Osnovni pojmi

V(G) množica vozlišč grafa G, E(G) množica povezav grafa G
$N_g(u)$ soseščina vozlišča u, $deg_G(u)$ stopnja vozišča
$\delta(G)$ minimalna stopnja grafa, $\Delta(G)$ maksimalna stopnja grafa
$\Omega(G)$ število komponent grafa,
$d_G(u,v)$ dolžina najkrajšega sprehoda med u,v
$diam(G)$ premer grafa, $rad(G)$ polmer grafa
$g(G)$ ožina grafa, $\tau(G)$ število vpetih dreves
$F(G)$ množica lic vložitve, $l(F)$ dolžina lica
$G \cong H$ izomorfna grafa

Barvanje grafov

K-barvanje je preslikava $C : V(G) \to [k]$, če velja: $uv \in E(G) \implies C(u) \neq C(v)$.
Kromatično število $\chi(G)$ je $\min\{k;\ \exists k - barvanje\ G\}$.
Klično število $\omega(G)$ je velikost največjega polnega podgrafa v G.
Spoj grafov $G \oplus H$ dobimo tako, da dodamo $\forall$ možne povezave med G in H.
K-barvanje povezav je $C : E(G) \to [k]$ če velja: $uv, uw \in E(G) \implies C(uv) \neq C(uw)$.
Kromatični indeks $\chi'(G)$ je $\min\{k;\ \exists k - barvanje\ povezav\ G\}$.
G je **razreda I** če $\chi'(G) = \Delta(G)$ in **razreda II** če $\chi'(G) = \Delta(G) + 1$.
Požrešni algoritem: (1) izberemo poljubni vrstni red vozlišč (2) vozlišča barvamo v tem vrstnem redu in ko je vozlišče na vrsti, ga pobarvamo z najmanjšo možno barvo (najmanjša barva, ki še ni bila uporabljena na njegovih že pobarvanih sosedih). Vedno $\exists$ vrstni red, da dobimo optimalno barvanje.

(1) H podgraf grafa G $\implies \chi(G) \geq \chi(H)$.
(2) $\chi(G) \geq \omega(G)$.
(3) $\chi(G) \leq \Delta(G) + 1$.
(4) G ni regularen $\implies \chi(G) \leq \Delta(G)$.
(Brooks) G povezan in ni niti poln, niti lih cikel $\implies \chi(G) \leq \Delta(G)$.
(5) Naj bo $d_1 \geq d_2 \geq \cdots \geq d_n$ zaporedje stopenj grafa,
tedaj velja: $\chi(G) \leq 1 + \underset{1 \leq i \leq n}{max}(min(d_i, i-1))$.
(6) $\chi(G \oplus H) = \chi(G) \oplus \chi(H)$.
(4CT) G ravninski $\implies \chi(G) \leq 4$. **(Vizing)** $\Delta(G) \leq \chi'(G) \leq \Delta(G) + 1$.
(6) $\forall n \geq 2$ je K_n razreda I $\Leftrightarrow$ n sod.
(7) $\forall$ dvodelen graf je razreda I.
(8) vsak Hamiltonov 3-regularen graf je razreda 1.
(9) regularen graf z liho mnogo točkami je razreda 2.
(10) $C_m \square C_n$ je razreda 2, če m in n nista liha. Če sta m,n sodi $\Xi = 2$, drugače $\Xi = 2$.
(11) G graf z n vozlišči: $s\sqrt{n} \leq \Xi(G) + \Xi(\overline{G}) \leq n + 1$.

Neodvisne in dominatne množice

Neodvisna množica $I \subseteq V(G)$ je taka, da $\forall i,j \in I$ i in j nista sosedni.
Neodvisnostno število $\alpha(G)$ je moč največje neodvisnostne množice v G. Neodvisna množica I je **maksimalna**, če ni vsebovana kot prava podmnožica v neki neodvisni množici.
Dominantna množica $X \subseteq V(G)$ je taka, da za $\forall v \in V(G)$ velja, $v \in X$ ali v ima soseda v X.
Dominacijsko število je moč najmanjše dominantne množice, oz. $\gamma(G)$. Dominantna množica D je **povezana**, če inducira povezan podgraf, $\gamma_c(G)$; **neodvisna**, če inducira podgraf brez povezav, $\gamma_i(G)$; **celotna**, če ima $\forall v \in V(G)$ soseda v D, $\gamma_t(G)$.
Soseščino vozlišča u definiramo kot odprto $N_g(u) = \{v : uv \in E(G)\}$ oz. zaprto $N_G[u] = N_G(u) \cup \{u\}$.
Zaprto soseščino množice D definiramo kot $N_G[D] = \underset{u \in D}{\cup} N_G[u]$.
2-pakiranje grafa je taka množica X da velja: $x,y \in X$; $x \neq y \implies d_G(x,y) \geq 3$. Moč največjega 2-pakiranja G je **2-pakirno število**, $\rho(G)$. Če za 2-pakiranje X grafa G velja: $\underset{u \in X}{\cup} N_G[u] = V(G)$, pravimo da je X **popolna koda** G.
(1) $\alpha(G)\dot{\chi}(G) \geq |V(G)|$.
(2) $\alpha(G) \leq |V(G)| - \frac{|E(G)|}{\Delta(G)}$.
(3) $\lceil \frac{|V(G)|}{\Delta(G)+1} \rceil \leq \gamma(G) \leq \lfloor \frac{|V(G)|}{2} \rfloor$.
(4) G povezan $\implies \gamma(G) \geq \rho(G)$.
(5) G premore popolno kodo $\implies \gamma(G) = \rho(G)$.
(6) H vpet podgraf v $G \implies \gamma(G) \leq \gamma(H)$.
(7) G povezan $\implies$ premore vpeto drevo T, da velja $\gamma(G) = \gamma(T)$.
(8) G ima vsaj 1 povezavo $\implies \gamma(G) \leq \chi(\overline{G})$.
(9) Za $\forall$ graf brez izoliranih vozlišč velja $\gamma(G) \leq \gamma_t(G) \leq 2\dot{\gamma}(G)$.

Algebrske strukture

		asoc	enota	inverz	komut	distrib
magma	$(M,\circ)$				?	
polgrupa	$(M,\circ)$	$\circ$			?	
monoid	$(M,\circ)$	$\circ$	$\circ$		?	
grupa	$(M,\circ)$	$\circ$	$\circ$	$\circ$	?	
abelova grupa	$(M,\circ)$	$\circ$	$\circ$	$\circ$	$\circ$	
bigrupoid	$(M, \oplus, \odot)$					?
polkolobar	$(M, \oplus, \odot)$	$\oplus$			$\oplus$,($\odot$?)	$\odot$
kolobar	$(M, \oplus, \odot)$	$\oplus$,$\odot$	$\oplus$	$\oplus$	$\oplus$,($\odot$?)	$\odot$
kolobar z enoto	$(M, \oplus, \odot)$	$\oplus$,$\odot$	$\oplus$,$\odot$	$\oplus$	$\oplus$,($\odot$?)	$\odot$
obseg	$(M, \oplus, \odot)$	$\oplus$,$\odot$	$\oplus$,$\odot$	$\oplus, \odot \setminus \{0\}$	$\oplus$	$\odot$
polje	$(M, \oplus, \odot)$	$\oplus$,$\odot$	$\oplus$,$\odot$	$\oplus, \odot \setminus \{0\}$	$\oplus$,$\odot$	$\odot$

vse strukture morajo biti zaprte za operacijo
? pomeni, da lastnost ni obvezna
primer: polgrupa z komut. operacijo je komutativna polgrupa

Lastnosti

asociativnost	$(a \circ b) \circ c = a \circ (b \circ c)$
enota	$a \circ e = e \circ a = a$
inverz	$a \circ a^{-1} = a^{-1} \circ a = e$
komutativnost	$a \circ b = b \circ a$
leva distributivnost	$(a \oplus b) \odot c = (a \odot c) \oplus (b \odot c)$
desna distributivnost	$c \odot (a \oplus b) = (c \odot a) \oplus (c \odot b)$
homomorfizem	$f(x \circ_1 y) = f(x) \circ_2 f(y)$
preslikava enote	$f(e_{\circ_1}) = e_{\circ_2}$
preslikava inverza	$f(a)^{-1} = f(a^{-1})$

Definicije

operacija na množici M je funkcija $f : M \times M \longrightarrow M$
grupoid je urejen par $(M,\circ)$, kjer je M množica in $\circ$ operacija na M
polgrupa je asociativen grupoid
monoid (magma) je polgrupa z enoto (enota je največ ena)
grupa je monoid z inverzom (inverz je za vsak element največ en)

surjektivnost (onto) $f : X \to Y$

$$\forall y \in Y, \exists x \in X : f(x) = y$$

injektivnost (one-to-one) $f : X \to Y$

$$\forall a,b \in X : f(a) = f(b) \implies a = b$$

$$\forall a,b \in X : a \neq b \implies f(a) \neq f(b)$$

če ima funkcija levi inverz je injetivna.
če ima funkcija desni inverz je surjektivna
funkcije so asociativne, njihova enota je $id_s(a) = a$

Lastnosti grup (G)

moč je število elementov; moč podgrupe deli moč grupe.
red elementa $a \in G$ je najmanjše $n \in \mathbb{N}$ da velja $a^n = e$, če tak n $\nexists$ je red elementa a neskončen. $\forall$ element $\forall$ vsake končne grupe ima končen red.
podgrupa je podmnožica končne grupe, če je zaprta za $\circ$.

$a,b,c \in G$	$ab = ac$	$\implies$	$b = c$
$a,b,c \in G$	$ba = ca$	$\implies$	$b = c$
$a,b \in G$	$ab = e$	$\implies$	$a = b^{-1}$ in $b = a^{-1}$
$a,b \in G$	$ab = e$	$\implies$	$(ab)^{-1} = b^{-1}a^{-1}$
$a,b \in G$	$ab = e$	$\implies$	$((a)^{-1})^{-1} = a$
$a,b,c \in G$	$aba^{-1} = c$	$\implies$	c je konjugiran b

ciklična grupa G je taka, da $\exists a \in G$, da je $<a> = \{a^n;\ n \in \mathbb{Z}\} \cong G$. Naj bo G poljubna grupa, in $a \in G$, potem je <a> ciklična podgrupa v G generirana z a.
center grupe $Z(G) = \{a;\ a \in G :\ ax = xa\ \forall x \in G\}$ je podgrupa v G.

levi/desni odsek podgrupe H (grupe G po a) je $aH = \{ah : h \in H\}$. Naj bo G grupa, $H \leq G$, $a,b \in G$, tedaj velja:
(1) $a \in aH$
(2) $aH = H \iff a \in H$
(3) bodisi $aH = bH$ bodisi $aH \cap bH = \emptyset$
(4) $aH = bH \iff a^{-1}b \in H$
(5) $|aH| = |bH|$
(6) $aH = Ha \iff H = aHa^{-1}$
(7) $aH \leq G \iff a \in H$

(Lagrange) Če je G končna grupa in $H \leq G$, potem $|H|$ deli $|G|$ in število različnih levih/desnih odsekov po H je $\frac{|G|}{|H|}$.
podgrupa edinka H je taka podgrupa v G, če velja:
$aH = Ha\ \forall a \in G\ oz.\ aHa^{-1} = H\ \forall a \in G$; pišemo $H \triangleleft G$
enostavna grupa G je taka, kjer G in id edini edinki G. $G/H = \{aH : a \in G\}$, kjer $H \triangleleft G$. G/H je grupa za $(aH) \cdot (bH) = (ab)H$; **faktorska grupa**.

Lastnosti kolobarjev (R)

direktna vsota $R \oplus S$ kjer R,S kolobarja, so $\forall$ urejeni pari (r,s) $r \in R$ $s \in S$, kjer $(r,s) + (r',s') = (r + r', s + s')$ in $(r,s)(r',s') = (rr', ss')$. $R \oplus S$ je kolobar.
center kolobarja $Z(R) = \{a \in R;\ ax = xa\ \forall x \in R\}$ je podkolobar.

delitelja niča sta taka $a,b \in R$ da velja $ab = 0$ in $a \neq 0$, $b \neq 0$.
pravilo krajšanja: $a,b,c \in R\ a \neq 0\ ab = ac \implies b = c$.
cel kolobar R je komutativen kolobar z enoto $1 \neq 0$, ki nima deliteljev niča.
(1) Naj bo $(R, +, \cdot)$ komutativen kolobar z enoto $1 \neq 0$: R cel $\iff$ velja pravilo krajšanja.
(2) Polje je cel kolobar.
(3) R končen cel kolobar $\implies R$ polje.
(4) Za $n \in \mathbb{N}$ $n \geq 2$ velja: $\mathbb{Z}_n$ cel kolobar $\iff$ $\mathbb{Z}_n$ je polje $\iff$ n je praštevilo.

karakteristika kolobarja je najmanjši $n \in \mathbb{N}$ da za $\forall a \in R$ $na = 0$. Če tak n ne $\exists$ ima R karakteristiko 0; $char(R)$.
(1) Naj bo R kolobar z enoto. Če je red elementa 1 v grupi $(R, +)$ enak n, potem je $char(R) = n$.
(2) Če R cel kolobar, potem bodisi $char(R) = 0$, bodisi $char(R) = p$, kjer p praštevilo.

ideal je tak podkolobar S kolobarja R, da velja: $r \in R\ s \in S \implies rs$,$sr \in S$. Naj bosta I, J ideala v R:
$I + J = \{i + j;\ i \in I\ j \in J\}$
$I \cdot J = \{i_1 j_1 + \cdots + i_n j_n;\ i_k \in I\ j_k \in J\ k \in [n]\}$

(1) $I + J$ in $I \cdot J$ sta ideala v R.
(2) I ideal $\implies$ R/I kolobar; **faktorski kolobar**.

Podstrukture

skrčitev operacije $\circ_N$ podeduje asociativnost in komutativnost
podgroupa: $\forall a,b \in H : a \circ b \in H$, $e_\circ \in H$, $\forall a \in H : a^{-1} \in H$
podkolobar: $\forall x,y \in N$ velja $x - y \in N$ in $xy \in N$

(N,∘) **podgrupoid** v (M,∘):
$\iff$ (M, ∘) grupoid, $N \subseteq M$, N zaprta za ∘
(N,∘) **(komutativna) podpolgrupa** v (M,∘):
$\iff$ (M, ∘) (komutativna) polgrupa, (N, ∘) podgrupoid
(N,∘) **podmonoid** v (M,∘):
$\iff$ (M, ∘) monoid, (N, ∘) podpolgrupa, $e \in N$
(N,∘) **podgrupa** v (M,∘):
$\iff$ (M, ∘) grupa, (N, ∘) podmonoid, $\forall a \in N\ \exists a^{-1} \in N$
$\iff$ (M, ∘) grupa, $\forall a,b \in N$ velja $a \circ b^{-1} \in N$
(N,⊕,⊙) **podkolobar** v (M,⊕,⊙): $N \subseteq M$
$\iff$ N podgrupa $(M,\oplus)$
$\iff$ N podgrupoid $(M,\odot)$
(K,⊕,⊙) **podobseg** v (L,⊕,⊙): $K \subseteq L$
$\iff$ K podgrupa $(L,\oplus)$
$\iff$ $K\backslash\{0\}$ podgrupa $(L\backslash\{0\},\odot)$

Homomorfizmi

homomorfizem ohranja lastnosti algebrske strukture
monomorfizem je **injektivni** homomorfizem
epimorfizem je **surjektivni** homomorfizem
izomorfizem je **bijektivni** homomorfizem
endomorfizem je preslikava na samega sebe
avtomorfizem je izomorfizem in endomorfizem

Homomorfizem grup $(G_1,\circ_1) \to (G_2,\circ_2)$

$$f : G_1 \to G_2 \quad \ni: \quad f(x \circ_1 y) = f(x) \circ_2 f(y) \quad \forall x,y \in G_1$$

slika enoto prve grupe v enoto druge grupe
slika inverz vsakega elementa prve grupe v inverz njegove slike

Homomorfizem kolobarjev $(M_1, \oplus_1, \odot_1) \to (M_2, \oplus_2, \odot_2)$

$$f : M_1 \to M_2 \quad \ni: \quad f(x \oplus_1 y) = f(x) \oplus_2 f(y) \quad \forall x,y \in M_1$$

$$f : M_1 \to M_2 \quad \ni: \quad f(x \odot_1 y) = f(x) \odot_2 f(y) \quad \forall x,y \in M_1$$

slika additivno enoto prve grupe v enoto druge grupe
slika additivni inverz vsakega elementa prve grupe v inverz njegove slike
slika multiplikativno enoto prve grupe v enoto druge grupe (če obstaja)

Linearna diofantska enačba

$$\forall a_1,a_2 \in \mathbb{Z}, a_1 \perp a_2 \implies \exists x,y \in \mathbb{Z} : a_1x + a_2y = 1$$

inverz elementa a v $\mathbb{Z}_p$ je tak $a^{-1} = x \ mod\ p$, da je $ax + py = 1$, $y \in \mathbb{Z}$, $a^{-1}\ \exists$ če gcd(a,p) = 1 $\implies$ $\mathbb{Z}_p$ polje, če p praštevilo.

$F[x]/(p)$ polje, če je $p \in F[x]$ nerazcepen polinom stopnje ≥ 1

Permutacije

permutacija na končno množico A je poljubna bijektivna funkcija $f : A \to A$. **permutacijska grupa** je množica nekaj permutacij nekaj permutacij iz A, ki z komponiranjem tvorijo grupo.
$S(A)$: množica ∀ permutacij na A
S_n: množica vseh permutacij na $\{1, 2, ..., n\}$; **polna simetrična grupa**
A_n: množica ∀ sodih permutacij iz S_n; **alternirajoča grupa**, $|A_n| = \frac{n!}{2}$
(Cayley) ∀ grupa je izomorfna kaki permutacijski grupi.

Za permutacijo iz S_n rečemo, da je dolžine n, pišemo:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ a_1 & a_2 & a_3 & \dots & a_{n-1} & a_n \end{pmatrix},$$

kjer so vsi a_i paroma različni elementi $\{1, 2, \dots, n\}$.
produkt permutacij: za poljubni permutaciji α in β iz S_n velja:

$$\alpha \circ \beta = \beta * \alpha = \beta\alpha$$

Identiteta reda n je

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n-1 & n \\ 1 & 2 & 3 & \dots & n-1 & n \end{pmatrix}.$$

Za ∀ permutacijo π ∃ inverzna permutacija π^{-1} in velja:

$$\pi * \pi^{-1} = \pi^{-1} * \pi = id.$$

k je **fiksna točka** $\pi \Leftrightarrow \pi(k) =$ k. Rečemo da π **pribije** k; id pribije vsa števila; π in π^{-1} pribijeta ista števila.

π je **cikel** ⇔ ∃ neprazno zaporedje različnih števil:

$$(a_0,a_1,a_2,\dots,a_{r-1})$$

iz množice $\{1,2,\dots,n\}$. Velja:
(1) π pribije vsa števila, ki niso v zaporedju
(2) za števila iz zaporedja velja $\pi(a_k) = a_{k+1 \bmod r}$
(3) r je dolžina cikla
(4) $C = (a_1a_2 \cdots a_n) \Rightarrow C^{-1} = (a_na_{n-1} \cdots a_1)$
(5) C_1 in C_2 disjunktna cikla $\Rightarrow C_1 * C_2 = C_2 * C_1$.
(6) cikel dolžine m razpade na gcd(m,k) ciklov dolžine m/gcd(m,k) v π^k

∀ permutacija se da (enolično) razcepiti na produkt disjunktnih ciklov. Razcep je enoličen do vrstnega reda ciklov. Elementi vsakega cikla razbitja tvorijo **orbite**.

Transpozicija je cikel dolžine 2. ∀ cikel daljši od 2 lahko zapišemo kot produkt transpozicij:

$$(a_1a_2 \cdots a_k) = (a_1a_2)(a_1a_3) \cdots (a_1a_k).$$

∀ permutacija se da zapisati kot produkt transpozicij (zapis ni enoličen, ohrani pa se parnost št. transpozicij). **Parnost** permutacije - št. transpozicij.

Naj ima permutacija $\pi \in S_n$ v zapisu k_i ciklov dolžine i, za $i = 1,...,n$.
Pravimo, da ima π **ciklično strukturo** $(k_1,k_2,...,k_n)$. Velja:

$$1k_1 + 2k_2 + 3k_3 + \ + nk_n = n$$

Red red(π) permutacije π je najmanjši $k \in \mathbb{N}$, za katerega velja $\pi^k =$ id.
(1) Cikel C dolžine m ⇒ red(C) = m
(2) π produkt tujih ciklov dolžine $m_1,m_2...m_k$ ⇒ red(π) = lcm(m_1, $m_2,...,m_k$)
(3) red(π) = red(π^{-1})

Konjugiranost je ekvivalenčna relacija:

$$\pi_1 \approx \pi_2 \ \Rightarrow \exists \tau : \pi_2 = \tau \circ \pi_1 \tau^{-1}$$

π in δ sta konjugirani ⇔ imata enako ciklično strukturo.

Teorija števil

Spodnji celi del $\lfloor x \rfloor = max\{k \in \mathbb{Z}; k \leq x\}$.
Zgornji celi del $\lceil x \rceil = min\{k \in \mathbb{Z}; k \geq x\}$.
Za $m,n \in \mathbb{Z}$ pravimo, da m **deli** n oz. $m \mid n$, če $\exists k \in \mathbb{Z}\ \ni: n = k \cdot m$. Drugače $m \nmid n$.

Lastnosti |
(1) refleksivnost, **(2)** tranzitivnost, **(3)** antisimetričnost na $\mathbb{N}$ in **(4)** delna urejenost na $\mathbb{N}$. **(5)** $m \mid a$ in $m \mid b \Rightarrow m \mid a+b$, **(6)** $m \mid a \Rightarrow m \mid n \cdot a\ n \in \mathbb{N}$

Izrek od deljenju
Naj bosta $n,m \in \mathbb{Z}$ ter m > 0. Potem ∃ enolično določena $k,r \in \mathbb{Z}$ tako da je $n = k \cdot m + r$ in $0 \leq r < m$. Pišemo $r = n \bmod m$.

Največji skupni delitelj gcd(m,n) = $max\{d \in \mathbb{N};\ d \mid m$ in $d \mid n\}$; $m,n \in \mathbb{Z}\ m,n \neq 0$. (gcd(0,n) = n)
Najmanjši skupni večkratnik lcm(m,n) = $min\{v \in \mathbb{N};\ m \mid v$ in $n \mid v\ v \neq 0\}$; $m,n \in \mathbb{Z}\ m,n \neq 0$. (lcm(0,n) = 0)

(T) Naj bo n skupni večkratnik a in b. Potem lcm(a,b) | n.

Evklidov algoritem

Naj bo $a = k \cdot b + r$ in $0 \leq r < b$. Velja gcd(a,b) = gcd(b,r).

Tuji števili

Če je gcd(a,b) = 1, potem sta si a,b∈ $\mathbb{N}$ **tuji** in pišemo $a \perp b$.

(T) Za a,b,c ∈ $\mathbb{N}$ velja: $a \mid b \cdot c \ \wedge\ a \perp b \Rightarrow a \mid c$.
(T) Za a,m ∈ $\mathbb{N}$ velja $m \perp a \Leftrightarrow m \perp (a \bmod m)$.
(I) Za $\forall a,b \in \mathbb{N}$ velja gcd(a,b)· lcm(a,b) = a·b.

Praštevila

$2 \leq$ n ∈ $\mathbb{N}$ je **praštevilo** če ima 2! delitelja - 1 in n. Drugače je n **sestavljeno število**. Par praštevil oblike (p, p + 2) imenujemo **praštevilska dvojčka**.

(T) Naj bosta a,b ∈ $\mathbb{N}$. Velja:
(1) Če je p praštevilo, potem $p \perp a$ ali $p \mid a$.
(2) Če je p praštevilo ter $p \mid a \cdot b$, potem $p \mid a$ ali $p \mid b$.
(3) Za a ≥ 2 ∃ praštevilo p, tako da $p \mid a$.

(I) Praštevil je ∞ mnogo.
(H) Praštevilskih dvojčkov je ∞ mnogo.

Kongruenca po modulu m

Naj bosta a,b ∈ $\mathbb{Z}$ ter m ∈ $\mathbb{N}$, če $m \mid a - b$ pravimo, da sta a in b **kongruenta po modulu** m, pišemo a≡ b (mod m) ⇔ $a \bmod m = b \bmod m$. Sledi ≡ (mod n) je **ekvivalenčna relacija** na $\mathbb{Z}$.

Lastnosti kongruence

(1) Če a ≡ b (mod m) in c ∈ $\mathbb{Z}$:

$$\begin{gathered} \text{a + c} \equiv \text{b + c (mod } m\text{)} \\ \text{a - c} \equiv \text{b − c (mod } m\text{)} \\ \text{a · c} \equiv \text{b · c (mod } m\text{)} \end{gathered}$$

(2) Če a ≡ b (mod m) in c ≡ d (mod m):

$$\begin{gathered} \text{a + c} \equiv \text{b + d (mod } m\text{)} \\ \text{a - c} \equiv \text{b − d (mod } m\text{)} \\ \text{a · c} \equiv \text{b · d (mod } m\text{)} \end{gathered}$$

(3) Če a ≡ b (mod m) in n ∈ $\mathbb{N}$, potem $a^n \equiv b^n$ (mod m).
(4) Če a · c ≡ b · c (mod m) in $c \perp m$, potem a ≡ b (mod m).

REA (Razširjen Evklidov algoritem)

REA poišče ne le gcd(a,b) ampak tudi $s,t \in \mathbb{Z}$, da velja $a \cdot s + b \cdot t =$ gcd(a,b).
Postopek
Začetne vrednosti:

$$\begin{gathered} r_{-1} = a \quad s_{-1} = 1 \quad t_{-1} = 0 \\ r_1 = b \quad s_1 = 0 \quad t_1 = 1 \end{gathered}$$

Iteracija za i = 1,2,...n+1, kjer je n+1 najmanjši indeks, za katerega $r_{n+1} = 0$:

$$\begin{gathered} k_i = \lfloor \tfrac{r_{i-2}}{r_{r-1}} \rfloor \\ r_i = r_{i-2} - k \cdot r_{i-1} \\ s_i = s_{i-2} - k \cdot s_{i-1} \\ t_i = t_{i-2} - k \cdot t_{i-1} \end{gathered}$$

	a	1	0
k_1	b	0	1
k_2	r_1	s_1	t_1
k_3	r_2	s_2	t_2
⋮	⋮	⋮	⋮
k_{n+1}	$r_n \neq 0$	s_n	t_n
	$r_{n+1} = 0$	s_{n+1}	t_{n+1}

$$a \cdot s_i + b \cdot t_i = r_i \ za\ i = -1,0,1 \dots n+1$$
$$r_n \mid r_i \ za\ i = n, n-1, \dots 0, -1$$
$$gcd(a,b) = r_n$$