuje kontradikcijom. Naime ako je to bi značilo da je ili no tada ne može biti višekratnik od , odnosno . Kontradikcija.

Kada spojimo i dobivamo početnu tvrdnju.

Budući da dijeli istodobno i , onda je najveći mogući djelitelj ta dva broja, tj. .

Propozicija: Pretpostavimo da su svi brojevi u jednakosti cijeli. Ako se zna da su svi brojevi, osim jednoga, djeljivi sa d, onda je i preostali broj djeljiv sa .

Dokaz: Ako se npr. zna da su svi brojevi osim djeljivi sa , onda je i broj djeljiv sa

**4.** Teorem o dijeljenju (citirati i dokazati)

Teorem: (O dijeljenju) Neka su zadani i . Onda postoje jedincati i takvi da je . Broj zove se kvocijent pri dijeljenju sa a ostatak.

Dokaz: Označimo sa , , skup svih cijelih brojeva koji leže u poluotvorenom intervalu Kako je unija svih jednaka i svi su međusobno disjunktni, postoji broj takav da je . Iz definicije intervala slijedi da je , tj. . Dakle traženi prikaz postoji.

Da bi dokazali da je taj prikaz jedincat, neka pored ovog rastava postoji još jedan: , gdje je i . Onda je tj. . Kako je i b dijeli jedino nulu u tom skupu, mora biti , tj. . Odavde slijedi zatim i .

**5.** Euklidov algoritam. Citirajte i dokažite teorem.

Propozicija: Neka su i . Onda je svaki zajednički djelitelj od ujedno i zajednički djelitelj od Posebno, vrijedi

Dokaz: Ako dijeli u relaciji , onda dijeli i (vidi Propoziciju iz pitanja 3.). Obratno, ako dijeli i , onda na isti način .

Teorem: (Euklidov algoritam za nalaženje najveće zajedničke mjere dvaju brojeva) Neka je i . Promatrajmo slijed ostataka koji se dobivaju kako je opisanu u teoremu o dijeljenju:

Pretpostavimo da je (tj. ne dijeli ). Onda postoji indeks takav da je i vrijedi .

Dokaz: Iz gornjih nejednakosti vidimo da je slijed opadajuć: . Kako je slijed omeđen odozdol s nulom, te kako se radi o cijelim brojevima, onda mora postojati indeks za koji će odgovarajući **r** biti jednak nula, recimo , a prethodni , gdje je , Prema prethodnoj propaziciji imamo , gdje smo u zadnjoj jednakosti koristili činjenicu da .

**6.** Objasni jednakost . Citiraj i dokaži pripadajući teorem.

Za svaki postoje takvi da je

Teorem: Neka su cijeli brojevi koji nisu oba jednaki . Onda je minimalni pozitivni broj u skupu jednak Drugim riječima .

Dokaz: Neprazan podskup skupa cijelih brojeva koji je zatvoren s obzirom na operaciju oduzimanja (tj. iz slijedi ) jednak je ili ili skupu svih cjelobrojnih višekratnika nekog prirodnog broja : (ovaj skup kraće označavamo sa m). Uočimo da je skup zatvoren s obzirom na operaciju oduzimanja, dotično ako su , , onda je i . Zbog S prema prethodnoj tvrdnji za minimalna pozitivan broj u skupu vrijedi . Kako su onda dijeli i , pa dijeli i S druge strane, po definiciji skupa S postoje takvi da je . Budući da odavde slijedi i da . Iz svojstva antisimetričnosti relacije djeljivosti | na skupu prirodnih brojeva dobivamo

**7.** Što su to prosti, a što složeni brojevi? Eratostenovo sito.

Za prirodni broj kažemo da je prost broj (prim-broj) ako su mu jedini djelitelji i , tj. ako ima samo trivijalne djelitelje. Za prirodni broj koji nije prost (tj. posjeduje netrivijalne djeljitelje) kažemo da je složen broj**.**

Eratostenovo sito: Ako želimo naći sve proste brojeve , koristimo sljedeći jednostavni postupak:

* Ispisujemo, po redu, sve prirodne brojeve od do ,
* Križamo ,
* Zaokružimo (prost) i križamo sve višekratnike od,
* Prvi preostali (prost) zaokružimo i križamo sve višekratnike od (koji nisu već prekriženi),
* Prvi preostali (prost) zaokružimo i križamo sve višekratnike od (koji nisu već prekriženi),itd.

Zaokruženi brojevi koji preostaju su upravo prosti brojevi .

**8.** Dokaži da prostih brojeva ima beskonačno mnogo.

Teorem: Skup svih prostih brojeva je beskonačan.

Dokaz: Dokaz ćemo provesti kontradikcijom (od suprotnog). Pretpostavimo dakle suprotno, tj. da je skup svih prostih brojeva konačan: Pogledajmo broj On nije djeljiv niti sa kojim od p-ova jer je ostatak djeljenja sa jednak uvijek . Prema osnovnom teoremu aritmetike, a ima rastav na proste faktore . Niti koji od prostih brojeva nije u , a to je proturječje s definicijom skupa .

**9.** Osnovni teorem aritmetike (citiraj i dokaži).

Teorem: (Rastav na proste djelitelje, Osnovni teorem aritmetike). Za svaki prirodni broj postoji jedincat rastav na proste djeljitelje gdje su svi različiti prosti brojevi koji dijele , poredani po veličini. Pritom zovemo kratnošću odgovarajućeg prostog broja u rastavu.

Dokaz:Neka je najmanji prosti faktor od , tj. . Ako je , onda je .

Ako nastavimo isti niz, na kraju će biti . Neki od prostih brojeva qi mogu biti jednaki. Nakon grupiranja po veličini, dobivamo rastav kao u teoremu.

Slijedi dokaz da je rastav broja na proste faktore jedinstven (do na njihov poredak). Pretpostavimo da imamo još jedan rastav na prostih faktora: poredanih po veličini. Onda je: . Kako dijeli lijevu stranu, onda on dijeli i desnu stranu, pa prema prethodnom korolaru on dijeli i neki od r-ova, npr. : | . Međutim, je prost broj i , pa slijedi da je . Podijelimo jednakost sa lijevo i desno, pa imamo da je . Na isti način dokažemo da je , pa je konačno i

**10.** Dokaži formulu

Lema (bez dokaza): Neka su rastavi na proste faktore brojeva , gdje su svi prosti faktori od zajedno (tako da neki mogu biti jednaki nuli). Definirajmo

, . Onda vrijedi , .

Propozicija: Između najveće zajedničke mjere i najmanjeg zajedničkog višekratnika dvaju prirodnih brojeva postoji sljedeća jednostavna veza:

Dokaz: Očigledno je , pa iz , (prethodna lema) dobivamo

**11.** Broj pozitivnih djelitelja prirodnog broja n. Dokaži formulu za .

Korolar: Djeljitelja prirodnog broja rastavljenog na proste faktore , ima ukupno

.

Dokaz: Svaki djeljitelj ima oblik , pri čemu je . Dakle broj djeljitelja od jednak je broju poredanih n-teraca , gdje svaki može poprimiti bilo koju od vrijednosti. Njihov ukupan broj je .

**12.** Kako se definira kongruencija po modulu n. Dokaži da je kongruencija po modulu n relacija ekvivalencije na skupu .

Kažemo da su cijeli brojevi kongruentni po modulu (ili modulo ), , ako je razlika djeljiva sa ,tj. . U tom slučaju pišemo i čitamo '' je kongruentan po modulu (modulo) ''. To je isto što i reći .

Propozicija: Kongruencija po modulu ima slijedeća svojstva:

Dokaz:

.

.

**13.** U kakvom su odnosu operacije zbrajanja i množenja (potenciranja) i relacija kongruencije po modulu n.Citirati i dokazati pojedine tvrdnje.

Propozicija: Ako je gdje je , onda vrijedi:

.

Dokaz:

Kako je i , za neke , onda vrijedi , tj..

Na sličan način je , tj..

Korolar: Ako je i bilo koji cijeli brojevi, onda vrijedi:

za svaki prirodni broj

bilo koji polinom s cjelobrojnim koeficijentima .

Dokaz: Prva dva svojstva slijede iz prethodne propozicije, jer vrijedi:

naime .

pa je .

Svojstvo slijedi iz prethodne propozicije (stavak množenjem kongruencije same sa sobom puta.

Svojstvo slijedi odmah iz svojstava iz korolara te svojstva iz prethodne propozicije.

**14.** Definicija Eulerove funkcije. Citirajte teorem o vrijednosti i dokažite neke posljedice toga teorema.

Funkcija koja prirodnom broju **n** pridružuje broj prirodnih brojeva koji su i relativno prosti sa **n** zove se Eulerova funkcija. Definiramo .

Teorem: Ako ima rastav na proste faktore , onda je .

Posljedice:

Za , , je .

Ako su relativno prosti brojevi, onda Eulerova funkcija ima multiplikativno svojstvo: .

Dokaz:

Broj svih brojeva koji su i nisu relativno prosti sa jednak je . To su naime svi brojevi čijizajednički faktor saje barem , tj. oblika , gdje je . Ovdje r poprima bilo koju vrijednost , a takvih ima . Prema tome je jednak ukupnom broju brojeva manjih od umanjenom za broj onih koji nisu relativno prosti sa : .

Ako imaju rastave na proste faktore i , onda kako je , slijedi , rastav na proste faktore od . Prema teoremu o vrijednost funkcije

.

**15.** Eulerova kongruencija. Citirajte teorem.

Teorem: Ako su relativno prosti prirodni brojevi, onda je .

**16.** Mali Fermatov teorem. Citirajte ga i dokažite.

Teorem: (Mali Fermatov stavak) Ako je prost broj, onda za svaki vrijedi , tj. . Posebno, ako nije višekratnik od , onda je .

Dokaz: Ako je višekratnik od , onda je tvrdnja trivijalna. Pretpostavimo zato da nije višekratnik od . Onda su i relativno prosti. Kako je , iz Eulerove kongruencije dobivamo . Tvrdnja slijedi množenjem kongruencije s .