UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA
MATEMATIKU I INFORMATIKU

Đorđe Dragić

Ispitivanja egzistencije rešenja sistema linearnih Diofantovih jednačina

Master rad

Mentor: dr Petar Đapić

Novi Sad, 2018.

Predgovor

Sistemi linearnih jednačina spadaju među najstarije matematičke probleme. Linearna Diofantova jednačina je jednačina oblika $a_1x_1 + a_2x_2 + \ldots + a_nx_n = b$, gde $a_1, \ldots, a_n, b \in \mathbb{Z}$ i rešenja tražimo isključivo u skupu celih brojeva. Ovaj rad se bavi ispitivanjem egzistencije rešenja sistema ovih jednačina.

U uvodnoj glavi dati su osnovni pojmovi, definicije i teoreme iz opšte i linearne algebre, neophodne za praćenje glavnih delova rada.

U drugoj glavi dati su osnovni pojmovi o sistemima linearnih jednačina, kao i najefikasniji algoritam za njihovo rešavanje, Gausov. Data je i Kroneker-Kapelijeva teorema. U nastavku, dokazana je teorema da je svaka matrica sa celobrojnim elementima ekvivalentna dijagonalnoj matrici specijalnog oblika. Centralno mesto u drugoj glavi zauzima teorema koja sadrži potrebne i dovoljne uslove da postoji celobrojno rešenje posmatranog sistema čime je dokazana i teorema van der Waerden-a o istom problemu.

Treća glava bavi se testerima, linearnim funkcijama, nad skupovima $\mathbb{Q}$ i $\mathbb{Z}_p$, gde je p prost broj. Cilj je pokazati da određeni sistemi nemaju rešenje. Uvode se definicije korisnih i beskorisnih testera i daje se algoritam za nalaženje korisnih testera, a ključnu ulogu ima teorema koja govori da postoje testeri definisani u $\mathbb{Z}_p$ koji su izvedeni iz testera definisanim u prstenu $\mathbb{Z}$. Pomoću ove teoreme se dolazi do korisnih testera. Na kraju glave dati su primeri koji ilustruju prethodno opisano.

U poslednjoj glavi se pokazuje kako testeri mogu biti korisni za pokazivanje i egzistencije rešenja. Pokazuje se da je egzistencija rešenja familije sistema linearnih Diofantovih jednačina uvek određena određenim skupom koji nazivamo kompletan skup testera. Pomoću Smitove normalne forme matrice sistema daje se jednostavan dokaz njegovog postojanja. Proučava se veza između minora matrice sistema i egzistencije kompletnog skupa testera. U ključnoj teoremi ove glave dokazuje se egzistencija kompletnog skupa testera matrice sistema nad $\mathbb{Z}$ i $\mathbb{Z}_d$, gde je d najveći zajednički delilac svih $r \times r$ minora matrice sistema, r je rang te matrice. U nastavku rada dokazuje se teorema o egzistenciji kompletnog skupa testera u $\mathbb{Z}$ i $\mathbb{Z}_m$, gde je m proizvo-

ljan prirodan broj takav da $d\,|m$, čiji značaj leži u izbegavanju rada sa matricama ogromnih koeficijenata. Dati su algoritmi za računanje testera u $\mathbb{Z}_m$, gde je m proizvoljan prirodan broj. Dati su primeri koji ilustruju prethodno izloženo gradivo. Na samom kraju rada su prikazana poređenja dve metode za pokazivanje egzistencije rešenja sistema linearnih Diofantovih jednačina opisane u ovom radu.

Veliku zahvalnost dugujem svom mentoru, dr Petru Đapiću, za nesebičnu pomoć pri izboru teme, koji je svojim savetima i primedbama doprineo izradi ovog master rada. Takođe, zahvaljujem se dr Ivici Bošnjaku i dr Siniši Crvenkoviću što su prihvatili da budu članovi komisije.

Na kraju, najveću zahvalnost dugujem svojoj porodici, majci Angelini i sestri Sanji, zbog beskrajne podrške koju mi svakodnevno pružaju i svim dragim osobama koje su mi bile podrška tokom školovanja.

Ovaj rad posvećujem pokojnom ocu Nenadu.

Đorđe Dragić

Sadržaj

Glava 1

Uvod

1.1 Osnovne definicije

Definicija 1.1.1 (*Skupovi*) *Koristićemo notaciju:*

$\mathbb{N}$ - *skup prirodnih brojeva,*
$\mathbb{Z}$ - *skup celih brojeva,*
$\mathbb{Q}$ - *skup racionalnih brojeva,*
$\mathbb{R}$ - *skup realnih brojeva.*

Sada ćemo se podsetiti definicije grupe, prstena i polja.

Definicija 1.1.2 *Ako je A proizvoljan skup, preslikavanje $\sigma : A \times A \to A$ se naziva binarna operacija skupa A. Tada se uređeni par (A, σ) naziva grupoid.*

Definicija 1.1.3 *Grupoid $(G, *)$ je grupa akko važi*

1. $(\forall x, y, z \in G)\, x * (y * z) = (x * y) * z$
2. $(\exists e \in G)(\forall x \in G)(x * e = e * x = x \wedge (\exists y \in G) x * y = y * x = e)$

Ako je i pored navedenih uslova ispunjen i uslov $(\forall x, y \in G)\, x * y = y * x$ onda se grupa naziva komutativna (ili Abelova).
Element e nazivamo neutralni.

Definicija 1.1.4 *Skup A, koji sadrži bar dva elementa, na kome su definisane dve binarne operacije, označimo ih sa $+$ i $\cdot$, je prsten u odnosu na te operacije, ako su ispunjeni sledeći uslovi:*

1. $(\forall x, y)\, x + y = y + x$

2. $(\forall x, y, z)\, x + (y + z) = (x + y) + z$

3. *Postoji element* 0 *tako da* $(\forall x)\, x+0 = x$, (*gde je sa* 0 *označen neutralni element operacije* +)

4. *Za svako* x *postoji* $-x$ *tako da* $x + (-x) = 0$

5. $(\forall x, y, z)\, x \cdot (y \cdot z) = (x \cdot y) \cdot z$

6. $(\forall x, y, z)\, (x \cdot (y + z) = x \cdot y + x \cdot z \wedge (y + z) \cdot x = y \cdot x + z \cdot x)$

Definicija 1.1.5 *Skup P, koji sadrži bar dva elementa, na kome su definisane dve binarne operacije, označimo ih sa* $+$ *i* $\cdot$ *, je polje u odnosu na te operacije, ako su ispunjeni sledeći uslovi:*

1. *Skup P u odnosu na operaciju* $+$ *čini komutativnu grupu.*

2. *Skup* $P\backslash\{0\}$*, gde je sa* 0 *označen neutralni element operacije* $+$*, u odnosu na operaciju* $\cdot$ *čini komutativnu grupu.*

3. $(\forall a, b, c \in P)\, (a \cdot (b + c) = a \cdot b + a \cdot c \wedge (b + c) \cdot a = b \cdot a + c \cdot a)$

Primer 1.1.1 Struktura $(\mathbb{Z}, +)$ je grupa, a $(\mathbb{N}, +)$ nije grupa. Strukture $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ su prsteni. Za $n \in \{2, 3, \ldots\}$ struktura $(\mathbb{Z}_n, +_n, \cdot_n)$ je prsten, gde je $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, $+_n$ sabiranje po modulu n, a $\cdot_n$ množenje po modulu n. Strukture $(\mathbb{R}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$ i $(\mathbb{Z}_2, +_2, \cdot_2)$ su polja, a $(\mathbb{Z}, +, \cdot)$ nije polje.

Definicija 1.1.6 *Prsten* $(A, +, \cdot)$ *je komutativan akko je* $\cdot$ *komutativna operacija. Prsten sa jedinicom je prsten u kome postoji neutralni element za operaciju* $\cdot$ *.*

Definicija 1.1.7 *Za prsten* $(A, +, \cdot)$ *kažemo da nema delitelje nule akko važi*

$$(\forall x, y \in A)(x \neq 0 \wedge y \neq 0 \Rightarrow x \cdot y \neq 0).$$

Definicija 1.1.8 *Integralni domen je komutativan prsten sa jedinicom bez delitelja nule.*

Ako je $(G, *)$ grupoid i $A, B \subseteq G$, tada koristimo oznaku

$$AB = \{a * b \,|\, a \in A, b \in B\}.$$

Definicija 1.1.9 *Neka je* $(P, +, \cdot)$ *prsten. Struktura* $(I, +, \cdot)$ *je ideal prstena* P $(I \lhd P)$ *akko* $I \subseteq P$ *i važi:*

1. $(I, +)$ *je komutativna grupa;*

2. $IP \subseteq I$, $PI \subseteq I$.

Definicija 1.1.10 *Integralni domen G je Euklidov ako postoji funkcija $\delta : a \to \delta(a)$ iz G u $\mathbb{N}$ tako da ako $a, b \neq 0 \in G$, onda postoje $q, r \in G$ takvi da važi $a = bq + r$, gde $\delta(r) < \delta(b)$.*

Prsten $\mathbb{Z}$ jeste Euklidov domen ako funkciju δ definišemo kao $\delta(a) = |a|$.

Definicija 1.1.11 *Integralni domen je domen glavnih ideala ako su svi njegovi ideali glavni ($\forall I \triangleleft P$ važi $I =< a >_i$)*

1.2 Matrice

Pre nego što uvedemo definiciju determinante definisaćemo matricu.

Definicija 1.2.1 *Matrica tipa $m \times n$ nad poljem $(P, +, \cdot)$ je preslikavanje $A : I \times J \to P$ gde je $I = \{1, \ldots, m\}$ i $J = \{1, \ldots, n\}$. Element $A(i, j)$ označavamo sa a_{ij}. Matricu A zapisujemo u obliku pravougaone šeme koja ima m vrsta i n kolona:*

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{bmatrix}$$

Celu matricu zapisujemo i u obliku $[a_{ij}]_{m,n}$. Prema definiciji preslikavanja, $[a_{ij}]_{m,n} = [b_{ij}]_{t,s}$ važi akko $m = t, n = s$ i za sve $1 \leq i \leq m$ i $1 \leq j \leq n$ važi $a_{ij} = b_{ij}$. Transponovana matrica matrice $[a_{ij}]_{m,n}$, u oznaci $[a_{ij}]^T_{m,n}$ je matrica $[a_{ji}]_{n,m}$. Ako je $m = n$ matricu $[a_{ij}]_{n,n}$ nazivamo kvadratna matrica reda n.

Elementi $a_{11}, a_{22}, \ldots, a_{nn}$ kvadratne matrice

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}$$

čine njenu glavnu dijagonalu, a elementi $a_{n1}, a_{n-1,2}, \ldots, a_{1n}$ sporednu.

Jedinična matrica je kvadratna matrica reda n kod koje je $a_{ii} = 1$, a $a_{ij} = 0$ za $i \neq j$ i označavamo je sa E:

$$E = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}_{n \times n}$$

Nula matrica je matrica tipa $m \times n$ čiji su svi elementi 0 i nju ćemo označavati sa O. Zbir matrica $[a_{ij}]_{m,n}$ i $[b_{ij}]_{m,n}$ istih formata je matrica data sa

$$[a_{ij}]_{m,n} + [b_{ij}]_{m,n} \stackrel{\text{def}}{=} [a_{ij} + b_{ij}]_{m,n}.$$

Ako je $[a_{ij}]_{m,n}$ proizvoljna matrica tada je rezultat njenog množenja brojem $k \in P$ matrica data sa

$$k \cdot [a_{ij}]_{m,n} = [k \cdot a_{ij}]_{m,n}.$$

Vektor je matrica tipa $1 \times n$ ili $n \times 1$. Matricu $(-1)A$ označavaćemo sa $-A$. Oduzimanje matrica definisaćemo sa

$$A - B = A + (-B).$$

Za svake tri matrice A, B, C, istog tipa nad poljem P i za svako $\alpha, \beta \in P$ važi:

1. $A + (B + C) = (A + B) + C$,
2. $A + O = O + A = A$,
3. $A + (-A) = (-A) + A = O$,
4. $A + B = B + A$,
5. $\alpha(A + B) = \alpha A + \alpha B$,
6. $(\alpha + \beta)A = \alpha A + \beta A$,
7. $\alpha(\beta A) = (\alpha\beta)A$,
8. $1A = A$.

Navedene jednakosti se lako dokazuju na osnovu odgovarajućih osobina polja P. Za razliku od sabiranja matrica i množenja matrica skalarom, koje se definišu jednostavno, množenje matrica se definiše na složeniji način.

Definicija 1.2.2 *Neka su date matrice $A = [a_{ij}]_{m,r}$ i $B = [b_{ij}]_{r,n}$. Proizvod matrica A i B je matrica tipa $m \times n$ data sa*

$$[a_{ij}]_{m,r} \cdot [b_{ij}]_{r,n} = [a_{i1}b_{1j} + a_{i2}b_{2j} + \ldots + a_{ir}b_{rj}]_{m,n}$$

Dakle, proizvod AB dve matrice A i B je definisan akko je broj kolona matrice A jednak broju vrsta matrice B. Ako postoji proizvod matrica A i B, ne mora postojati proizvod matrica B i A. Ako postoje oba proizvoda tada rezultat ne moraju biti matrice istog tipa, a ako jesu istog tipa ne moraju biti jednake. Dakle, množenje matrica nije komutativno.
Za svaku kvadratnu matricu A istog reda kao E važi

$$AE = EA = A.$$

Kvadratna matrica čiji su svi elementi izvan glavne dijagonale jednaki nuli naziva se dijagonalna matrica.

Teorema 1.2.1 *Ako su $A = [a_{ij}], B = [b_{ij}]$ i $C = [c_{ij}]$ tri matrice takve da su proizvodi AB i BC definisani, onda su i proizvodi $(AB)C$ i $A(BC)$ takođe definisani i*

$$A(BC) = (AB)C.$$

1.3 Determinante

Da bismo mogli da damo definiciju determinante n-tog reda potrebno je da se najpre upoznamo sa permutacijama.

Definicija 1.3.1 *Neka je S konačan skup sa n elemenata. Bijektivno preslikavanje skupa S na S naziva se permutacija tog skupa.*

Kako za izučavanje permutacija individualna svojstva elemenata skupa S nemaju značaja, uzećemo da skup S čini prvih n prirodnih brojeva $1, 2, \ldots, n$. Takođe permutacije možemo pisati u obliku tablice

$$\begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$$

gde se ispod elementa 1 nalazi element i_1, itd. Elementi $i_1, i_2, \ldots, i_n$ skupa $\{1, 2, \ldots, n\}$, napisani u određenom poretku, potpuno određuju permutaciju tog skupa. Koristićemo skraćeni zapis $(i_1, i_2, \ldots, i_n)$ permutacije $\pi(k) = i_k$, $\forall k \in S$, gde $1 \to i_1, \ldots, n \to i_n$.

Smatramo da su $(2,1,3), (2,3,1), (1,2,3), (1,3,2), (3,1,2), (3,2,1)$ permutacije skupa $\{1, 2, 3\}$.

Definicija 1.3.2 *Za bilo koji par elemenata i, j permutacije, takav da i prethodi j, rećićemo da čini inverziju ukoliko je $i > j$.*

Definicija 1.3.3 *Permutaciju koja ima paran broj inverzija nazivamo parna, a permutaciju sa neparnim brojem inverzija nazivamo neparna.*

Primer 1.3.1 Neka je $S = \{1, 2, 3, 4, 5\}$. Permutacija $(2, 5, 3, 1, 4)$ je neparna jer ima 5 inverzija, a permutacija $(4, 3, 2, 1, 5)$ je parna jer ima 6 inverzija.

Definicija 1.3.4 *Ako u nekoj permutaciji uzajamno zamene mesta bilo koja dva elementa, a ostali elementi se ne pomerajaju, onda se dobija nova permutacija. Takva transformacija permutacije naziva se transpozicija.*

Teorema 1.3.1 *Svaka transpozicija menja parnost permutacije.*

Dokaz. Prvo ćemo razmotriti slučaj kada su elementi i, j koji zamenjuju mesta susedni, tj. posmatramo permutaciju oblika:

$$a_1, a_2, \ldots, a_p, i, j, b_1, b_2, \ldots, b_q.$$

Posle transpozicije dobija se permutacija

$$a_1, a_2, \ldots, a_p, j, i, b_1, b_2, \ldots, b_q.$$

Primećujemo da je broj inverzija koji i i j obrazuju sa $a_1, a_2, \ldots, a_p, b_1, b_2, \ldots, b_q$ isti i u jednoj i u drugoj permutaciji. Ako je $i > j$, onda par i, j čini inverziju u prvoj permutaciji ali ne čini u drugoj, a obrnuto važi ako je $i < j$. Dakle, broj inverzija nove permutacije se za jedan razlikuje od broja inverzija stare permutacije, pa je parnost permutacije promenjena.
Sada razmatramo slučaj kada i i j nisu susedni:

$$a_1, a_2, \ldots, a_p, i, c_1, c_2, \ldots, c_r, j, b_1, b_2, \ldots, b_q.$$

Izvršimo niz od $r+1$ transpozicija na ovoj permutaciji i dobijamo permutaciju

$$a_1, a_2, \ldots, a_p, c_1, c_2, \ldots, c_r, j, i, b_1, b_2, \ldots, b_q.$$

Ako sada izvršimo niz od r transpozicija dobićemo permutaciju

$$a_1, a_2, \ldots, a_p, j, c_1, c_2, \ldots, c_r, i, b_1, b_2, \ldots, b_q.$$

Ova permutacija je dobijena od polazne zamenom mesta elemenata i i j vršenjem $r + 1 + r = 2r + 1$ transpozicija susednih elemenata. Videli smo da svaka transpozicija susednih elemenata menja parnost, pa posle vršenja neparnog broja takvih transpozicija parnost permutacije će opet biti promenjena, što je i trebalo dokazati.

□

Sada ćemo definisati determinantu n-tog reda.

Definicija 1.3.5 *Ako je*

$$A = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{bmatrix}$$

kvadratna matrica reda n nad poljem $(P, +, \cdot)$, onda je determinanta reda n matrice A algebarski zbir svih mogućih proizvoda od po n elemenata matrice A, takvih da se u svakom proizvodu pojavljuje po jedan i samo jedan element iz svake vrste i svake kolone date matrice (svaki takav proizvod nazivamo član determinante), gde član $a_{1i_1}a_{2i_2}\cdots a_{ni_n}$ uzimamo sa znakom + ako je permutacija $i_1, i_2, \dots, i_n$ parna, a sa znakom − ako je ta permutacija neparna. Determinantu matrice A označavamo sa $|A|$ ili

$$\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}.$$

Postupak računanja determinanti se pojednostavljuje ako matrica sadrži nule. Zbog toga su posebno značajne transformacije matrice kojima se matrica može dovesti na oblik koji sadrži veći broj nula.

Vrste determinante su vrste njene odgovarujuće matrice, a kolone determinante su kolone njene odgovarajuće matrice.

Teorema 1.3.2 *Determinanta se ne menja ako se njene vrste zamene kolonama ne menjajući poredak, tj. ako je*

$$D_1 = \begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}, \quad D_2 = \begin{vmatrix} a_{11} & a_{21} & \dots & a_{n1} \\ a_{12} & a_{22} & \dots & a_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1n} & a_{2n} & \dots & a_{nn} \end{vmatrix}$$

onda je $D_1 = D_2$.

Teorema 1.3.3 *Ako dve vrste (ili kolone) determinante zamene mesta, determinanta menja znak.*

Teorema 1.3.4 *Determinanta je jednaka nuli ako su bilo koje njene dve vrste (ili kolone) jednake.*

Teorema 1.3.5 *Ako je svaki element k-te vrste determinante D n-tog reda prikazan kao zbir dva sabirka, tj.* $a_{kj} = b_{kj} + c_{kj}, (j = 1, 2, \ldots, n)$*, onda je ta determinanta jednaka zbiru determinanti* D_1 *i* D_2 *čije su sve vrste, sem k-te, iste kao u determinanti D, k-ta vrsta determinante* D_1 *je* $b_{k1}, b_{k2}, \ldots, b_{kn}$*, a determinante* D_2 *je* $c_{k1}, c_{k2}, \ldots, c_{kn}$*.*

Pre nego što navedemo ostale osobine definisaćemo dva nova pojma.

Definicija 1.3.6 *Minor* M_{ij} *elementa* a_{ij} *(koji se nalazi u i-toj vrsti i j-toj koloni) determinante D reda n, je determinanta reda* $n-1$ *koja se dobija iz D izostavljanjem i-te vrste i j-te kolone.*
Alegebarski komplement (ili kofaktor) A_{ij} *elementa* a_{ij} *je*

$$A_{ij} = (-1)^{i+j} M_{ij}.$$

Teorema 1.3.6 *Ako su svi elementi i-te vrste determinante D jednaka nuli, sem elementa* a_{ij} *koji ne mora biti jednak nuli, onda je*

$$D = a_{ij} A_{ij}.$$

Teorema 1.3.7 *Determinanta je jednaka zbiru proizvoda elemenata jedne vrste (ili kolone) i njihovih algebarskih komplemenata, tj. ako je* $A = [a_{ij}]_{n,n}$ *proizvoljna matrica,* $1 \leq i, j \leq n$ *tada je:*

$$|A| = a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in}.$$

Teorema 1.3.8 *Ako je determinanta* D_1 *dobijena od determinante D tako što je svaki element jedne vrste (ili kolone) determinante D pomnožen istim brojem k, onda je*

$$k \cdot D = D_1.$$

Teorema 1.3.9 *Determinanta je jednaka nuli ako su elementi jedne njene vrste (ili kolone) proporcionalni elementima neke druge vrste (ili kolone).*

Teorema 1.3.10 *Determinanta se ne menja ako se elementima jedne njene vrste (ili kolone) dodaju odgovarajući elementi neke druge vrste (ili kolone) prethodno pomnoženi nekim brojem datog polja.*

Teorema 1.3.11 *Zbir proizvoda svih elemenata neke vrste (ili kolone) determinante i algebarskih komplemenata odgovarajućih elemenata neke druge vrste (ili kolone) jednak je nuli, tj. ako je* $A = [a_{ij}]_{n,n}$ *proizvoljna matrica,* $1 \leq i, j \leq n \wedge i \neq j$ *tada je:*

$$a_{i1}A_{j1} + a_{i2}A_{j2} + \ldots + a_{in}A_{jn} = 0.$$

1.4 Vektorski prostori

Definicija 1.4.1 *Skup V je vektorski prostor nad poljem P ako je na V definisana binarna operacija $+$ tako da V u odnosu na tu operaciju čini komutativnu grupu, a svakom paru (α, a), $\alpha \in P$, $a \in V$, pridružen je jedan element iz skupa V, koji označavamo sa αa i nazivamo ga proizvod α i a, tako da važi:*

1. $(\forall \alpha \in P)(\forall a, b \in V) \qquad \alpha(a+b) = \alpha a + \alpha b,$
2. $(\forall \alpha, \beta \in P)(\forall a \in V) \qquad (\alpha+\beta)a = \alpha a + \beta a,$
3. $(\forall \alpha, \beta \in P)(\forall a \in V) \qquad \alpha(\beta a) = (\alpha\beta)a,$
4. $(\forall a \in)V \qquad 1a = a,$

gde je sa 1 označen jedinični element polja P.

Elemente skupa V nazivamo vektori, a elemente polja P nazivamo skalari. Vektorski prostor V nad poljem P označavaćemo i sa $V(P)$.

Teorema 1.4.1 *Neka je V vektorski prostor nad poljem P. Tada važi:*

(1) nula-vektor je jedinstven,

(2) za svaki vektor suprotni vektor je jedinstven,

(3) $(\forall a \in V)\ -(-a) = a,$

(4) Važi zakon skraćivanja za sabiranje vektora,

(5) $(\forall \alpha \in P)\, \alpha 0_V = 0_V$, *(Sa 0_V označen je nula-vektor iz V.)*

(6) $(\forall a \in V)\, 0a = 0,$

(7) $(\forall \alpha \in P)(\forall a \in V)\, (-\alpha)a = -(\alpha a) = \alpha(-a),$

(8) $(\forall \alpha \in P)(\forall a \in V)\, \alpha a = 0 \Leftrightarrow \alpha = 0 \vee a = 0.$

Dokaz. Osobine 1-4 važe u svakoj grupi.

(5) Kako je za svako $\alpha \in P$, $\alpha 0_V = \alpha(0_V + 0_V) = \alpha 0_V + \alpha 0_V$, sledi $\alpha 0_V = 0_V$.

(6) Kako je za svako $a \in V$, $0a = (0+0)a = 0a + 0a$, sledi $0a = 0$.

(7) Za svako $a \in V$ i $\alpha \in P$, $0 = 0a = (\alpha - \alpha)a = \alpha a + (-\alpha)a$, odakle je $(-\alpha)a = -(\alpha a)$. Slično, $0 = \alpha 0 = \alpha(a - a) = \alpha a + \alpha(-a)$, pa je $\alpha(-a) = -(\alpha a)$.

(8) Na osnovu (5) i (6) sledi $(\forall \alpha \in P)(\forall a \in V)\alpha = 0 \vee a = 0 \Rightarrow \alpha a = 0$. Obrnuto, ako je $\alpha a = 0$, onda je $\alpha = 0$ ili $\alpha \neq 0$. U prvom slučaju nema šta da se dokazuje, a ako je $\alpha \neq 0$, onda postoji $\alpha^{-1} \in P$, pa je

$$\alpha^{-1}(\alpha a) = \alpha^{-1}0 \to (\alpha^{-1}\alpha)a = 0 \to 1a = 0 \to a = 0.$$

□

Definicija 1.4.2 *Neka je V vektorski prostor nad poljem P. Podskup W skupa V je potprostor vektorskog prostora V, ako je W vektorski prostor nad poljem P u odnosu na restrikcije na W sabiranja vektora i množenja vektora skalarom.*

Sledeća teorema daje jednostavan kriterijum za utvrđivanje da li je neki podskup vektorskog prostora potprostor.

Teorema 1.4.2 *Neprazan podskup W vektorskog prostora V nad poljem P je potprostor od V ako i samo ako za svako $\alpha, \beta \in P$, $a, b \in W$*

$$\alpha a + \beta b \in W. \tag{1.1}$$

Dokaz. Nije teško proveriti da je uslov (1.1) ekvivalentan sa sledećim uslovom: za svako $\alpha \in P$, $a, b \in W$

$$\alpha a \in W \wedge a + b \in W. \tag{1.2}$$

Ako je W potprostor, on je zatvoren u odnosu na množenje vektora skalarom i sabiranje vektora, pa odatle sledi da važi (1.2) (a to znaži da važi i (1.1)). Neka je sada ispunjen uslov (1.1)(a to znači i (1.2)). Iz (1.2) sledi da je W zatvoren u odnosu na sabiranje vektora a proizvod skalara iz P i vektora iz W je vektor u W. Asocijativnost i komutativnost se prenosi sa skupa V na skup W. Neutralni element za sabiranje 0 pripada W jer za $0 \in P$ i $a \in W$, $0a = 0 \in W$. Za svaki neutralni element $a \in W$, $(-1)a = -a \in W$. Zbog toga je $(W, +)$ komutativna grupa. Takođe važe i svi uslovi iz definicije vektorskog prostora za W.

□

Primer 1.4.1 Neka je

$$\left\{\begin{array}{l} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = 0 \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = 0 \end{array}\right.$$

homogen sistem jednačina sa koeficijentima iz polja P. Skup rešenja ovog sistema je potprostor vektorskog prostora P^n. Zaista, neka su $c = (c_1, c_2, \ldots, c_n)$ i $d = (d_1, \ldots, d_n)$ dva rešenja sistema. Ubacimo $\alpha c + \beta d$ u proizvoljnu (recimo i-tu) jednačinu umesto $(x_1, \ldots, x_n)$. Tada je

$$a_{i1}(\alpha c_1 + \beta d_1) + \ldots + a_{in}(\alpha c_n + \beta d_n) =$$

$$\alpha(a_{i1}c_1 + \ldots + a_{in}c_n) + \beta(a_{i1}d_1 + \ldots + a_{in}d_n) = 0 + 0 = 0,$$

pa je i $\alpha c + \beta d$ takođe rešenje datog sistema.

Definicija 1.4.3 *U vektorskom prostoru $V(P)$, vektor v je linearna kombinacija vektora $a_1, \ldots, a_n$ ako postoje skalari $\alpha_1, \ldots, \alpha_n$ takvi da je*

$$v = \alpha_1 a_1 + \ldots + \alpha_n a_n.$$

Ako je S bilo koji neprazan podskup vektorskog prostora V onda je skup $L(S)$ svih linearnih kombinacija vektora iz S potprostor vektorskog prostora V.

Definicija 1.4.4 *Ako je S bilo koji neprazan podskup vektorskog prostora V, onda se potprostor $L(S)$ svih linearnih kombinacija vektora iz S naziva potprostor generisan skupom S.*
Potprostor $L(S)$ je očigledno minimalan prostor koji sadrži skup S.
Elemente skupa S nazivaćemo generatori potprostora $L(S)$ i rećićemo da oni generišu potprostor $L(S)$.
Ako je $L(S) = V$ onda je vektorski prostor V generisan skupom S a elementi skupa S su generatori prostora V.

Definicija 1.4.5 *U vektorskom prostoru $V(P)$ niz vektora $(a_1, \ldots, a_n)$ je linearno zavisan, ako postoje skalari $\alpha_1, \ldots, \alpha_n$, od kojih je bar jedan različit od nule, takvi da je*

$$\alpha_1 a_1 + \ldots + \alpha_n a_n = 0.$$

Niz vektora koji nije linearno zavisan je linearno nezavisan.

Teorema 1.4.3 *U vektorskom prostoru $V(P)$ niz vektora $(a_1, \ldots, a_n)$, $n \geq 2$, je linearno zavisan ako i samo ako među vektorima $a_2, \ldots, a_n$ postoji vektor a_k koji je linearna kombinacija vektora $a_1, \ldots, a_{k-1}$.*

Primetimo da je niz koji sadrži nula-vektor linearno zavisan.

Definicija 1.4.6 *Baza konačno generisanog vektorskog prostora je niz vektora koji je linearno nezavisan i koji generiše vektorski prostor.*

Teorema 1.4.4 *U vektorskom prostoru $V(P)$ niz vektora je baza ako i samo ako je taj niz maksmimalan linearno nezavisan niz.*

Teorema 1.4.5 *U vektorskom prostoru $V(P)$ niz vektora $(a_1, \ldots, a_n)$ je baza ako i samo ako se svaki vektor $x \in V$ može na jedinstven način napisati u obliku*

$$x = \sum_{i=1}^{n} \alpha_i a_i, \ \alpha_1, \ldots, \alpha_n \in P. \tag{1.3}$$

Teorema 1.4.6 *Ako je $(a_1, \ldots, a_k)$ linearno nezavisan niz vektora konačno generisanog vektorskog prostora $V(P)$, onda je taj niz baza vektorskog prostora ili postoje vektori $b_1, \ldots, b_m \in V$ takvi da je $(a_1, \ldots, a_k, b_1, \ldots, b_m)$ baza vektorskog prostora (tj. u konačno generisanom vektorskom prostoru svaki linearno nezavisan niz vektora je baza ili se može dopuniti do baze tog vektorskog prostora).*

Definicija 1.4.7 *Broj vektora baze konačno generisanog nenula vektorskog prostora $V(P)$ naziva se dimenzija tog vektorskog prostora i označava sa $dim(V)$. Dimenzija nula-prostora je* 0.

1.5 Inverzna matrica. Elementarne transformacije. Rang matrice

Definicija 1.5.1 *Neka je*

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix}$$

kvadratna matrica reda n. Ako je sa A_{ij} označen kofaktor elementa a_{ij} u determinanti $|A|$, onda se matrica

$$A^* = \begin{bmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & a_{22} & \ldots & A_{n2} \\ \vdots & \vdots & \ddots & \vdots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{bmatrix}$$

naziva adjungovana matrica matrice A.

Definicija 1.5.2 *Kvadratna matrica A je regularna ili invertibilna ako postoji kvadratna matrica B takva da je*

$$AB = BA = E.$$

Matrica B koja zadovoljava prethodni uslov naziva se inverzna matrica za matricu A i najčešće se označava sa A^{-1}.
Kvadratna matrica za koju ne postoji inverzna matrica naziva se singularna.

Sledeća teorema daje kriterijum pomoću koga se može utvrditi da li je neka matrica regularna.

Teorema 1.5.1 *Kvadratna matrica A je regularna akko je $|A| \neq 0$.*

Definicija 1.5.3 *Elementarne transformacije matrice A tipa $m \times n$ su sledeće transformacije:*

1. *međusobna zamena dve vrste (kolone) matrice A,*
2. *Množenje svih elemenata jedne vrste (kolone) matrice A skalarom različitim od nule,*
3. *Dodavanje elemenata jedne vrste (kolone) matrice A, prethodno pomnoženih istim skalarom, odgovarajućim elementima neke druge vrste (kolone) te matrice.*

Ako je matrica B dobijena od matrice A vršenjem konačnog niza elementarnih transformacija, onda kažemo da je matrica A ekvivalentna sa matricom B i to zapisujemo $A \sim B$.

Definicija 1.5.4 *Elementarne matrice su matrice dobijene vršenjem jedne od elementarnih transformacija na jedniničnoj matrici E.*
Označavamo ih sa:
E_{ij} *(matrica dobijena od jedinične matrice zamenom i-te i j-te vrste),*
$E_i(a)$ *(matrica dobijena od jedinične množenjem elemenata i-te vrste sa a),*
$E_{ij}(a)$ *(matrica dobijena od jedinične dodavanjem elemenata j-te vrste, prethodno pomnoženih sa a, odgovarajućim elementima i-te vrste).*

Neka je $A = [a_{ij}]$ proizvoljna matrica tipa $m \times n$ nad poljem P. Ako kolone matrice A posmatramo kao vektore vektorskog prostora P^n:

$$k_1 = (a_{11}, a_{21}, \ldots, a_{m1}),\ k_2 = (a_{12}, a_{22}, \ldots, a_{m2}), \ldots,\ k_n = (a_{1n}, a_{2n}, \ldots, a_{mn}),$$

onda se potprostor $L(k_1, k_2, \ldots, k_n)$ vektorskog prostora P^n, generisan vektorima $k_1, k_2, \ldots, k_n$, naziva prostor kolona matrice A.
Slično se definiše prostor vrsta matrice A.

Definicija 1.5.5 *Dimenzija prostora kolona matrice A naziva se rang po kolonama matrice A. Dimenzija prostora vrste matrice A naziva se rang po vrstama matrice A.*

Teorema 1.5.2 *Rang po kolonama proizvoljne matrice A jednak je rangu po vrstama te matrice.*

Dokaz. Neka je $A = [a_{ij}]$ matrica tipa $m \times n$ nad poljem P. Prostor kolona $L(k_1, k_2, \ldots, k_n)$ date matrice generisan je vektorima

$$k_1 = (a_{11}, a_{21}, \ldots, a_{m1}),\ k_2 = (a_{12}, a_{22}, \ldots, a_{m2}), \ldots,\ k_n = (a_{1n}, a_{2n}, \ldots, a_{mn}).$$

Pretpostavimo da je rang po kolonama (tj. dimenzija prostora kolona) date matrice r i neka je r vektora

$$p_1 = (b_{11}, b_{21}, \ldots, b_{m1}),\ p_2 = (b_{12}, b_{22}, \ldots, b_{m2}), \ldots,\ p_r = (b_{1n}, b_{2n}, \ldots, b_{mr})$$

čine bazu prostora kolona.
Svaki od vektora $k_1, k_2, \ldots, k_n$ može prikazati kao linearna kombinacija vektora baze $p_1, p_2, \ldots, p_r$:

$$\begin{aligned} k_1 &= c_{11}p_1 + c_{12}p_2 + \ldots + c_{1r}p_r, \\ k_2 &= c_{21}p_1 + c_{22}p_2 + \ldots + c_{2r}p_r, \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ k_r &= c_{n1}p_1 + c_{n2}p_2 + \ldots + c_{nr}p_r, \end{aligned}$$

gde su c_{ij} skalari.
Ako u gornjim jednakostima izjednačimo odgovarajuće komponente vektora na levoj i desnoj strani jednakosti, dobićemo da za svako $i = 1, 2, \ldots, m$ važi

$$\begin{aligned} a_{i1} &= c_{11}b_{i1} + c_{12}b_{i2} + \ldots + c_{1r}b_{ir}, \\ a_{i2} &= c_{21}b_{i1} + c_{22}b_{i2} + \ldots + c_{2r}b_{ir} \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{in} &= c_{n1}b_{i1} + c_{n2}b_{i2} + \ldots + c_{nr}b_{ir}. \end{aligned}$$

Ovaj sistem skalarnih jednačina može se napisati u obliku vektorske jednačine (za svako $i = 1, 2, \ldots, m$)):

$$(a_{i1}, a_{i2}, \ldots, a_{in}) = b_{i1}(c_{11}, c_{21}, \ldots, c_{n1}) + b_{i2}(c_{12}, c_{22}, \ldots, c_{n2}) + \ldots +$$

$$b_{ir}(c_{1r}, c_{2r}, \ldots, c_{nr}).$$

Dokazali smo da je svaka vrsta matrice A linearna kombinacija r vektora $(c_{11}, c_{21}, \ldots, c_{n1}), (c_{12}, c_{22}, \ldots, c_{n2}), \ldots, (c_{1r}, c_{2r}, \ldots, c_{nr})$, a to znači da je prostor vrsta matrice A dimenzije manje ili jednake r. Dakle, rang po vrstama

matrice A je manji ili jednak od ranga po kolonama te matrice.
Analogno se dokazuje da važi i obrnuto, tj. da je rang po kolonama manji ili jednak od ranga po vrstama date matrice, što znači da su ti rangovi jednaki, što je i trebalo dokazati.

□

Prethodna teorema nam omogućava da definišemo rang matrice kao zajedničku vrednost za rang po kolonama i rang po vrstama.

Definicija 1.5.6 *Rang po kolonama, odnosno rang po vrstama, matrice A nazivamo rang matrice i označavamo sa $rang(A)$.*

Definicija 1.5.7 *Neka je $A = [a_{ij}]$ matrica tipa $m \times n$ nad poljem P. Ako je $k \leq m$, $l \leq n$, i ako odaberemo proizvoljnih k vrsta i l kolona matrice A, onda svi elementi te matrice koji se nalaze u presecima odabranih vrsta i kolona čine podmatricu formata $k \times l$ date matrice.*
Minor matrice je determinanta njene kvadratne podmatrice.

Teorema 1.5.3 *Matrica A, različita od nula matrice, je ranga r ako i samo ako je bar jedan njen minor reda r različit od nule, a svi minori reda $r + 1$ su jednaki nuli.*

Sada ćemo pokazati kako se do ranga matrice može doći jednostavnije, korišćenjem elementarnih transformacija.

Teorema 1.5.4 *Vršenjem elementarnih transformacija na matrici ne menja se njen rang.*

Dokaz. Neka je $A = [a_{ij}]$ proizvoljna matrica tipa $m \times n$ nad poljem P.
Matrica $E_{ij}A$ ima iste vrste kao A, jedino su i-ta i j-ta vrsta zamenile mesta što ne utiče na linearnu zavisnost vektora vrsta te metrice, pa je $rang(E_{ij}A) = rang(A)$.
Analogno, posmatrajući kolone matrice A, dobija se da je $rang(E_{ij}^T A) = rang(A)$.
Matrica $E_i(\alpha)A, \alpha \neq 0$, ima iste vrste kao A, jedino je i-ta vrsta pomnožena sa $\alpha(\neq 0)$, što ne utiče na linearnu zavisnost vektora vrsta te matrice, pa je $rang(E_i(\alpha)A) = rang(A)$.
Analogno, posmatrajući kolone matrice A, dobija se da je $rang(AE_i^T(\alpha)) = rang(A)$.
Matricu A zapisaćemo u obliku $A = [A_1, \ldots, A_n]$, gde su $A_i = [a_{ij}]_{m\times 1}$ kolone matrice A. Tada je $AE_{ij}^T(\alpha) = [A_1, \ldots, A_{i-1}, A_i + \alpha A_j, A_{i+1}, \ldots, A_n]$.
Uporedićemo potprostore vektorskog prostora P, $S = L(A_1, \ldots, A_n)$ i $T =$

$L(A_1, \ldots, A_{i-1}, A_i + \alpha A_j, A_{i+1}, \ldots, A_n)$.
Očigledno je $S \supseteq T$ jer je svaki generator prostora T linearna kombinacija vektora iz S. Međutim, kako je $A_i = (A_i + \alpha A_j) - \alpha A_j$, vidimo da je i svaki generator prostora S linearna kombinacija vektora iz T, pa je $T \supseteq S$. Prema tome, $S = T$, što znači da je $rang(AE_{ij}^T(\alpha)) = rang(A)$.
Analogno se dokazuje da je $rang(E_{ij}(\alpha)A = rang(A)$.

□

Primer 1.5.1 Odrediti rang matrice

$$A = \begin{bmatrix} 17 & 102 & 136 & 187 \\ 13 & 78 & 104 & 143 \\ 29 & 174 & 232 & 319 \end{bmatrix}.$$

Na matrici A vršimo sledeće elementarne transformacije: drugoj vrsti dodajemo prvu pomnoženu sa $-\frac{13}{17}$, a zatim trećoj vrsti dodajemo prvu pomnoženu sa $-\frac{29}{17}$. Dobijamo da je $rang(A) = 1$.

$$A = \begin{bmatrix} 17 & 102 & 136 & 187 \\ 13 & 78 & 104 & 143 \\ 29 & 174 & 232 & 319 \end{bmatrix} \sim \begin{bmatrix} 17 & 102 & 136 & 187 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

Teorema 1.5.5 *Svaka matrica $A = [a_{ij}]_{m\times n}$ nad poljem P elementarnim transformacijama se može svesti na matricu*

$$B = \begin{bmatrix} b_{11} & b_{12} & b_{13} & \ldots & b_{1r} & \ldots & b_{1n} \\ 0 & b_{22} & b_{23} & \ldots & b_{2r} & \ldots & b_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & b_{rr} & \ldots & b_{rn} \\ 0 & 0 & 0 & \ldots & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & \ldots & 0 \end{bmatrix},$$

gde je $0 \leq r \leq \min\{m, n\}$, $b_{ii} \neq 0$, $i = 1, \ldots, r$.

Dokaz. Ako je $A = O$, teorema očigledno važi ($r = 0$).
Ako je $A \neq O$, onda postoji element $a_{ij} \neq 0$. Sada ćemo zameniti prvu i i-tu vrstu i prvu i j-tu kolonu. Time element a_{ij} dolazi u gornji levi ugao. Dakle, matricu A smo transformisali u matricu $C = [c_{ij}]$ kod koje je $c_{11} = a_{ij}$. Ako drugoj vrsti matrice C dodamo prvu vrstu pomnoženu sa $-c_{21}/c_{11}$, trećoj

vrsti prvu pomnoženu sa $-c_{31}/c_{11}$ itd., poslednjoj vrsti prvu pomnoženu sa $-c_{m1}/c_{11}$, dobićemo matricu

$$D = \begin{bmatrix} c_{11} & c_{12} & \dots & c_{1n} \\ 0 & d_{22} & \dots & d_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & d_{m2} & \dots & d_{mn} \end{bmatrix}.$$

Ako su svi elementi d_{ij} jednaki nuli posao je završen.
Ako nisu, onda postoji element $d_{pq} \neq 0$, pa ako zamenimo drugu i p-tu vrstu i drugu i q-tu kolonu matrice D, dobijamo matricu D_1 kod koje se element d_{pq} nalazi na poziciji $(2, 2)$. Primenjujući isti postupak na D_1, dobićemo matricu

$$F = \begin{bmatrix} c_{11} & c_{12} & c_{13} & \dots & c_{1n} \\ 0 & d_{22} & d_{23} & \dots & d_{2n} \\ 0 & 0 & f_{33} & \dots & f_{3n} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & f_{m3} & \dots & f_{mn} \end{bmatrix}.$$

Produžujući ovaj postupak dalje, na kraju dobijamo matricu B navedenu u teoremi.

□

Matrica B iz prethodne teoreme naziva se stepenasta matrica. Rang te matrice je r, pa prema tome je i rang matrice A takođe r.

Posledica 1.5.1 *Svaka matrica $A = [a_{ij}]_{m\times n}$ nad poljem P, elementarnim transformacijama može se svesti na matricu tipa $m \times n$*

$$\begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 0 & \dots & 0 \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & 0 & \dots & 0 \end{bmatrix},$$

koja ima r jedinica na dijagonali bloka koji čine prvih r vrsta i prvih r kolona, a svi ostali elementi su nule.

Glava 2

O sistemima linearnih Diofantovih jednačina

2.1 Sistemi linearnih jednačina

2.1.1 Osnovni pojmovi

Definicija 2.1.1 *Linearna jednačina sa nepoznatim* $x_1, x_2, \ldots, x_n$ *je jednačina oblika*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \tag{2.1}$$

gde su $a_1, a_2, \ldots, a_n$ *elementi nekog polja* P *koje nazivamo koeficijentima jednačine, a* b *je takođe iz* P *koji nazivamo slobodan član jednačine.*
Ako je $b = 0$ *jednačinu (2.1) nazivamo homogena linearna jednačina.*

Definicija 2.1.2 *Sistem od* m *linearnih jednačina sa* n *nepoznatih* x_1,x_2,. . .,x_n *je sistem*

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m, \end{cases} \tag{2.2}$$

gde su $a_{ij}, b_i (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n)$ *elementi nekog polja* P.
Ako je svaka jednačina sistema (2.2) homogena, sistem nazivamo homogen sistem linearnih jednačina.

Definicija 2.1.3 *Rešenje sistema linearnih jednačina (2.2) je uređena* n*-torka elemenata* $(k_1, k_2, \ldots, k_n)$ *iz* P*, takva da je svaka jednačina sistema zadovoljena za vrednosti* $x_1 = k_1, x_2 = k_2, \ldots, x_n = k_n$*, tj. tačne su sledeće*

jednakosti:

$$\begin{array}{l} a_{11}k_1 + a_{12}k_2 + \ldots + a_{1n}k_n = b_1, \\ a_{21}k_1 + a_{22}k_2 + \ldots + a_{2n}k_n = b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}k_1 + a_{m2}k_2 + \ldots + a_{mn}k_n = b_m. \end{array} \tag{2.3}$$

Svaki homogen sistem linearnih jednačina ima očigledno bar jedno rešenje, to je n-torka $(0, 0, \ldots, 0)$. To rešenje homogenog sistema nazivamo trivijalno. Ostala rešenja, ukoliko postoje, nazivamo netrivijalna.

Definicija 2.1.4 *Sistem linearnih jednačina je saglasan (mogući, konzistentan) ako ima bar jedno rešenje. Ukoliko sistem nema ni jedno rešenje on je protivrečan (kontradiktoran, nemoguć, nesaglasan). Saglasan sistem je određen ako ima jedno i samo jedno rešenje, a neodređen ako ima više od jednog rešenja.*

Definicija 2.1.5 *Dva sistema linearnih jednačina su ekvivalentna ako i samo ako je svako rešenje prvog sistema rešenje i drugog i obrnuto, svako rešenje drugog sistema je rešenje prvog.*
Za svaka dva protivrečna sistema rećićemo da su ekvivalentna.
Dakle, dva sistema linearnih jednačina su ekvivalentna ako i samo ako su im skupovi rešenja jednaki.

Kako se mogu naći sva rešenja sistema linearnih jednačina? Cilj je da polazeći od datog sistema, dođemo do njemu ekvivalentnog sistema jednostavnog oblika čija se rešenja lako uočavaju. To se može postići vršenjem elementarnih transformacija na datom sistemu koje ćemo sada definisati.

Definicija 2.1.6 *Elementarne transformacije sistema linearnih jednačina su sledeće transformacije tog sistema:*

1. *međusobna zamena bilo koje dve jednačine,*
2. *množenje bilo koje jednačine brojem različitim od nule,*
3. *dodavanje jedne jednačine pomnožene bilo kojim brojem nekoj drugoj jednačini.*

Dokazaćemo da elementarne transformacije prevode dati sistem u ekvivalentan sistem.

Teorema 2.1.1 *Vršenjem konačnog broja elementarnih transformacija na sistemu linearnih jednačina (2.2) dobija se sistem ekvivalentan sa datim.*

Dokaz. Očigledno je da se zamenom dve vrste dobijaju ekvivalentni sistemi i da se množenjem jedne jednačine brojem različitim od nule dobija takođe ekvivalentan sistem.
Pretpostavimo, određenosti radi, da je prva jednačina sistema (2.2) pomnožena brojem k i dodata drugoj. Dobija se sistem

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n = b_1, \\ (a_{21}+ka_{11})x_1 + (a_{22}+ka_{12})x_2 + \ldots + (a_{2n}+ka_{1n})x_n = b_2 + kb_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n = b_m. \end{cases} \tag{2.4}$$

Ako je $(k_1, k_2, \ldots, k_n)$ rešenje sistema (2.2), onda su tačne i jednakosti (2.3), pa odatle sledi da su i jednakosti

$$\begin{array}{l} a_{11}k_1 + a_{12}k_2 + \ldots + a_{1n}k_n = b_1, \\ a_{21}k_1 + a_{22}k_2 + \ldots + a_{2n}k_n + k(a_{11}k_1 + \ldots + a_{1n}k_n) = b_2 + kb_1, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}k_1 + a_{m2}k_2 + \ldots + a_{mn}k_n = b_m, \end{array} \tag{2.5}$$

tačne, tj, $(k_1, k_2, \ldots, k_n)$ je rešenje i sistema (2.4).

Obrnuto, ako pretpostavimo da je $(k_1, k_2, \ldots, k_n)$ rešenje i sistema (2.4), tj. da su jednakosti (2.5) tačne, onda dodavanjem prve od tih jednačina pomnožene sa $-k$ drugoj, dobijamo da su tačne i jednakosti (2.3) a to znači da je $(k_1, k_2, \ldots, k_n)$ rešenje i sistema (2.2).

Dakle, sistemi (2.2) i (2.4) su ekvivalentni.

□

Može se desiti da se posle vršenja određenog broja elementarnih transformacija dođe do sistema u kome su u jednoj jednačini svi koeficijenti jednaki nuli. Ako je i slobodan član te jednačine jednak nuli, onda je svaka n-torka brojeva rešenje te jednačine, pa se izostavljajući tu jednačinu dobija sistem ekvivalentan sa polaznim. Ako je slobodan član te jednačine različit od nule, onda ona uopšte nema rešenje pa je dobijeni sistem protivrečan, a takođe i polazni sistem.

2.1.2 Gausov algoritam

Neka je sistem jednačina (S) konjukcija jednačina $J_1, \ldots, J_m$ sa po n promenljivih. U k-tom koraku algoritma ćemo eliminisati po jednu promenljivu iz svih jednačina $k+1, k+2, \ldots, m$, ukoliko je to moguće. Algoritam se završava kada nije moguće eliminisati ni jednu promenljivu ili kada je $k = m$. k-ti korak algoritma se sastoji u sledećem:

1. Pronaći proizvoljan koeficijent različit od nule u nekoj od jednačina $J_k, \ldots, J_m$. Ukoliko takav koeficijent ne postoji, tada se postupak završava. Ukoliko takav koeficijent postoji, neka je to a_{ij} u jednačini J_i gde je $i \geq k$.

2. Promeniti redosled jednačina $J_k, \ldots, J_m$ tako da se na k-tom mestu nalazi jednačina J_i. Promeniti redosled promenljivih $x_j, \ldots, x_n$ tako da je promenljiva x_j k-ta po redu. Ne gubeći na opštosti, promenljivu x_j u nastavku označavamo x_k. Sada se koeficijent a_{ij} nalazi na poziciji kk.

3. Svakoj od jednačina J_i za $k+1 \leq i \leq m$ dodati jednačinu J_k pomnoženu brojem $-a_{kk}^{-1} \cdot a_{ik}$. Tada će koeficijenti na poziciji ik biti

$$a_{ik} - a_{kk}^{-1} \cdot a_{ik} \cdot a_{kk} = 0,$$

   čime smo eliminisali koeficijente uz x_k u jednačinama $J_{k+1}, \ldots, J_m$.

4. Ukoliko je $k = m$, postupak je završen. U suprotnom se k uvećava za 1 i postupak se ponavlja.

Jasno je da se ovaj postupak mora završiti u najviše m koraka. Na osnovu Teoreme 2.1.1 sledi da se svakim korakom dobija sistem ekvivalentan polaznom sistemu. Razmotrićemo karakter rešenja sistema jednačina u zavisnosti od tačke u kojoj je algoritam završio sa radom.

- Ukoliko se postupak završi u koraku 4, tada je polazni sistem ekvivalentan trougaonom sistemu u kome je poslednja jednačina $a_{mm}x_m = b_m$. Množenjem te jednačine sa a_{mm}^{-1} koje postoji jer prema uslovu prvog koraka $a_{mm} \neq 0$, dobijamo $x_m = b_m \cdot a_{mm}^{-1}$. Sada zamenom x_m u jednačini J_{m-1} dobijamo jedinstvenu vrednost za x_{m-1}. Ponavljajući ovaj postupak dolazimo do jedinstvenog rešenja jednačine.

- Ukoliko se postupak završi u prvom koraku, tada su svi koeficijenti a_{ij} za $k \leq i \leq m$ i $k \leq j \leq n$ jednaki nuli. Razlikujemo dve mogućnosti.

  (a) Svi slobodni članovi b_i za $k \leq i \leq m$ su jednaki nuli. Tada će sistem biti zadovoljen za proizvoljne vrednosti promenljivih $x_k, \ldots, x_m$, jer ostale promenljive možemo odrediti tako što zamenimo proizvoljne vrednosti $x_k, \ldots, x_m$ u jednačine $J_1, \ldots, J_{k-1}$ čime se sistem svodi na trougaoni sistem iz prethodnog slučaja 1. Pošto vrednosti $m - k + 1$ promenljivih možemo birati slobodno, kažemo da je sistem neodređen i ima $m - k + 1$ stepeni slobode.

(b) Jedan od slobodnih članova je različit od nule, neka je to član b_i. Kako su leve strane svih jednačina jednake 0, jednakost J_i ne može biti zadovoljena, pa je sistem protivrečan.

2.2 Sistemi linearnih jednačina i matrice

Sistem linearnih jednačina (2.2) se može u matričnom obliku pisati na sledeći način:

$$AX = B,$$

gde je $A = [a_{ij}]$ matrica tipa $m \times n$,

$$X = \begin{bmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{bmatrix}, \quad B = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}$$

Matrica A naziva se matrica sistema (2.2) (ili matrica koeficijenata), a matrica

$$\overline{A} = \begin{bmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{bmatrix}$$

naziva se proširena matrica sistema (2.2).

Sistem (2.2) može se napisati i u sledećem obliku:

$$\begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} x_1 + \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} x_2 + \ldots + \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} x_n = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}.$$

Sledeća teorema daje kriterijum po kome se može utvrditi da li je sistem linearnih jednačina saglasan ili ne.

Teorema 2.2.1 (*Kroneker-Kapelijeva teorema*) *Sistem linearnih jednačina (2.2) je saglasan ako i samo ako je rang matrice sistema jednak rangu proširene matrice sistema.*

Dokaz. ($\Rightarrow$) Pretpostavimo da je sistem (2.2) saglasan i dokažimo da je $rang(A) = rang(\overline{A})$. Pošto je sistem saglasan on ima bar jedno rešenje, tj. postoje elementi $c_1, c_2, \ldots, c_n$ polja P takvi da je

$$\begin{bmatrix} a_{11} \\ a_{21} \\ \vdots \\ a_{m1} \end{bmatrix} c_1 + \begin{bmatrix} a_{12} \\ a_{22} \\ \vdots \\ a_{m2} \end{bmatrix} c_2 + \ldots + \begin{bmatrix} a_{1n} \\ a_{2n} \\ \vdots \\ a_{mn} \end{bmatrix} c_n = \begin{bmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{bmatrix}. \qquad (2.6)$$

Poslednja kolona matrice $\overline{A}$ jednaka je linearnoj kombinaciji njenih prvih n kolona, pa ako prvu kolonu te matrice pomnožimo sa $-c_1$ i dodamo poslednjoj itd., na kraju n-tu kolonu pomnožimo sa $-c_n$ i dodamo poslednjoj koloni, dobićemo matricu

$$C = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} & 0 \\ a_{21} & a_{22} & \ldots & a_{2n} & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} & 0 \end{bmatrix}.$$

Matrica C je dobijena od matrice $\overline{A}$ vršenjem elementarnih transformacija, dakle $rang(C) = rang(\overline{A})$. S obzirom da poslednja kolona matrice C, koja se sastoji samo od nula, ne utiče na maksimalan broj linearno nezavisnih vektora kolona te matrice, tj. na rang matrice C, sledi da je $rang(C) = rang(A)$. Prema tome, $rang(A) = rang(\overline{A})$.
($\Leftarrow$) Pretpostavimo sada da je $rang(A) = rang(\overline{A}) = r$ i dokažimo da je sistem (2.2) saglasan. Dakle, u skupu kolona matrice A postoji r kolona koje čine maksimalan linearno nezavisan skup, a te iste kolone čine i maksimalan linearno nezavisan skup kolona matrice $\overline{A}$ (jer bi u suprotnom dobili da je $rang(\overline{A}) > rang(A)$). Poslednja kolona matrice $\overline{A}$ jednaka je nekoj linearnoj kombinaciji ovih r kolona, a to znači da je poslednja kolona matrice $\overline{A}$ jednaka i linearnoj kombinaciji svih kolona matrice A. Prema tome, postoje skalari $c_1, c_2, \ldots, c_n$ takvi da važi (2.6), pa je $(c_1, c_2, \ldots, c_n)$ jedno rešenje datog sistema, tj. sistem je saglasan.

□

2.3 Pokazivanje egzizstencije rešenja sistema linearnih Diofantovih jednačina računanjem Smitove normalne forme matrice sistema

Osnovno pitanje koje se postavlja u vezi sa sistemima linearnih Diofantovih jednačina je

Da li sistem linearnih Diofantovih jednačina ima rešenje? Ako postoje rešenja, kako ih možemo pronaći? $(*)$

Posmatrajući sistem linearnih jednačina $A\mathbf{x} = \mathbf{b}$, gde je $A = [a_{ij}]$ celobrojna matrica tipa $m \times n$, i $\mathbf{b}$ vektor kolona tipa $m \times 1$ sa celobrojnim komponentama , pitamo se da li sistem ima celobrojno rešenje, tj. da li postoji $n \times 1$ vektor $\mathbf{x}$ sa celobrojnim komponentama?

Teorema 2.3.1 (*van der Waerden*) *Postoji celobrojno rešenje datog sistema ako i samo ako za svaku vektor vrstu* $\mathbf{v}$ *sa racionalnim komponentama tako da* $\mathbf{v}A$ *ima celobrojne komponente,* $\mathbf{vb}$ *je ceo broj.*

Označimo sa $M_{m,n}(G)$ skup svih matrica tipa $m \times n$ sa elementima iz domena glavnih ideala G, a sa $M_k(G)$ označavamo skup svih kvadratnih matrica tipa $k \times k$ sa elementima iz G. Za dve matrice $A, B \in M_{m,n}(G)$ kažemo da su ekvivalentne ako postoje invertibilne matrice $P \in M_m(G)$ i $Q \in M_n(G)$, takve da je $B = PAQ$. Sada ćemo posmatrati problem pronalaženja matrice specijalnog oblika ekvivalentne sa matricom A.

Teorema 2.3.2 *Ako* $A \in M_{m,n}(G)$*,* G *je domen glavnih ideala, onda je matrica* A *ekvivalentna matrici oblika*

$$diag\{d_1, d_2, \ldots, d_r, 0, \ldots, 0\}$$

$$\equiv \begin{bmatrix} d_1 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_2 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & d_r & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{bmatrix} \tag{2.7}$$

gde $d_i \neq 0$ *i* $d_i | d_j$ *ako* $i \leq j$*.*

Matrice P i Q pomoću kojih transformišemo matricu A u matricu oblika (2.7) dobićemo kao proizvode matrica nekih posebnih oblika koje ćemo sada definisati. Uvodimo prvo određene invertibilne (kvadratne) matrice sa elementima iz G tipa $m \times m$ ili $n \times n$, koje ćemo zvati elementarnim, i posmatraćemo posledice levih i desnih množenja matrice A ovim matricama. U nastavku će postati jasno koje dimenzije matrica uzimamo. Označimo sa 1 jediničnu matricu.

Prvo, neka $b \in G$ i neka je $i \neq j$. Neka je $T_{ij}(b) = 1 + be_{ij}$ gde je e_{ij} matrica sa svim nulama osim na poziciji (i, j) gde je 1. T_{ij} je invertibilna matrica jer je

$$T_{ij}(b)T_{ij}(-b) = (1 + be_{ij})(1 - be_{ij}) = 1$$

Sledeće, neka je u invertibilan element iz G i neka je $D_i(u) = 1+(u-1)e_{ii}$. $D_i(u)$ je dijagonalna matrica sa u na poziciji (i, i) dok su ostali dijagonalni elementi 1. Onda je $D_i(u)$ invertibilna sa $D_i(u)^{-1} = D_i(u^{-1})$. Konačno, neka je $P_{ij} = 1 - e_{ii} - e_{jj} + e_{ij} + e_{ji}$. I ova matrica je invertibilna jer je $P_{ij}^2 = 1$.

Lako se proverava da

I Levo množenje matrice A sa $m \times m$ matricom $T_{ij}(b)$ daje matricu čija je i-ta vrsta dobijena tako što se j-ta vrsta matrice A pomnoži sa b i doda i-toj vrsti matrice A, dok su ostale vrste identične kao u matrici A.
Desno množenje matrice A sa $n \times n$ matricom $T_{ij}(b)$ daje matricu čija je j-ta kolona dobijena tako što se i-ta kolona matrice A pomnoži sa b i doda j-toj koloni matrice A, dok su ostale kolone identične kao u matrici A.

II Levo množenje matrice A sa $m \times m$ matricom $D_i(u)$ predstavlja množenje i-te vrste matrice A sa u, ostavljajući ostale vrste kao u A.
Desno množenje matrice A sa $n \times n$ matricom $D_i(u)$ predstavlja množenje i-te kolone matrice A sa u, ostavljajući ostale kolone kao u A.

III Levo množenje matrice A sa $m \times m$ matricom P_{ij} menja mesta i-toj i j-toj vrsti matrice A, ostavljajući ostale vrste kao u A.
Desno množenje matrice A sa $n \times n$ matricom P_{ij} menja mesta i-toj i j-toj koloni matrice A, ostavljajući ostale kolone kao u A.

Nazvaćemo matrice $T_{ij}(b)$, $D_i(u)$, P_{ij} elementarnim matricama tipa I, II i III, redom. Levo (desno) množenje matrice A sa jednom od ovih matrica zvaćemo elementarnom transformacijom vrsta (kolona) odgovarajućeg tipa. Takve elementarne transformacije daju matrice ekvivalentne matrici A.

Dokaz Teoreme 2.3.2. Prvo ćemo dokazati specijalan slučaj kada je G Euklidov domen sa funkcijom δ iz G u skup $\mathbb{N}$ (Definicija 1.1.10). Ako je $A = 0$, onda je dokaz završen. Inače, neka je a_{ij} nenula element matrice A tako da je $\delta(a_{ij})$ minimalno. Elementarnim transformacijama vrsta i kolona ovaj element dovodimo na poziciju $(1, 1)$. Neka je $k > 1$ i $a_{1k} = a_{11}b_k + b_{1k}$, gde $\delta(b_{1k}) < \delta(a_{11})$. Sada oduzmimo prvu kolonu pomnoženu sa b_k od k-te. Ova elementarna transformacija menja element a_{1k} sa b_{1k}. Ako je $b_{1k} \neq 0$ dobijamo matricu ekvivalentnu matrici A za koju je minimum

funkcije δ za nenula elemente manji od minimuma u matrici A. Ponovimo ovaj postupak za novu matricu. Slično, ako je $a_{k1} = a_{11}b_k + b_{k1}$, gde $b_{k1} \neq 0$ i $\delta(b_{k1}) < \delta(a_{11})$, onda elementarnom transformacijom tipa I na vrste dobijamo ekvivalentnu matricu za koju je minimum funkcije δ za nenula elemente smanjen. Pošto je "stepen" funkcije δ nenegativan ceo broj, konačan broj koraka ovog postupka daje ekvivalentnu matricu $B = [b_{ij}]$ takvu da $b_{11}|b_{1k}$ i $b_{11}|b_{k1}$ za svako k. Zatim, elementarnom transformacijom na vrstama i kolonama tipa I dobijamo ekvivalentnu matricu oblika

$$\begin{bmatrix} b_{11} & 0 & \dots & 0 \\ 0 & c_{22} & \dots & c_{2n} \\ \dots & \dots & \dots & \dots \\ 0 & c_{m2} & \dots & c_{mn} \end{bmatrix} \tag{2.8}$$

Možemo napraviti da $b_{11}|c_{kl}$ za svako k, l. Jer ako $b_{11} \nmid c_{kl}$ onda možemo dodati k-tu vrstu prvoj i dobiti novu prvu vrstu $(b_{11}, c_{k2}, \dots, c_{kl}, \dots, c_{kn})$. Ponavljanjem prvog postupka c_{kl} menjamo za nenula element za koji funkcija δ ima manju vrednost nego za b_{11}. Konačan broj koraka navedenog postupka daje matricu (2.8) ekvivalentnu matrici A u kojoj je $b_{11} \neq 0$ i $b_{11}|c_{kl}$ za svako k, l. Sada ponovimo postupak na podmatricu $[c_{kl}]$. Dobijamo ekvivalentnu matricu oblika

$$\begin{bmatrix} b_{11} & 0 & 0 & \dots & 0 \\ 0 & c_{22} & 0 & \dots & 0 \\ 0 & 0 & d_{33} & \dots & d_{3n} \\ \dots & \dots & \dots & \dots & \\ 0 & 0 & d_{m3} & \dots & d_{mn} \end{bmatrix} \tag{2.9}$$

za koju $c_{22} \nmid d_{pq}$ za svako p, q. Štaviše, elementarne transformacije kolona i vrsta podmatrice $[c_{kl}]$ koje daju matricu (2.9) ne utiču na uslov deljivosti elementom b_{11}. Dakle, $b_{11}|c_{22}$ i $b_{11}|d_{pq}$. Ponavljajući ovaj postupak dobijamo ekvivalentnu dijagonalnu matricu $diag\{d_1, d_2, \dots, d_r, 0, \dots, 0\}$ gde $d_i|d_j$ za $i \leq j$ ($d_1 = b_{11}, d_2 = c_{22}$, itd.).

Dokaz u opštem slučaju je sličan prethodnom. Ovde koristimo indukciju po dužini nenula elementa $a \in G$ u $\delta(a)$. Definišemo dužinu elementa $a \neq 0$, $l(a)$, kao broj prostih faktora u njegovoj faktorizaciji $a = p_1 p_2 \cdots p_r$, p_i su prosti brojevi , $i \in \{1, \dots, r\}$. Uzimamo da je $l(u) = 0$ ako je u jedinica. Pored elementarnih transformacija koje su bile dovoljne u slučaju kada je G

bio Euklidov domen potrebno je da koristimo i množenje matricama oblika

$$\begin{bmatrix} x & s & & & & \\ y & t & & & 0 & \\ & & 1 & & & \\ & & & 1 & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{bmatrix} \tag{2.10}$$

gde je $\begin{bmatrix} x & s \\ y & t \end{bmatrix}$ invertibilna matrica. Kao u prethodnom slučaju možemo pretpostaviti da je $a_{11} \neq 0$ i $l(a_{11}) \leq l(a_{ij})$ za svako $a_{ij} \neq 0$. Pretpostavimo $a_{11} \nmid a_{1k}$. Menjanjem mesta drugoj i k-toj koloni možemo pretpostaviti $a_{11} \nmid a_{12}$. Neka je $a = a_{11}, b = a_{12}$ i $d = NZD(a,b)$ tako da je $l(d) < l(a)$. Postoje elementi $x, y \in G$ takvi da $ax+by = d$. Neka je $s = bd^{-1}$, $t = -ad^{-1}$. Onda iz matrične jednakosti

$$\begin{bmatrix} -t & s \\ y & -x \end{bmatrix} \begin{bmatrix} x & s \\ y & t \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$$

sledi da su obe matrice invertibilne (pošto je G komutativan). Onda je i (2.10) invertibilna, pa desnim množenjem matrice A ovom matricom dobijamo matricu čija je prva vrsta $(d, 0, a_{13}, \ldots, a_{1n})$ i $l(d) < l(a_{11})$. Slično, ako $a_{11} \nmid a_{k1}$ za neko k, elementarnim transformacijama zajedno sa levim množenjem matricom (2.10) dobijamo ekvivalentnu matricu u kojoj je dužina nekog nenula elementa manja od $l(a_{11})$. Na ovaj način možemo dobiti da $a_{11}|a_{1k}$ i $a_{11}|a_{k1}$ za svako k. Elementarnim transformacijama dobijamo matricu oblika (2.8). Ostatak dokaza je u suštini isti kao za Euklidov domen. Jedina razlika je da nastavljamo da smanjujemo dužinu umesto stepen funkcije δ.

□

Dijagonalna matrica iz Teoreme 2.3.2 je jedinstveno određena i nazivamo je Smitova normalna forma matrice A.

Označimo sa $M_{m,n}(\mathbb{Z})$, $1 \leq m \leq n$, prsten svih celobrojnih matrica tipa $m \times n$, a sa $SL_k(\mathbb{Z})$ skup invertibilnih celobrojnih kvadratnih matrica tipa $k \times k$. Onda prethodnu teoremu možemo zapisati i u sledećoj verziji:

Teorema 2.3.3 *Neka $A \in M_{m,n}(\mathbb{Z})$. Postoje $P \in SL_m(\mathbb{Z})$ i $Q \in SL_n(\mathbb{Z})$ takve da*

$$PAQ = D = diag\{d_1, d_2, \ldots, d_r, 0, \ldots, 0\},$$

gde $d_i > 0$, $i = 1, \ldots, r$, i $d_i | d_{i+1}$ za $i = 1, \ldots, r-1$.

Matrice P i Q odgovaraju kompozicijama elementarnih transformacija na vrstama i kolonama matrice A, redom.

Napomenimo da Teoremu 2.3.3 možemo iskoristiti da bismo odgovorili na pitanje $(*)$. Sistem linearnih jednačina $A\mathbf{x} = \mathbf{b}$ zapišimo kao $D\mathbf{y} = \mathbf{c}$, gde je $Q\mathbf{y} = \mathbf{x}$, $PAQ = D$ i $P\mathbf{b} = \mathbf{c}$. Rešenje dijagonalnog sistema $D\mathbf{y} = \mathbf{c}$ se lako određuje.

Pitanje pronalaska odgovarajućeg algoritma za računanje Smitove normalne forme za celobrojnu matricu nije trivijalno i postoje razni algoritmi za njeno računanje. Za više detalja, videti [1] i [13].

Teorema 2.3.2 ima interesantnu istoriju. Pitanje $(*)$ nije bilo u potpunosti postavljeno sve do sredine 19-tog veka. Neki posebni slučajevi su se pojavili 1849-1850. godine u Hermitovim istraživanjima u teoriji brojeva [20]. Heger je formulisao uslove rešivosti sistema $A\mathbf{x} = \mathbf{b}$ u slučaju kada je matrica A punog ranga nad $\mathbb{Z}$. 1861. godine ovaj problem je u potpunosti rešio Smit (Henry John Stephen Smith) [16]. Teorema 2.3.2 se pojavila u sličnom obliku kao gore navedenom 1868. godine u jednoj raspravi Frobeniusa [4], koji je uopštio Hegerov problem i istakao unimodularnost transformacija.

Do tada su bili otkriveni mnogi rezultati iz oblasti abelovih grupa. Gaus je predstavio ideju o abelovoj grupi koja se razvila zajedno sa studijama Gausa, Šeringa, Kronekera i Dirihlea iz oblasti teorije brojeva, i studijama Gausa, Abela i Jakobija o eliptičnim funkcijama. 1879. godine Frobenius i Stickelberger [5] su otkrili i koristili vezu između teorije konačno generisanih abelovih grupa i Smitove teoreme. Iste godine, Frobenius pokazuje da Smitova teorija može biti korištena za klasifikaciju kvadratnih matrica nad poljima, do na sličnosti. Priča nas podseća da su mnogi osnovni pojmovi i činjenice iz linearne algebre bili otkriveni u kontekstu teorije brojeva.

Sada ćemo dokazati teoremu koja sadrži i dokaz Teoreme 2.3.1.

Teorema 2.3.4 *Neka su A, P, Q, D definisani kao u Teoremi 2.3.3, $\mathbf{b} \in \mathbb{Z}^n$ i $\mathbf{c} = P\mathbf{b}$. Tada su sledeći uslovi ekvivalentni:*

(1) Sistem linearnih jednačina $A\mathbf{x} = \mathbf{b}$ ima celobrojno rešenje

(2) Sistem linearnih jednačina $D\mathbf{y} = \mathbf{c}$ ima celobrojno rešenje

(3) Za svaki racionalan vektor $\mathbf{u}$ takav da je $\mathbf{u}A$ celobrojni vektor, $\mathbf{ub}$ je ceo broj

(4) Za svaki racionalan vektor $\mathbf{v}$ takav da je $\mathbf{v}D$ celobrojni vektor, $\mathbf{vc}$ je ceo broj.

Dokaz. (1) $\Leftrightarrow$ (2): $A\mathbf{x} = \mathbf{b} \Leftrightarrow (P^{-1}DQ^{-1})\mathbf{x} = \mathbf{b} \Leftrightarrow D(Q^{-1}\mathbf{x}) = \mathbf{c} \Leftrightarrow D\mathbf{y} = \mathbf{c}$, gde je $\mathbf{y} = Q^{-1}\mathbf{x}$ i $\mathbf{c} = P\mathbf{x}$. Pošto $Q \in SL_m(\mathbb{Z})$, onda i

$Q^{-1} \in SL_m(\mathbb{Z})$. Dakle, $\mathbf{x} \in \mathbb{Z}^n \Leftrightarrow \mathbf{y} = Q^{-1}\mathbf{x} \in \mathbb{Z}^n$.

(3) $\Leftrightarrow$ (4): $\mathbf{v}D \in \mathbb{Z}^n \Leftrightarrow \mathbf{v}(PAQ) \in \mathbb{Z}^n \Leftrightarrow (\mathbf{v}P)A \in \mathbb{Z}^n Q^{-1} = \mathbb{Z}^n \Leftrightarrow \mathbf{u}A \in \mathbb{Z}^n$, gde je $\mathbf{u} = \mathbf{v}P$. $P \in SL_n(\mathbb{Z})$, onda $\mathbf{u} \in \mathbb{Q}^m \Leftrightarrow \mathbf{v} \in \mathbb{Q}^m$, i, zbog (3), $\mathbf{ub} \in \mathbb{Z}$. Ali $\mathbf{ub} \in \mathbb{Z} \Leftrightarrow (\mathbf{v}P)(P^{-1}\mathbf{c}) \in \mathbb{Z} \Leftrightarrow \mathbf{vc} \in \mathbb{Z}$. Dakle, (3) implicira (4). Obrnuto, $\mathbf{u}A \in \mathbb{Z}^n \Leftrightarrow \mathbf{v}D \in \mathbb{Z}^n$ i $\mathbf{vc} \in \mathbb{Z} \Leftrightarrow \mathbf{ub} \in \mathbb{Z}$. Dakle, (4) implicira (3).

(2) $\Leftrightarrow$ (4): $D\mathbf{y} = \mathbf{c}$ implicira $\mathbf{v}(D\mathbf{y}) = \mathbf{vc}$ za svaki vektor $\mathbf{v} \in \mathbb{Q}^m$, odakle je $(\mathbf{v}D)\mathbf{y} = \mathbf{vc}$. Ako $\mathbf{v}D \in \mathbb{Z}^n$, onda $\mathbf{vc} \in \mathbb{Z}$. Dakle, (2) implicira (4). Da bismo dokazali da (4) implicira (2), prvo zapažamo da je $\mathbf{c} = (c_1, \ldots, c_r, 0, \ldots, 0)$. Pretpostavimo suprotno, $c_j \neq 0$, $j > r$. Posmatrajmo vektor $\mathbf{v} = (0, \ldots, 0, 1/(2c_j), 0, \ldots, 0)$, gde se $1/(2c_j)$ nalazi na j-toj poziciji. Pošto je $\mathbf{v}D = \mathbf{0} \in \mathbb{Z}^n$, onda zbog (4) $\mathbf{vc} = 1/2 \in \mathbb{Z}$, kontradikcija. Dakle, $c_j = 0$ za $j > r$. Sledeće, za $i = 1, \ldots, r$, posmatrajmo vektore $\mathbf{v_i} = (0, \ldots, 0, 1/d_i, 0, \ldots, 0)$. Kako $\mathbf{v_i}D \in \mathbb{Z}^n$, onda zbog (4), $\mathbf{v_i c} \in \mathbb{Z}$ i stoga $c_i/d_i \in \mathbb{Z}$. Neka je $\mathbf{y} = (y_1, \ldots, y_r, 0, \ldots, 0)$, gde $y_i = c_i/d_i$, $i = 1, \ldots, r$. Onda $\mathbf{y} \in \mathbb{Z}^n$, i $D\mathbf{y} = \mathbf{c}$.

□

Sa notacijom u Teoremi 2.3.4, umesto rešenja sistema $A\mathbf{x} = \mathbf{b}$ možemo tražiti rešenje sistema $D\mathbf{y} = \mathbf{c}$ primenom elementarnih transformacija (nad $\mathbb{Z}$) vrsta i kolona matrice A. Matrice P i Q možemo dobiti množenjem matricama koje odgovaraju ovim transformacijama. Sistem $D\mathbf{y} = \mathbf{c}$ ima rešenje ako i samo ako $c_{r+1} = \ldots = c_m = 0$, i $d_i | c_i$ za $i = 1, \ldots, r$. Opšte rešenje sistema $D\mathbf{y} = \mathbf{c}$ možemo zapisati u obliku $\mathbf{y} = (y_1, \ldots, y_r, t_1, \ldots, t_{m-r})$, gde $y_i = c_i/d_i$, $i = 1, \ldots, r$, i $t_1, \ldots, t_{m-r}$ su proizvoljni celobrojni parametri. Onda je opšte rešenje sistema $A\mathbf{x} = \mathbf{b}$ samo $Q\mathbf{y}$.

Teorema 2.3.5 *Neka $A \in M_{m,n}(\mathbb{Z})$, i $\mathbf{b} \in \mathbb{Z}^n$. Onda sistem linearnih jednačina $A\mathbf{x} = \mathbf{b}$ ima celobrojno rešenje ako i samo ako odgovarajući sistem kongruencija $A\mathbf{x} \equiv \mathbf{b} \pmod n$ ima rešenje za svaki pozitivan ceo broj n.*

Dokaz. Očigledno, prvi iskaz implicira drugi. Pretpostavimo sada da sistem kongruencija $A\mathbf{x} \equiv \mathbf{b} \pmod n$ ima rešenje za svaki pozitivan ceo broj n. Neka su P, Q, D, $\mathbf{y}$ i $\mathbf{c}$ definisani kao u Teoremi 2.3.4, i neka je $N \in \mathbb{Z}$ takav da promena iz $A\mathbf{x} = \mathbf{b}$ u $D\mathbf{y} = \mathbf{c}$ koristi cele brojeve čije su apsolutne vrednosti manje od N. Onda za svako $n \geq N$, $A\mathbf{x} \equiv \mathbf{b} \pmod n \Leftrightarrow D\mathbf{y} \equiv \mathbf{c} \pmod n \Leftrightarrow d_i y_i \equiv c_i \pmod n$, $i = 1, \ldots, r$. Poslednji sistem kongruencija je rešiv u slučaju kada je n umnožak od d_r. Pošto $d_i | d_r$ za svako i, $1 \leq i \leq r$, ovo implicira $d_i | (d_i y_i - c_i)$, pa $d_i | c_i$ za svako $i = 1, \ldots, r$. Dakle, $D\mathbf{y} = \mathbf{c}$ ima celobrojno rešenje, onda i $A\mathbf{x} = \mathbf{b}$ ima celobrojno rešenje.

□

Primer 2.3.1 Rešiti sistem linearnih Diofantovih jednačina $A\mathbf{x} = \mathbf{b}$, gde je

$$A = \begin{bmatrix} 3 & 1 & 5 \\ -6 & 3 & 4 \end{bmatrix},\ \mathbf{x} = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix},\ \mathbf{b} = \begin{bmatrix} 12 \\ -7 \end{bmatrix}.$$

U cilju istovremenog određivanja invertibilnih matrica P i Q, tako da je $PAQ = D$, stavimo kao početne vrednosti

$$P = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix},\ Q = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

i sve transformacije nad vrstama ponovimo na tekućoj matrici P, dok sve transformacije nad kolonama ponovimo na tekućoj matrici Q. Kada matrica A bude dovedena na Smitov oblik ($PAQ = D$) matrice P i Q dobiće svoju pravu vrednost.

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 3 & 1 & 5 \\ -6 & 3 & 4 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 3 & 5 \\ 3 & -6 & 4 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \sim$$

$$\begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 3 & -15 & -11 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & -3 & -5 \\ 0 & 0 & 1 \end{bmatrix} \sim$$

$$\sim \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & -15 & -11 \end{bmatrix}\begin{bmatrix} 0 & 1 & 0 \\ 1 & -3 & -5 \\ 0 & 0 & 1 \end{bmatrix} \sim$$

$$\sim \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & -15 & 4 \end{bmatrix}\begin{bmatrix} 0 & 1 & -1 \\ 1 & -3 & -2 \\ 0 & 0 & 1 \end{bmatrix} \sim$$

$$\sim \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 4 \end{bmatrix}\begin{bmatrix} 0 & -3 & -1 \\ 1 & -11 & -2 \\ 0 & 4 & 1 \end{bmatrix} \sim$$

$$\sim \underbrace{\begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix}}_{P}\underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}}_{D}\underbrace{\begin{bmatrix} 0 & -3 & 11 \\ 1 & -11 & 42 \\ 0 & 4 & -15 \end{bmatrix}}_{Q}$$

$$\mathbf{c} = P\mathbf{b} = \begin{bmatrix} 1 & 0 \\ -3 & 1 \end{bmatrix} \begin{bmatrix} 12 \\ -7 \end{bmatrix} = \begin{bmatrix} 12 \\ -43 \end{bmatrix}$$

Rešavajući jednačinu $D\mathbf{y} = \mathbf{c}$, dobijamo $\mathbf{y} = (12, -43, t)^T$, gde $t \in \mathbb{Z}$. Konačno,

$$\mathbf{x} = Q\mathbf{y} = \begin{bmatrix} 129 + 11t \\ 485 + 42t \\ -172 - 15t \end{bmatrix}, t \in \mathbb{Z}.$$

Glava 3

Pokazivanje nepostojanja rešenja sistema linearnih Diofantovih jednačina pomoću testera

3.1 Uvod

U ovoj glavi bavimo se metodom koji pruža direktan dokaz da ne postoji rešenje za neke familije sistema linearnih Diofantovih jednačina sa istim zavisnim a različitim nezavisnim promenljivama. U poređenju sa drugim metodama koje se koriste za rešavanje ovih sistema, ovaj metod pruža jednostavniji način pokazivanja nerešivosti ovih sistema. Definisaćemo testere, linearne funkcije, pomoću kojih dolazimo do zaključaka da određeni sistemi linearnih jednačina nemaju rešenja. Pokazaćemo metod za pronalaženje ovakvih funkcija i primenićemo na neke primere.

3.2 Sistemi linearnih Diofantovih jednačina

Problem sa kojim se susrećemo definišemo ih kao traženje celobrojnih vrednosti $x_1, \ldots, x_M$ koje ispunjavaju skup linearnih jednačina, kao što sledi:

$$\begin{aligned}
a_{11}x_1 + a_{12}x_2 + \ldots + a_{1M}x_M &= y_1,\\
a_{21}x_1 + a_{22}x_2 + \ldots + a_{2M}x_M &= y_2,\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NM}x_n &= y_N,
\end{aligned}$$

gde su a_{ij} i y_j celi brojevi, koje redom nazivamo zavisnim i nezavisnim promenljivama jednačina.

Problem možemo izraziti preko matrica, kao pronalaženje $x_1, x_2, \ldots, x_M \in \mathbb{Z}$ tako da

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1M} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NM} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_M \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_N \end{bmatrix}. \tag{3.1}$$

Označićemo sa M broj nepoznatih, a sa N broj jednačina. Dodeljivanjem različitih vrednosti nezavisnim promenljivama, dobijaju se različiti sistemi. Označićemo sa K broj takvih sistema. Fokusiraćemo se na problem utvrđivanja da li postoje celobrojne vrednosti koje su rešenje jednog od tih sistema. Koristeći matrice, poslednji problem uključuje pronalaženje $x_1, x_2, \ldots, x_M \in \mathbb{Z}$ takvih da

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1M} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NM} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_M \end{bmatrix} \in \left\{ \begin{bmatrix} y_{11} \\ \vdots \\ y_{N1} \end{bmatrix}, \ldots, \begin{bmatrix} y_{1K} \\ \vdots \\ y_{NK} \end{bmatrix} \right\} \tag{3.2}$$

gde $\forall a_{ij} \in \mathbb{Z}$ i $\forall y_{ij} \in \mathbb{Z}$.

U izrazu (3.2) $N \times M$ matricu sa zavisnim promenljivama označićemo sa A:

$$A = \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1M} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NM} \end{bmatrix}$$

gde $\forall a_{ij} \in \mathbb{Z}$, a

$$Y = \{(y_{11}, \ldots, y_{N1}), \ldots, (y_{1K}, \ldots, y_{NK})\}, \text{gde } y_{ij} \in \mathbb{Z}.$$

Kažemo da (3.2) ima rešenje koje odgovara $(y_1, \ldots, y_N) \in Y$, ako postoje $x_1, x_2, \ldots, x_M \in \mathbb{Z}$ tako da važi (3.1).

3.3 Testeri

Da bismo utvrdili da ne postoji rešenje za problem (3.2), koristićemo tehniku koja se zasniva na testerima, čiju ćemo definiciju sada dati.

Definicija 3.3.1 (*Tester*) *Neka je R prsten $\mathbb{Q}$ ili $\mathbb{Z}_n$ (gde $n \in \mathbb{N}$).*
Funkcija $f : \mathbb{Z}^N \to R$ je tester nad R sistema jednačina (3.2) akko ispunjava sledeće uslove:

- $\forall k, z_1, \ldots, z_N \in \mathbb{Z}\ f(kz_1, \ldots, kz_N) = kf(z_1, \ldots, z_N)$

- $\forall z_1, \ldots, z_N, \omega_1, \ldots, \omega_N \in \mathbb{Z}\ f(z_1 + \omega_1, \ldots, z_N + \omega_N) = f(z_1, \ldots, z_N) + f(\omega_1, \ldots, \omega_N)$
- $f(a_{11}, \ldots, a_{N1}) = 0, \ldots, f(a_{1M}, \ldots, a_{NM}) = 0$

Značaj testera leži u činjenici da obezbeđuju jednostavan način određivanja da li sistem jednačina (3.2) ima rešenje koje odgovara $(y_1, \ldots, y_N) \in Y$.

Teorema 3.3.1 *Neka je f tester nad prstenom $\mathbb{Q}$ ili $\mathbb{Z}_n$. Ako postoje $x_1, x_2, \ldots, x_M \in \mathbb{Z}$ takvi da*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1M}x_M &= y_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2M}x_M &= y_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots & \\ a_{N1}x_1 + a_{N2}x_2 + \ldots + a_{NM}x_n &= y_N, \end{aligned}$$

onda

$$f(y_1, \ldots, y_N) = 0.$$

Dokaz. $f(y_1, \ldots, y_N) = f(a_{11}x_1 + \ldots + a_{1M}x_M, \ldots, a_{N1}x_1 + \ldots + a_{NM}x_M) = f(a_{11}x_1, a_{21}x_1, \ldots, a_{N1}x_1) + \ldots + f(a_{1M}x_M, \ldots, a_{NM}x_M) = x_1 f(a_{11}, \ldots, a_{N1}) + \ldots + x_M f(a_{1M}, \ldots, a_{NM}) = 0.$

□

Definicija 3.3.2 *Element $(y_1, \ldots, y_N) \in Y$ je nekompaktibilan sa testerom f akko $f(y_1, \ldots, y_N) \neq 0$.*

Prema prethodnoj teoremi, kada je element u Y nekompaktibilan sa testerom, onda ovaj element može biti uklonjen iz skupa Y. U slučaju da ne postoji nijedan element u skupu Y, onda ne postoji ni rešenje za sistem (3.2). U cilju dokazivanja nepostojanja rešenja za sistem (3.2), pokušaćemo pronaći testere pomoću kojih ćemo ukloniti sve elemente skupa Y. To znači da nas ne interesuju testeri koji su kompaktibilni sa svim elementima skupa Y.

Definicija 3.3.3 (*Beskoristan tester*) *Tester f je beskoristan akko za svako $(y_1, \ldots, y_N) \in Y$ $f(y_1, \ldots, y_N) = 0$.*
Kažemo da je tester f koristan akko nije beskoristan.

Sada se postavlja pitanje kako pronaći testere. Uvodimo sledeće oznake:

- W - skup testera definisanih nad prstenom $\mathbb{Q}$
- W_n - skup testera definisanih nad prstenom $\mathbb{Z}_n$

Svaki tester u W je preslikavanje oblika

$$f(z_1, \ldots, z_N) = z_1\alpha_1 + \ldots + z_N\alpha_N.$$

Zapravo, u nastavku ćemo testere u $\mathbb{Q}$ obeležavati kao uređenu N-torku $(\alpha_1, \ldots, \alpha_N)$, gde $\alpha_i \in \mathbb{Q}$.

Na isti način, svaki tester u W_n je preslikavanje oblika

$$f(z_1, \ldots, z_N) = z_1\alpha_1 + \ldots + z_N\alpha_N \bmod n.$$

U nastavku ćemo testere u $\mathbb{Z}_n$ obeležavati kao uređenu N-torku $(\alpha_1, \ldots, \alpha_N)$, gde $\alpha_i \in \mathbb{Z}_n$.

Teorema 3.3.2 *Skup W (zajedno sa uobičajenim operacijama $+$ i $\cdot$ definisanim na funkcijama) je konačno dimenzionalni vektorski prostor nad poljem $\mathbb{Q}$. Na isti način, ako je p prost broj, skup W_p (zajedno sa uobičajenim operacijama $+$ i $\cdot$ definisanim na funkcijama) je konačno dimenzionalni vektorski prostor nad poljem $\mathbb{Z}_p$.*

Dokaz. $(W, +)$ je komutativna grupa. Zaista, sabiranje elemenata iz W je unutrašnja operacija u W, asocijativna i komutativna (osobine slede iz odgovarajućih osobina racionalnih brojeva), neutralni element je tester $(0, 0, \ldots, 0)$, a za svaki element $(\alpha_1, \ldots, \alpha_N)$ iz W, $(-\alpha_1, \ldots, -\alpha_N)$ je suprotni element u odnosu na operaciju $+$. Da važe i osobine $1 - 4$ iz definicije vektorskog prostora jednostavno se pokazuje na osnovu odgovarajućih osobina racionalnih brojeva.
Na isti način se pokazuje i za W_p.

□

3.4 Nalaženje korisnih testera

U ovom delu upoznaćemo se sa metodom pronalaženja testera nad $\mathbb{Q}$ i $\mathbb{Z}_p$ (gde je p prost broj). Prvo ćemo se upoznati sa nekim specijalnim testerima (trivijalni tester i tester izveden iz W).

Definicija 3.4.1 (*trivijalni tester*) *Trivijalni tester nad $\mathbb{Q}$ ili nad $\mathbb{Z}_p$ (gde je p prost broj) je tester takav da važi*

$$\forall z_1, \ldots, z_N \in \mathbb{Z}\ f(z_1, \ldots, z_N) = 0$$

Ovaj tester je generisan vektorom $(0, \ldots, 0)$.

Definicija 3.4.2 (*Tester izveden iz W*) *Tester* $(\alpha_1, \ldots, \alpha_N) \in W_p$ *je izveden iz testera* $f \equiv (\beta_1, \ldots, \beta_N) \in W \cap \mathbb{Z}^N$ (*tj.* $f \in W$ *i* $\forall \beta_i \in \mathbb{Z}$) *akko*

$$\forall i \in \{1, \ldots, N\}\ \alpha_i = (\beta_i \bmod p).$$

Koristićemo oznaku $(f \bmod p)$ *da označimo* $(\alpha_1, \ldots, \alpha_N) \in W_p$.

Sledeća teorema daje karakterizaciju beskorisnih testera nad $\mathbb{Q}$ i nad $\mathbb{Z}_p$ (gde je p prost broj).

Teorema 3.4.1 *Važi sledeće:*

(i) *Trivijalni tester nad* $\mathbb{Q}$ *i nad* $\mathbb{Z}_p$ (*gde je p prost broj*) *je beskoristan.*

(ii) *Skup beskorisnih testera u* W (W_p) *je vektorski potprostor vektorskog prostora* W (W_p).

(iii) *Ako je* $f \in W \cap \mathbb{Z}^N$ *beskoristan tester, onda je i* $(f \bmod p) \in W_p$ *takođe beskoristan tester.*

Dokaz. Očigledno je da važi (i), a važi i (iii) zbog osobina kongruencija. Sada ćemo proveriti (ii). Ako označimo sa W_b skup beskorisnih testera iz skupa W, iz Teoreme 1.4.2 sledi da je dovoljno pokazati da za svako $f, g \in W_b$ i za svako $k \in \mathbb{Q}$ $f + g \in W_b$ i $kf \in W_b$. Neka su $(\alpha_1, \ldots, \alpha_N)$ i $(\beta_1, \ldots, \beta_N)$ generatori testera f i g redom, gde $\alpha_i, \beta_i \in \mathbb{Q}, \forall i = 1, \ldots, N$. Kako $f, g \in W_b$ to znači da za svako $(y_1, \ldots, y_N) \in Y$ $f(y_1, \ldots, y_N) = 0$ i $g(y_1, \ldots, y_N) = 0$, tj. $y_1\alpha_1 + \ldots + y_N\alpha_N = 0$ i $y_1\beta_1 + \ldots + y_N\beta_N = 0$. Sada važi $(f+g)(y_1, \ldots, y_N) = y_1(\alpha_1 + \beta_1) + \ldots + y_N(\alpha_N + \beta_N) = y_1\alpha_1 + \ldots + y_N\alpha_N + y_1\beta_1 + \ldots + y_N\beta_N = 0 + 0 = 0$.
Sada ćemo pokazati da $kf \in W_b$, tj. za svako $(y_1, \ldots, y_N) \in Y$ važi $(kf)(y_1, \ldots, y_N) = 0$. Kako je $(kf)(y_1, \ldots, y_N) = y_1k\alpha_1 + \ldots + y_Nk\alpha_N = k(y_1\alpha_1 + \ldots + y_N\alpha_N) = k \cdot 0 = 0$, sledi da je W_b vektorski potprostor vektorskog prostora W.
Analogno se pokazuje za skup W_p.

□

Kako nas interesuju samo testeri koji uklanjaju bar jedan element skupa Y, nećemo se baviti trivijalnim i testerima izvedenim iz W_p.

Sada ćemo proučavati vezu između vektorskih prostora W i W_p. Kako bismo pojednostavili sledeće korake, uvešćemo sledeću notaciju.

Definicija 3.4.3 *Neka je $B = [b_{ij}]$, $b_{ij} \in \mathbb{Z}$ proizvoljna matrica nad $\mathbb{Z}$ i neka je p prost broj, definisaćemo matricu nad $\mathbb{Z}_p$:*

$$B_p = B \bmod p = [b_{ij} \bmod p].$$

Napomena. Postoji bijekcija između minora matrice B_p i minora matrice B. Svaki $r \times r$ minor matrice B, $d = |b_{ij}|$, je povezan sa $r \times r$ minorom matrice B_p na sledeći način:

$$d_p = |b_{ij} \bmod p| = d \bmod p.$$

Teorema 3.4.2 *Neka je B matrica nad $\mathbb{Z}$. Tada je $rang(B_p) = r$ akko za svaki $m \times m$ minor matrice B, d, (gde je $m > r$), važi $(d \bmod p) = 0$.*

Dokaz. Ako je $rang(B_p) = r$ onda je $rang(B) \geq r$. Na osnovu Teoreme 1.5.3 postoji $r \times r$ minor matrice B_p, različit od nule, a svi minori matrice B_p reda $r+1 \times r+1$ su jednaki nuli, pa tada i za svaki minor $m \times m$ matrice B, d, (gde je $m > r$) važi $(d \bmod p) = 0$.
Pretpostavimo sada da je za svaki $m \times m$ minor matrice B, d, $(d \bmod p) = 0$, tj. $d_p = 0$, gde je d_p proizvoljan minor matrice B_p reda $m \times m$. Tada na osnovu Teoreme 1.5.3 sledi da je $rang(B_p) < m$, što je i trebalo pokazati.

□

Sledeća teorema je korisna za određivanje vektora koji predstavljaju testere u W ili u W_p.

Teorema 3.4.3 *Važi sledeće:*

(i) *$f \equiv (\alpha_1, \ldots, \alpha_N) \in W$ akko su tačne sledeće jednačine:*

$$\underbrace{\begin{bmatrix} a_{11} & a_{21} & \ldots & a_{N1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{1M} & a_{2M} & \ldots & a_{NM} \end{bmatrix}}_{A^T} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}. \tag{3.3}$$

(ii) *$f_p \equiv (\alpha_1, \ldots, \alpha_N) \in W_p$ akko su tačne sledeće jednačine:*

$$\underbrace{\begin{bmatrix} a_{11} \bmod p & a_{21} \bmod p & \ldots & a_{N1} \bmod p \\ \vdots & \vdots & \ddots & \vdots \\ a_{1M} \bmod p & a_{2M} \bmod p & \ldots & a_{NM} \bmod p \end{bmatrix}}_{A_p^T} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \bmod p. \tag{3.4}$$

Dokaz. Sledi direktno iz definicije testera, jer treći uslov kaže da je $f(a_{11},\dots,a_{N1}) = 0,\dots,f(a_{1M},\dots,a_{NM}) = 0$, a kako znamo da je $f \equiv (\alpha_1,\dots,\alpha_N)$ to je ekvivalentno sa

$$\begin{aligned} a_{11}\alpha_1 + a_{21}\alpha_2 + \dots + a_{N1}\alpha_N &= 0, \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ a_{1M}\alpha_1 + a_{2M}\alpha_2 + \dots + a_{NM}\alpha_N &= 0, \end{aligned}$$

a to je ustvari (3.3).
Analogno se pokazuje za (3.4).

□

Teorema 3.4.4 *Važi sledeće:*

(i) $dim(W) = N - rang(A)$

(ii) $dim(W_p) = N - rang(A_p)$.

Sledeća teorema je ključna za izvođenje važnih posledica koje ćemo koristiti u algoritmu za pronalaženje korisnih testera.

Teorema 3.4.5 *Neka je p proizvoljan prost broj i neka je $r = dim(W) \leq N$. Tada postoje testeri $f_1,\dots,f_r \in W_p$ tako da su $f_1,\dots,f_r$ linearno nezavisni i svi su izvedeni iz W.*

Dokaz. Dokaz ćemo dati indukcijom po m $\forall m \leq r\, \exists f_1,\dots,f_m \in W_p$ takvi da su $f_1,\dots,f_m$ linearno nezavisni i svi su izvedeni iz W.
(Baza indukcije) $m = 1 \leq r \leq N$
Neka je $g = (\alpha_1,\dots,\alpha_N) \in W \cap \mathbb{Z}^N$ tako da $g \neq 0$ (jer skup koji se sastoji samo od jednog vektora jednakog nuli je linearno zavisan) i neka je $d = NZD(\alpha_1,\dots,\alpha_N)$. Tada sledi $g' = g/d \in W \cap \mathbb{Z}^N$ i $(g' \bmod p) \neq 0$. Dakle, $(g' \bmod p) \in W_p$ je izveden iz W i $g' \neq 0$.
(Indukcijski korak) $m + 1 \leq r \leq N$
Zbog indukcijske hipoteze, postoje $g_1,\dots,g_m \in W \cap \mathbb{Z}^N$ takvi da: $(g_1 \bmod p),\dots,(g_m \bmod p)$ su linearno nezavisni u W_p. Možemo definisati (h_n), niz elemenata u $W \cap \mathbb{Z}^N$ tako da

(i) $g_1,\dots,g_m,h_0$ su linearno nezavisni u W (jer je $dim(W) > m$ i $g_1,\dots,g_m$ su linearno nezavisni, pa postoji $h_0 \in W \cap \mathbb{Z}^N$ tako da su $g_1,\dots,g_m,h_0$ su linearno nezavisni).

(ii) Ako su $(g_1 \bmod p),\dots,(g_m \bmod p),(h_i \bmod p)$ linearno nezavisni u W_p, onda

$$h_{i+1} = h_i.$$

(iii) Ako su $(g_1 \bmod p), \ldots, (g_m \bmod p), (h_i \bmod p)$ linearno zavisni u W_p, onda postoji linearna kombinacija $L = \tau_1 g_1 + \ldots + \tau_m g_m + \tau_0 h_i \bmod p = 0$, gde $\tau_i \in \mathbb{Z}$, $i \in \{0, 1, \ldots, m\}$ i τ_0 nije deljivo sa p, jer su $(g_1 \bmod p), \ldots, (g_m \bmod p)$ linearno nezavisni u W_p (indukcijska hipoteza) i ako bi τ_0 bilo deljivo sa p onda bi $(g_1 \bmod p), \ldots, (g_m \bmod p), (h_i \bmod p)$ bili linearno nezavisni. Kako je p prost broj, onda je $NZD(\tau_0, p) = 1$ pa postoje celi brojevi α i β takvi da $\alpha\tau_0 + \beta p = 1$. $\alpha\tau_0 \equiv 1 \bmod p$ pa sledi da postoji $k \in \mathbb{Z}$ tako da $\alpha\tau_0 = pk + 1$. Imamo da je $\alpha L = \alpha\tau_1 g_1 + \ldots + \alpha\tau_m g_m + \alpha\tau_0 h_i = \alpha\tau_1 g_1 + \ldots + \alpha\tau_m g_m + (pk+1)h_i$. Posmatrajući ovu jednakost po $\bmod p$ dobijamo $0 = \lambda_1 g_1 + \ldots + \lambda_m g_m + h_i \bmod p$, gde $\lambda_i \equiv \alpha\tau_i \pmod p$, $i \in \{1, \ldots, m\}$, odakle sledi

$$h_{i+1} = (\lambda_1 g_1 + \ldots + \lambda_m g_m + h_i)/p$$

Označimo sa $C_i = (g_1, \ldots, g_m, h_i)$, $\forall i \in \mathbb{N}$, matricu čiji su vektori kolone $g_1, \ldots, g_m, h_i$.
Neka su $\{d_{i,1}, \ldots, d_{i,s}\}$ $(m+1) \times (m+1)$ minori matrice C_i.
Ako su $(g_1 \bmod p), \ldots, (g_m \bmod p), (h_i \bmod p)$ linearno zavisni u W_p, tada je

(a) $\forall d_{ij}$ $(m+1) \times (m+1)$ minor matrice C_i, $d_{ij} \bmod p = 0$ (Teorema 3.4.2).

(b) $(m+1) \times (m+1)$ minori matrice C_{i+1} su $\{d_{i,1}/p, \ldots, d_{i,s}/p\}$. Ovo je zbog činjenice $C_{i+1} = (g_1, \ldots, g_m, h_{i+1}) = (g_1, \ldots, g_m, (\lambda_1/p)g_1) + \ldots + (g_1, \ldots, g_m, (\lambda_m/p)g_m) + (g_1, \ldots, g_m, (1/p)h_i)$.

Zbog (b) sledi da $\exists n \in \mathbb{N}$ tako da za neko d, $(m+1) \times (m+1)$ minor matrice C_n, $d \bmod p \neq 0$.
Dakle, zbog Teoreme 3.4.2, važi da je $rang(C_n) \geq m+1$ što je ekvivalentno da su $(g_1 \bmod p), \ldots, (g_m \bmod p), (h_i \bmod p) \in W_p$ linearno nezavisni.

□

Posledica 3.4.1 *Neka je p prost broj.*

(i) *$\exists f \in W$ takav da f nije trivijalan tester $\Leftrightarrow dim(W) > 0$.*

(ii) *$\exists f_p \in W_p$ takav da f nije izveden iz $W \Leftrightarrow dim(W_p) > dim(W)$.*

Ova posledica je značajna za određivanje da li postoje netrivijalni testeri u W i testeri u W_p koji nisu izvedeni iz W.

Posledica 3.4.2 *Važi*

(i) *$\exists f \in W$ takav da f nije trivijalan tester $\Leftrightarrow rang(A) < N$.*

(ii) $\exists f_p \in W_p$ *takav da* f *nije izveden iz* $W \Leftrightarrow \forall d, r \times r$ *minor matrice* A, *gde je* $r = rang(A)$, *važi* $p|d$.

Dokaz.

(i) Zbog (i) iz Posledice 3.4.1, sledi da $\exists f \in W$ takav da f nije trivijalan $\Leftrightarrow dim(W) > 0 \Leftrightarrow N - rang(A) > 0 \Leftrightarrow rang(A) < N$.

(ii) ($\Rightarrow$) Zbog (ii) iz Posledice 3.4.1, imamo
$\exists f_p \in W_p$ koji nije izveden iz $W \Leftrightarrow dim(W_p) > dim(W) \Leftrightarrow rang(A_p) < rang(A) \Leftrightarrow$ za svaki $r \times r$ minor matrice A_p, d, važi da je $d = 0$. Dakle, $p|d$.
($\Leftarrow$) Zbog Teoreme 3.4.2 imamo da za svaki $r \times r$ minor matrice A, d, važi $p|d \Leftrightarrow rang(A_p) < rang(A) \Leftrightarrow dim(W_p) > dim(W) \Leftrightarrow \exists f_p \in W_p$ takav da f nije izveden iz W.

□

Sumirajući sve, Teorema 3.4.3 pruža metod za pronalaženje svih testera u W i W_p gde je p prost broj. Ako su neki od ovih testera korisni, onda nam mogu pomoći u rešavanju problema tako što ćemo eliminisati neke elemente iz skupa Y. Međutim, neki od ovih testera mogu biti beskorisni. Zaista, prema Teoremi 3.4.1, trivijalni tester, $(0, \ldots, 0)$, je jedan beskoristan tester, i ako $f \in W$ beskoristan tester, onda je izvedeni tester $(f \bmod p) \in W_p$ takođe beskoristan tester. Dakle, ne interesuju nas ovakvi testeri.

Posledica 3.4.2 postavlja neke uslove vezane za matricu A za pronalaženje testera u W i u W_p koji nisu trivijalni niti izvedeni iz W. Imajući u vidu ovu teoremu, predlažemo sledeći algoritam. Ulaz ovog algoritma je izraz oblika (3.2) sa skupom mogućih nezavisnih promenljivih skupa Y, a njegov izlaz je podskup $Y^* \subseteq Y$ koji sadrži elemente iz Y kompaktibilne sa svim testerima iz W i iz W_p (gde je p proizvoljan prost broj).

Koraci 1, 2, 3 i 4 u algoritmu grade bazu testera u W, $\{b_1, \ldots, b_s\}$, i eliminišu elemente iz Y koji su nekompaktibilni sa ovom bazom. Kada smo eliminisali sve elemente iz Y nekompaktibilne sa bazom, testeri u W, $\{b_1, \ldots, b_s\}$ postaju beskorisni. Dakle, svi testeri u W su beskorisni (dimenzija vektorskog potprostora beskorisnih testera u W je jednaka dimenziji vektorskog prostora W). Dakle, sada svi testeri u W_p izvedeni iz W su beskorisni (Teorema 3.4.1).

Koraci 5 i 6 su namenjeni da pronađu testere u W_p, gde je p prost broj. Zbog (ii) Posledice 3.4.2, znamo koji prosti brojevi su mogući za pronalaženje korisnih testera u W_p (tj. testera koji nisu trivijalni niti izvedeni iz W). Kada pronađemo bazu $\{b_1, \ldots, b_t\}$ skupa W_p i eliminišemo sve elemente u Y koji su

nekompaktibilni sa ovom bazom, možemo reći da nema više korisnih testera u W_p (dimenzija vektorskog potprostora beskorisnih testera u W_p je jednaka dimenziji vektorskog prostora W_p).

Algoritam.

1. $s := N$
2. Računamo sve $s \times s$ minore matrice A, $d_1, \ldots, d_m$
3. Ako su sve determinante jednake nuli onda
   - 3.1 $s := s - 1$
   - 3.2 Vratiti se na korak 2
4. Ako je $s \neq N$ onda,
   - 4.1 Izračunati bazu skupa W, $b_1, \ldots, b_s$
   - 4.2 Eliminisati $y \in Y$ pomoću testera $b_1, \ldots, b_s$
5. Izračunati d kao $d := NZD(d_1, \ldots, d_m)$
6. Za svaki prost broj, p, takav da $p|d$
   - 6.1 Izračunati bazu skupa W_p, $b_1, \ldots, b_t$
   - 6.2 Eliminisati $y \in Y$ pomoću testera $b_1, \ldots, b_t$

Kroz ovaj algoritam pronalazimo sve testere u W ili W_p gde je p proizvoljan prost broj, ne tražimo testere u W_n gde n nije prost broj. Pored toga, efikasnost ovog algoritma dosta zavisi od veličine matrice A. Sledeća teorema je korisna, jer nam pokazuje kako brzo možemo pronaći testere u nekim specijalnim slučajevima.

Teorema 3.4.6 *Važi sledeće:*

(i) *Ako* $\forall i \in \{1, \ldots, N\}\, \forall j \in \{1, \ldots, M\}\ \ a_{ij} = a_{Nj}$, *onda*

$$\{(1, 0, 0, \ldots, 0, -1), (0, 1, 0, \ldots, 0, -1), \ldots, (0, 0, \ldots, 0, 1, -1)\} \subseteq W.$$

(ii) *Ako* $\exists d \in \mathbb{Z}^+$ *tako da* $\forall i \in \{1, \ldots, N\}\, \forall j \in \{1, \ldots, M\}\, d|(a_{ij} - a_{Nj})$, *onda*

$$\{(1, 0, 0, \ldots, 0, -1), (0, 1, 0, \ldots, 0, -1), \ldots, (0, 0, \ldots, 0, 1, -1)\} \subseteq W_d.$$

(iii) *Neka su* $\alpha, \beta \in \mathbb{Z}$ *takvi da* $|\alpha - \beta| > 1$.
Ako $\forall i \in \{1, \ldots, N\}\, \forall j \in \{1, \ldots, M\}\, b_{ij} \in \{\alpha, \beta\}$, *onda*

$$\{(1, 0, 0, \ldots, 0, -1), (0, 1, 0, \ldots, 0, -1), \ldots, (0, 0, \ldots, 0, 1, -1)\} \subseteq W_{|\alpha-\beta|}.$$

(iv) *Neka* $i \in \{1, \ldots, M\}$.
Ako $\forall j \in \{1, \ldots, N\}\, \exists d_j \in \mathbb{Z}^+\ d_j | b_{ji}$, *onda*

$$f(z_1, \ldots, z_N) \equiv (z_j \bmod d_j) \in W_{d_j}.$$

(v) *Ako* $\forall j \in \{1, \ldots, M\}\, b_{1j} + \ldots + b_{Nj} = 0$, *onda*

$$(1, 1, \ldots, 1) \in W.$$

(vi) *Ako* $\exists d \in \mathbb{Z}^+$ *takvo da* $\forall j \in \{1, \ldots, M\}, d | (b_{1j} + \ldots + b_{Nj})$, *onda*

$$(1, 1, \ldots, 1) \in W_d.$$

Dokaz.

(i) Sistem jednačina koji posmatramo je sledeći:

$$\begin{bmatrix} a_{N1} & a_{N2} & \ldots & a_{NM} \\ \vdots & \vdots & \ddots & \vdots \\ a_{N1} & a_{N2} & \ldots & a_{NM} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_M \end{bmatrix} = \begin{bmatrix} y_1 \\ \vdots \\ y_N \end{bmatrix}.$$

Sve vrste matrice koja sadrži zavisne promenljive su jednake, pa da bi bilo moguće rešavati ovaj sistem moraju i sve vrste matrice kolone koja sadrži nezavisne promenljive $y_1, \ldots, y_N$ biti jednake, recimo y_N. Dakle, mora važiti uslov

$$\begin{aligned} y_1 &= y_N \\ y_2 &= y_N \\ &\vdots \\ y_{N-1} &= y_N \end{aligned}$$

Uslov $y_1 = y_N$ nam daje tester oblika $f(z_1, \ldots, z_N) = z_1 - z_N$, tj. vektor koji generiše tester je $(1, 0, \ldots, 0, -1)$, itd. uslov $y_{N-1} = y_N$ nam daje tester oblika $f(z_1, \ldots, z_N) = z_{N-1} - z_N$, tj. vektor koji generiše tester je $(0, 0, \ldots, 1, -1)$. Dobili smo da skupu testera W pripadaju testeri $\{(1, 0, 0, \ldots, 0, -1), (0, 1, 0, \ldots, 0, -1), \ldots, (0, 0, \ldots, 0, 1, -1)\}$, što je i trebalo dokazati.

(ii) Uslov $\forall i \in \{1,\ldots,N\}\,\forall j \in \{1,\ldots,M\}\, d|(a_{ij}-a_{Nj})$ je zapravo $a_{ij} \equiv a_{Nj} \bmod d$, pa posmatrajući sistem jednačina po $(\bmod d)$ slučaj se svodi na (i).

(iii) Neka važi dati uslov. Funkcije $f_1(z_1,\ldots,z_N) = z_1 - z_N \bmod|\alpha-\beta|$, $f_2(z_1,\ldots,z_N) = z_2 - z_N \bmod|\alpha-\beta|$, itd. $f_{N-1}(z_1,\ldots,z_N) = z_{N-1} - z_N \bmod|\alpha-\beta|$ zadovoljavaju prva dva uslova Definicije 3.3.1. Očigledno je da važi i treći uslov ove definicije jer je $f_i(b_{11},\ldots,b_{N1}) = b_{i1}-b_{N1} = |\alpha-\beta| = 0\,(\bmod|\alpha-\beta|)$, itd. $f_i(b_{1M},\ldots,b_{NM}) = b_{iM}-b_{NM} = |\alpha-\beta| = 0\,(\bmod|\alpha-\beta|)$ za $i \in \{1,\ldots,N-1\}$.

(iv) Matricu sistema sa zavisnim promenljivama označimo sa $B = [b_{ij}]_{N\times M}$. Dati uslov nam kaže da postoje brojevi $d_1,\ldots,d_N \in \mathbb{Z}^+$ takvi da d_1 deli prvu vrstu matrice B, d_2 deli drugu vrstu matrice B, itd. d_N deli poslednju vrstu matrice B. $f(z_1,\ldots,z_N) \equiv (z_j \bmod d_j)$ jeste tester u W_{d_j}. Proverićemo treći uslov Definicije 3.3.1. $f(b_{1i},b_{2i},\ldots,b_{Ni}) = (b_{ji} \bmod d_j) = 0$, gde $i \in \{1,\ldots,M\}$ i $j \in \{1,\ldots,N\}$.

(v) Pošto je f tester, onda važi

$$\begin{aligned} f(b_{11},\ldots,b_{N1}) &= 0 = b_{11}+\ldots+b_{N1} \\ f(b_{12},\ldots,b_{N2}) &= 0 = b_{12}+\ldots+b_{N2} \\ &\vdots \\ f(b_{1M},\ldots,b_{NM}) &= 0 = b_{1M}+\ldots+b_{NM} \end{aligned}$$

a to znači da $(1,1,\ldots,1) \in W$.

(vi) Ako važi uslov

$$\begin{array}{c} d|b_{11}+\ldots+b_{N1} \\ d|b_{12}+\ldots+b_{N2} \\ \vdots \\ d|b_{1M}+\ldots+b_{NM} \end{array} \quad\Leftrightarrow\quad \begin{array}{c} (b_{11}+\ldots+b_{N1}) \bmod d = 0 \\ (b_{12}+\ldots+b_{N2}) \bmod d = 0 \\ \vdots \\ (b_{1M}+\ldots+b_{NM}) \bmod d = 0 \end{array}$$

onda je očigledno da $(1,1,\ldots,1) \in W_d$.

□

3.5 Primeri

U ovom delu pokazaćemo primenu metoda za pokazivanje nepostojanja rešenja sistema linearnih Diofantovih jednačina kroz neke primere.

Primer 3.5.1

$$\begin{bmatrix} 2 & -2 & 1 \\ 1 & 1 & -2 \\ -3 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \left\{ \begin{bmatrix} -25 \\ 18 \\ 5 \end{bmatrix}, \begin{bmatrix} 20 \\ 17 \\ -35 \end{bmatrix}, \begin{bmatrix} 132 \\ -28 \\ -97 \end{bmatrix} \right\}$$

$|A| = 0$, a postoji minor reda 2×2, $\begin{vmatrix} 2 & -2 \\ 1 & 1 \end{vmatrix} \neq 0$ pa na osnovu Teoreme 1.5.3 sledi da je $rang(A) = 2$. Onda je $dim(W) = N - rang(A) = 3 - 2 = 1$ što znači da se baza vektorskog prostora W sastoji od samo jednog vektora koga možemo dobiti rešavajući sledeći sistem jednačina:

$$\begin{bmatrix} 2 & 1 & -3 \\ -2 & 1 & 1 \\ 1 & -2 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Rešavajući sistem Gausovim postupkom dobijamo sistem koji je ekvivalentan polaznom sistemu:

$$\left[\begin{array}{ccc|c} 2 & 1 & -3 & 0 \\ -2 & 1 & 1 & 0 \\ 1 & -2 & 1 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 2 & 1 & -3 & 0 \\ 0 & 2 & -2 & 0 \\ 0 & -\frac{5}{2} & -\frac{5}{2} & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 2 & 1 & -3 & 0 \\ 0 & 2 & -2 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

Ovde je najpre prva vrsta dodata drugoj, a zatim pomnožena sa $-\frac{1}{2}$ i dodata trećoj. U sledećem koraku je druga vrsta pomnožena sa $\frac{5}{4}$ i dodata trećoj. Dobili smo sistem ekvivalentan polaznom koji je neodređen i čija rešenja zapisujemo u obliku

$$RS = \{(x_3, x_3, x_3) | x_3 \in \mathbb{Q}\}.$$

Baza vektorskog prostora W je $\{(1, 1, 1)\}$, odnosno

$$f(z_1, z_2, z_3) = z_1 + z_2 + z_3.$$

Bazu vektorskog prostora W smo mogli lako pronaći primenjujući Teoremu 3.4.6 (v). Sada ćemo eliminisati elemente iz skupa Y koji su nekompaktibilni sa testerom f:

$$f(-25, 18, 5) = -25 + 18 + 5 = -2 \neq 0,$$

$$f(20, 17, -35) = 20 + 17 - 35 = 2 \neq 0,$$

$$f(132, -28, -97) = 132 - 28 - 97 = 7 \neq 0.$$

Pošto smo eliminisali sve elemente skupa Y, zaključujemo da nijedan od 3 sistema nema rešenje.

Napominjemo da ne postoji nijedan koristan tester u skupu W_p, gde je p prost broj. Zaista, na osnovu (ii) Posledice 3.4.2 postoji $f_p \in W_p$ koji nije izveden iz W akko p deli svaki $r \times r$ minor matrice A, gde je r rang matrice A. U ovom primeru računajući sve 2×2 minore matrice A dobijamo:

$$\left\{\begin{vmatrix} 2 & 1 \\ -2 & 1 \end{vmatrix}, \begin{vmatrix} 2 & -3 \\ -2 & 1 \end{vmatrix}, \begin{vmatrix} -2 & 1 \\ 1 & -2 \end{vmatrix}, \begin{vmatrix} -2 & 1 \\ 1 & 1 \end{vmatrix}, \begin{vmatrix} 2 & 1 \\ 1 & -2 \end{vmatrix},\right.$$

$$\left.\begin{vmatrix} 2 & -3 \\ 1 & 1 \end{vmatrix}, \begin{vmatrix} 1 & -3 \\ 1 & 1 \end{vmatrix}, \begin{vmatrix} 1 & -3 \\ -2 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ -2 & 1 \end{vmatrix}\right\} = \{3, -3, 4, -4, 5, -5\}$$

pa ne postoji prost broj koji deli sve ove minore.

Primer 3.5.2

$$\begin{bmatrix} -3 & 2 & 2 \\ 2 & -3 & 2 \\ 2 & 2 & -3 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \left\{ \begin{bmatrix} 15 \\ 4 \\ 41 \end{bmatrix}, \begin{bmatrix} -10 \\ 3 \\ -23 \end{bmatrix}, \begin{bmatrix} 16 \\ -9 \\ 58 \end{bmatrix}, \begin{bmatrix} 105 \\ 75 \\ 792 \end{bmatrix}, \begin{bmatrix} 79 \\ 33 \\ 0 \end{bmatrix} \right\}$$

$|A| = 25 \neq 0$ pa sledi da je $rang(A) = 3$. Onda je $dim(W) = 3 - 3 = 0$ što znači da nema testera u W. Na osnovu (ii) Posledice 3.4.2 kako je $|A| = 25$ jedini prost broj koji deli 25 je broj 5. Dakle, tražimo testere u W_5. Primenjujući Teoremu 3.4.3, bazu skupa W_5 računamo rešavajući sledeći sistem jednačina:

$$\begin{bmatrix} 2 & 2 & 2 \\ 2 & 2 & 2 \\ 2 & 2 & 2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Kako je

$$\left[\begin{array}{ccc|c} 2 & 2 & 2 & 0 \\ 2 & 2 & 2 & 0 \\ 2 & 2 & 2 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 2 & 2 & 2 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

sledi $RS = \{(-x_2 - x_3, x_2, x_3) \bmod 5 \,|\, x_2, x_3 \in \mathbb{Z}\}$. Ako uzmemo da je $x_2 = x_3 = 1$ sledi $(-2, 1, 1) \bmod 5 = (3, 1, 1)$, i $x_2 = 1, x_3 = 0$ sledi $(-1, 1, 0) \bmod 5 = (4, 1, 0)$. Ispitaćemo da li su ovi vektori linearno nezavisni. Iz

$$\alpha(3, 1, 1) + \beta(4, 1, 0) = 0$$

sledi

$$\begin{aligned} 3\alpha + 4\beta &= 0 \\ \alpha + \beta &= 0 \\ \alpha &= 0 \end{aligned}$$

pa je $\alpha = \beta = 0$. Dakle, vektori su linearno nezavisni. Treba još pokazati da generišu prostor W_5.

Neka je (a, b, c) proizvoljan vektor iz W_5, tj. on je oblika $(-b-c, b, c) \bmod 5$. Vektorska jednačina

$$\alpha(3, 1, 1) + \beta(4, 1, 0) = (a, b, c)$$

je ekvivalentna sa sistemom od tri skalarne jednačine

$$\begin{aligned} 3\alpha + 4\beta &= a \\ \alpha + \beta &= b \\ \alpha &= c \end{aligned} .$$

Odavde sledi da je $\alpha = c$, $\beta = b - c$, a jednačina $3\alpha + 4\beta = a \Leftrightarrow 4b - c = a \,(\mathrm{mod}\, 5) \Leftrightarrow -b - c = a \,(\mathrm{mod}\, 5)$ što znači da postoji rešenje ovog sistema za svako $(a, b, c) \in W_5$. Dakle, baza vektorskog prostora W_5 je $\{(4, 1, 0), (3, 1, 1)\}$. Odnosno,

$$f_5^1(z_1, z_2, z_3) = (4z_1 + z_2) \bmod 5$$

$$f_5^2(z_1, z_2, z_3) = (3z_1 + z_2 + z_3) \bmod 5$$

Sada ćemo eliminisati elemente skupa Y koji su nekompaktibilni sa testerom f_5^1 :

$$f_5^1(15, 4, 41) = 4 \cdot 15 + 4 \bmod 5 = 64 \bmod 5 = 4 \neq 0,$$

$$f_5^1(-10, 3, -23) = 4 \cdot (-10) + 3 \bmod 5 = -37 \bmod 5 = 3 \neq 0,$$

$$f_5^1(16, -9, 58) = 4 \cdot 16 - 9 \bmod 5 = 55 \bmod 5 = 0,$$

$$f_5^1(105, 75, 792) = 4 \cdot 105 + 75 \bmod 5 = 495 \bmod 5 = 0,$$

$$f_5^1(79, 33, 0) = 4 \cdot 79 + 33 \bmod 5 = 349 \bmod 5 = 4 \neq 0.$$

Tester f_5^1 je uklonio elemente $(15, 4, 41)$, $(-10, 3, -23)$ i $(79, 33, 0)$ iz Y. Sada, pomoću testera f_5^2 :

$$f_5^2(16, -9, 58) = 3 \cdot 16 - 9 + 58 \bmod 5 = 97 \bmod 5 = 2 \neq 0,$$

$$f_5^2(105, 75, 792) = 3 \cdot 105 + 75 + 792 \bmod 5 = 1282 \bmod 5 = 2 \neq 0$$

uklanjamo i elemente $(16, -9, 58)$ i $(105, 75, 792)$ iz skupa Y.
Pošto su testeri f_5^1 i f_5^2 uklonili sve elemente iz skupa Y, imamo da polazni sistemi nemaju rešenje.

Primer 3.5.3

$$\begin{bmatrix} 1 & 1 & -2 & 4 \\ 1 & -2 & 1 & -2 \\ -2 & 1 & 1 & -2 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix} = \left\{ \begin{bmatrix} 36 \\ 13 \\ -49 \end{bmatrix}, \begin{bmatrix} -23 \\ 35 \\ -8 \end{bmatrix}, \begin{bmatrix} 20 \\ -41 \\ 21 \end{bmatrix}, \begin{bmatrix} 56 \\ -35 \\ -21 \end{bmatrix}, \begin{bmatrix} -61 \\ 87 \\ 0 \end{bmatrix} \right\}$$

$rang(A) = 2$ jer je

$$\begin{bmatrix} 1 & 1 & -2 & 4 \\ 1 & -2 & 1 & -2 \\ -2 & 1 & 1 & -2 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & -2 & 4 \\ 0 & -3 & 3 & -6 \\ 0 & 3 & -3 & 6 \end{bmatrix} \sim \begin{bmatrix} 1 & 1 & -2 & 4 \\ 0 & -3 & 3 & -6 \\ 0 & 0 & 0 & 0 \end{bmatrix}$$

$dim(W) = N - rang(A) = 3 - 2 = 1$ pa sledi da se baza vektorskog prostora W sastoji od jednog vektora. Primetimo da je zbir svake kolone naše matrice A jednak nuli, pa primenjujući Teoremu 3.4.6 (v) zaključujemo da je baza od W jednaka $\{(1, 1, 1)\}$, odnosno

$$f(z_1, z_2, z_3) = z_1 + z_2 + z_3.$$

Sada ćemo eliminisati elemente skupa Y koji su nekompaktibilni sa testerom f:

$$f(36, 13, -49) = 36 + 13 - 49 = 0,$$
$$f(-23, 35, -8) = -23 + 35 - 8 = 4 \neq 0,$$
$$f(20, -41, 21) = 20 - 41 + 21 = 0,$$
$$f(56, -35, -21) = 56 - 35 - 21 = 0,$$
$$f(-61, 87, 0) = -61 + 87 + 0 = 26 \neq 0.$$

Tester f je uklonio $(-23, 35, -8)$ i $(-61, 87, 0)$ iz skupa Y. Sada računamo sve 2×2 minore matrice A.

$$\left\{ \begin{vmatrix} 1 & 1 \\ 1 & -2 \end{vmatrix}, \begin{vmatrix} 1 & -2 \\ 1 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ -2 & 1 \end{vmatrix}, \begin{vmatrix} 1 & -2 \\ -2 & 1 \end{vmatrix}, \begin{vmatrix} 1 & 1 \\ 4 & -2 \end{vmatrix}, \right.$$

$$\left. \begin{vmatrix} 1 & -2 \\ 4 & -2 \end{vmatrix}, \begin{vmatrix} 1 & -2 \\ -2 & -2 \end{vmatrix}, \begin{vmatrix} -2 & 1 \\ 4 & -2 \end{vmatrix}, \begin{vmatrix} -2 & 1 \\ 4 & -2 \end{vmatrix} \right\} = \{0, 3, -3, 6, -6\}$$

Jedini prost broj koji deli sve 2×2 minore matrice A je 3. Na osnovu Posledice 3.4.2 tražimo testere u W_3. $dim(W_3) = N - rang(A_3) = 3 - 1 = 2$. Primenjujući Teoremu 3.4.3, bazu skupa W_3 računamo rešavajući sledeći sistem jednačina:

$$\begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Kako je

$$\left[\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 \end{array}\right] \sim \left[\begin{array}{ccc|c} 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right]$$

sledi $RS = \{(-x_2 - x_3, x_2, x_3) \bmod 3 \,|\, x_2, x_3 \in \mathbb{Z}\}$. Ako uzmemo da je $x_2 = x_3 = 1$ sledi $(-2, 1, 1) \bmod 3 = (1, 1, 1)$, i $x_2 = 1, x_3 = 0$ sledi $(-1, 1, 0) \bmod 3 = (2, 1, 0)$. Dakle, baza vektorskog prostora W_3 je $\{(2, 1, 0), (1, 1, 1)\}$. Odnosno,

$$f_3^1(z_1, z_2, z_3) = (2z_1 + z_2) \bmod 3$$

$$f_3^2(z_1, z_2, z_3) = (z_1 + z_2 + z_3) \bmod 3$$

Primetimo da je tester f_3^2 izveden iz testera f. Sada ćemo eliminisati elemente iz Y koji su nekompaktibilni sa testerom f_3^1:

$$f_3^1(36, 13, -49) = 2 \cdot 36 + 13 \bmod 3 = 85 \bmod 3 = 1 \neq 0,$$

$$f_3^1(20, -41, 21) = 2 \cdot 20 - 41 \bmod 3 = -1 \bmod 3 = 2 \neq 0,$$

$$f(56, -35, -21) = 2 \cdot 56 - 35 \bmod 3 = 77 \bmod 3 = 2 \neq 0.$$

Pošto smo pomoću testera f i f_3^1 eliminisali sve elemente skupa Y, zaključujemo da polazni sistemi nemaju rešenje.

Glava 4

Pokazivanje egzistencije rešenja sistema linearnih Diofantovih jednačina pomoću testera

4.1 Uvod

U ovoj glavi proučavamo mogućnost pronalaženja rešenja određene familije sistema linearnih Diofantovih jednačina sa istim zavisnim i različitim nezavisnim promenljivama koristeći metod koji je zasnovan na testerima sa kojima smo se upoznali u prethodnoj glavi. Ispitivanje egzistencije rešenja sistema linearnih Diofantovih jednačina može se vršiti pomoću Smitove normalne forme za datu matricu. Računanje Smitove normalne forme pomoću klasičnog metoda zasnovanog na Gausovom postupku eliminacije je eksponencijalne složenosti, potrebno je mnogo vremena. Upoznali smo se sa metodom zasnovanom na linearnim funkcijama koje se nazivaju "Testeri" i koje su davale odgovor nepostojanja rešenja određenih sistema linearnih Diofantovih jednačina. Takođe smo se upoznali i sa metodom dobijanja testera definisanih nad prstenima $\mathbb{Q}$ i $\mathbb{Z}_p$, gde je p prost broj. Međutim, nije razmatrano pitanje računanja testera nad prstenom $\mathbb{Z}_m$, gde m nije prost broj. Osim toga, testere nismo koristili za dokazivanje postojanja rešenja sistema, već isključivo za dokazivanje nepostojanja rešenja.

U ovom delu ćemo pokazati kako testeri mogu biti korisni za pokazivanje i egzistencije rešenja, kao što ćemo pokazati u nastavku, egzistencija rešenja familije linearnih Diofantovih jednačina je uvek određena određenim skupom testera. Pored toga, proučavaćemo i neke metode za pronalaženje odgovarajućih testera nad prstenom $\mathbb{Z}_m$, gde m nije prost broj.

4.2 Kompletan skup testera

U prethodnoj glavi upoznali smo se sa problemom sa kojim se susrećemo (3.1). Definisali smo testere, čiji značaj leži u činjenici da pružaju jednostavan način određivanja da li sistem jednačina (3.1) ima rešenje koje odgovara $y_1, \ldots, y_N \in \mathbb{Z}$, o čemu je govorila teorema 3.3.1. U primerima 3.5.1, 3.5.2 i 3.5.3 videli smo kako testeri mogu biti korisni u pokazivanju nepostojanja rešenja određenih sistema linearnih Diofantovih jednačina. Međutim, neka pitanja u vezi testera se sama nameću:

- Ako sistem linearnih Diofantovih jednačina nema rešenje koje odgovara $(y_1, \ldots, y_N)$, da li uvek postoji tester f takav da je $f(y_1, \ldots, y_N) \neq 0$?
- Da li postoji konačan skup testera $\{f_1, \ldots, f_k\}$ takav da, ako je $f_1(y_1, \ldots, y_N) = \ldots = f_k(y_1, \ldots, y_N) = 0$, možemo zaključiti da sistem linearnih jednačina ima rešenje koje odgovara $(y_1, \ldots, y_N)$?

U nastavku ćemo se uveriti da je odgovor na oba pitanja pozitivan. Sada ćemo dati definiciju kompletnog skupa testera.

Definicija 4.2.1 *Neka su $f_1, \ldots, f_k$ testeri koji odgovaraju matrici A. $\{f_1, \ldots, f_k\}$ je kompletan skup testera matrice A ako i samo ako važi sledeća osobina:*
Sistem jednačina (3.1) ima rešenje koje odgovara $y_1, \ldots, y_N \in \mathbb{Z}$

$$\Leftrightarrow$$

$$f_1(y_1, \ldots, y_N) = f_2(y_1, \ldots, y_N) = \ldots = f_k(y_1, \ldots, y_N) = 0.$$

Sada ćemo pokazati egzistenciju kompletnog skupa testera za dijagonalnu matricu.

Teorema 4.2.1 *Neka je*

$$B = \begin{bmatrix} d_1 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & d_2 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & d_r & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{bmatrix}$$

dijagonalna matrica tipa $N \times M$ takva da $\forall i \in \{1, 2, \ldots, r\}$ $d_i \neq 0$.
Neka je $g_i(y_1, \ldots, y_N) = y_i \bmod d_i$, gde $i \in \{1, 2, \ldots, r\}$.

Neka je $f_j(y_1, \ldots, y_N) = y_j$ *gde* $j \in \{r+1, \ldots, N\}$.
Tada imamo da je $\{g_1, g_2, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ *kompletan skup testera matrice* B.

Dokaz. Lako se pokazuje da su $g_1, g_2, \ldots, g_r, f_{r+1}, \ldots, f_N$ testeri. Pošto je $A = diag(d_1, d_2, \ldots, d_r, 0, \ldots, 0)$ dijagonalna matrica, onda sistem linearnih Diofantovih jednačina izgleda:

$$\begin{aligned} d_1 \cdot x_1 &= y_1 \\ d_2 \cdot x_2 &= y_2 \\ &\cdots \\ d_r \cdot x_r &= y_r \\ 0 &= y_{r+1} \\ 0 &= y_{r+2} \\ &\cdots \\ 0 &= y_N. \end{aligned}$$

Ovaj sistem ima rešenje ako i samo ako

$$d_1|y_1,\ d_2|y_2,\ \ldots, d_r|y_r,\ y_{r+1} = 0,\ \ldots, y_N = 0$$

$$\Leftrightarrow$$

$$g_1(y_1, \ldots, y_N) = \ldots = g_r(y_1, \ldots, y_N) = f_{r+1}(y_1, \ldots, y_N) = \ldots = f_N(y_1, \ldots, y_N) = 0.$$

Dakle, $\{g_1, g_2, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ je kompletan skup testera.

□

Pomoću Smitove normalne forme matrice možemo dokazati da za svaku celobrojnu matricu postoji kompletan skup testera.

Teorema 4.2.2 *Postoji kompletan skup testera za svaku matricu* A *nad prstenom* $\mathbb{Z}$.

Dokaz. Neka je A proizvoljna celobrojna matrica tipa $N \times M$. Na osnovu Teoreme 2.3.3 matricu A možemo zapisati u obliku $A = LDR$, gde je L invertibilna $N \times N$ matrica, R invertibilna $M \times M$ matrica a $D = \{d_1, \ldots, d_r, 0, \ldots, 0\}$ dijagonalna matrica. Tada važi:
Sistem (3.1) ima rešenje koje odgovara $\mathbf{y} \in \mathbb{Z}^N \Leftrightarrow$
$\exists \mathbf{x} \in \mathbb{Z}^M$ tako da $A\mathbf{x} = \mathbf{y} \Leftrightarrow$
$\exists \mathbf{x} \in \mathbb{Z}^M$ tako da $LDR\mathbf{x} = \mathbf{y} \Leftrightarrow$
$\exists \mathbf{x} \in \mathbb{Z}^M$ tako da $D(R\mathbf{x}) = L^{-1}\mathbf{y} \Leftrightarrow$
$\exists \mathbf{z} \in \mathbb{Z}^M$ tako da $D\mathbf{z} = \mathbf{w}$ gde $\mathbf{w} = L^{-1}\mathbf{y}$. Prema Teoremi 4.2.1, postoji kompletan skup testera $\{g_1, g_2, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ za matricu D.

Dakle, sistem (3.1) ima rešenje koje odgovara $\mathbf{y} \in \mathbb{Z}^N \Leftrightarrow$
$g_1(\mathbf{w}) = \ldots = g_r(\mathbf{w}) = f_{r+1}(\mathbf{w}) = \ldots = f_N(\mathbf{w}) = 0 \Leftrightarrow$
$g_1(L^{-1}\mathbf{y}) = \ldots = g_r(L^{-1}\mathbf{y}) = f_{r+1}(L^{-1}\mathbf{y}) = \ldots = f_N(L^{-1}\mathbf{y}) = 0.$
Odnosno, $\{g_1^*, \ldots, g_r^*, f_{r+1}^*, \ldots, f_N^*\}$ je kompletan skup testera sistema $A\mathbf{x} = \mathbf{y}$, gde:
$g_i^*(\mathbf{y}) = g_i(L^{-1}\mathbf{y})$ gde $i \in \{1, \ldots, r\}$, i
$f_i^*(\mathbf{y}) = f_i(L^{-1}\mathbf{y})$ gde $i \in \{r+1, \ldots, N\}$.

□

Teorema 4.2.2 nam pokazuje da egzistencija rešenja sistema (3.1) može biti lako određena pomoću određenog skupa testera koji smo nazvali kompletan skup testera. Prema dokazu te teoreme, ovaj kompletan skup testera možemo dobiti računajući Smitovu normalnu formu matrice A.

Ipak, računanje Smitove normalne forme za celobrojnu matricu može se dugo izvršavati i zauzeti veći deo memorije koja može premašiti memoriju jednog procesora. Računanje Smitove normalne forme matrice A uključuje transformacije njenih vrsta i kolona. Vrsta r_i u matrici A može biti zamenjena vrstom $r_i + kr_j$, gde je k ceo broj, a r_j neka druga vrsta matrice A. Analogno, kolonu c_i matrice A možemo zameniti kolonom $c_i = kc_j$, gde je k ceo broj, a c_j neka druga kolona matrice A. Transformacije kolona i vrsta odgovaraju matricama L i R iz dokaza Teoreme 4.2.2, redom. Glavni problem nastaje kada treba da izračunamo Smitovu normalnu formu za matricu velikih dimenzija, jer je to previše naporan posao.

Zato ćemo u nastavku proučavati kako da izračunamo kompletan skup testera ne računajući Smitovu normalnu formu matrice.

Primer 4.2.1 Računamo kompletan skup testera matrice A koristeći Teoremu 4.2.2.

$$\underbrace{\left[\begin{array}{ccc|cccc} 1 & 2 & 2 & 1 & 0 & 0 & 0 \\ 2 & 0 & 1 & 0 & 1 & 0 & 0 \\ 2 & 1 & -1 & 0 & 0 & 1 & 0 \\ 2 & -1 & 1 & 0 & 0 & 0 & 1 \end{array}\right]}_{A \qquad\qquad E_4} \rightarrow \left[\begin{array}{ccc|cccc} 1 & 2 & 2 & 1 & 0 & 0 & 0 \\ 0 & -4 & -3 & -2 & 1 & 0 & 0 \\ 0 & -3 & -5 & -2 & 0 & 1 & 0 \\ 0 & -5 & -3 & -2 & 0 & 0 & 1 \end{array}\right] \rightarrow$$

$$\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -4 & -3 & -2 & 1 & 0 & 0 \\ 0 & -3 & -5 & -2 & 0 & 1 & 0 \\ 0 & -5 & -3 & -2 & 0 & 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & -3 & -2 & 1 & 0 & 0 \\ 0 & 2 & -5 & -2 & 0 & 1 & 0 \\ 0 & -2 & -3 & -2 & 0 & 0 & 1 \end{array}\right] \rightarrow$$

$$\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & -3 & -2 & 1 & 0 & 0 \\ 0 & 0 & -11 & -6 & 2 & 1 & 0 \\ 0 & 0 & 3 & 2 & -2 & 0 & 1 \end{array}\right] \rightarrow \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & -11 & -6 & 2 & 1 & 0 \\ 0 & 0 & 3 & 2 & -2 & 0 & 1 \end{array}\right] \rightarrow$$

$$\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & -1 & 0 & -2 & 1 & 0 & 0 \\ 0 & 0 & 1 & 2 & -6 & 1 & 4 \\ 0 & 0 & 3 & 2 & -2 & 0 & 1 \end{array}\right] \rightarrow \underbrace{\left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{array}\right]}_{D} \underbrace{\left|\begin{array}{cccc} 1 & 0 & 0 & 0 \\ -2 & 1 & 0 & 0 \\ 2 & -6 & 1 & 4 \\ -4 & 16 & -3 & -11 \end{array}\right]}_{L^{-1}}$$

Testeri su sledeći:

$$g_1^*(y_1, y_2, y_3, y_4) = g_2^*(y_1, y_2, y_3, y_4) = g_3^*(y_1, y_2, y_3, y_4) = 0$$

$$f_4(y_1, y_2, y_3, y_4) = (0, 0, 0, 1)L^{-1}(y_1, y_2, y_3, y_4)^T = -4y_1 + 16y_2 - 3y_3 - 11y_4$$

Dakle, kompletan skup testera je $\{f_4\}$.

4.3 Veza između testera i minora matrice A

U ovom delu pokazaćemo neke veze minora matrice A i egzistencije kompletnog skupa testera. U Teoremi 4.3.5 ćemo dokazati egzistenciju kompletnog skupa testera matrice A nad $\mathbb{Z}$ i $\mathbb{Z}_d$, gde je d najveći zajednički delilac svih $r \times r$ minora matrice A (r je rang matrice A).

U ovom delu koristićemo sledeće oznake:

- Neka je $r = rang(A)$ gde koeficijenti matrice A pripadaju prstenu $\mathbb{Z}$.
- Neka je d najveći zajednički delilac svih $r \times r$ minora matrice A.
- Neka je B $r \times r$ minor matrice A:

$$B = \left|\begin{array}{ccc} a_{11} & \dots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \dots & a_{rr} \end{array}\right|$$

  Pretpostavićemo da je $B \neq 0$ (ovo možemo dobiti transformacijama na vrstama i kolonama matrice A, jer ako je $r = rang(A)$ onda mora postojati minor reda $r \times r$ koji je različit od nule).

- Neka je B_{jk} (gde $j \in \{1, \dots, r\}$ i $k \in \{1, \dots, M\}$) sledeći $r \times r$ minor matrice A:

$$B_{jk} = \left|\begin{array}{ccccccc} a_{11} & \dots & a_{1,j-1} & a_{1k} & a_{1,j+1} & \dots & a_{1r} \\ a_{21} & \dots & a_{2,j-1} & a_{2k} & a_{2,j+1} & \dots & a_{2r} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & \dots & a_{r,j-1} & a_{rk} & a_{r,j+1} & \dots & a_{rr} \end{array}\right|.$$

- Neka je A_{ij} (gde $i \in \{1, \ldots, r\}$ i $j \in \{1, \ldots, r\}$ sledeći minor:

$$A_{ij} = \begin{vmatrix} a_{11} & \ldots & a_{1,j-1} & a_{1,j+1} & \ldots & a_{1r} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{i-1,1} & \ldots & a_{i-1,j-1} & a_{i-1,j+1} & \ldots & a_{i-1,r} \\ a_{i+1,1} & \ldots & a_{i+1,j-1} & a_{i+1,j+1} & \ldots & a_{i+1,r} \\ \vdots & & \vdots & \vdots & & \vdots \\ a_{r1} & \ldots & a_{r,j-1} & a_{r,j+1} & \ldots & a_{rr} \end{vmatrix}.$$

Sledeće teoreme nam govore o povezanosti determinanata B_{jk} i A_{ij}.

Teorema 4.3.1 *$\forall j \in \{1, \ldots, r\}$ $\forall k \in \{1, \ldots, M\}$ važi:*

$$B_{jk} = (-1)^{k+1} A_{1j} a_{1k} + (-1)^{k+2} A_{2j} a_{2k} + \ldots + (-1)^{k+r} A_{rj} a_{rk}$$

Dokaz. Sledi iz Teoreme 1.3.7 i definicije determinanata B_{jk} i A_{ij}.

□

Teorema 4.3.2 *$\forall j \in \{1, \ldots, r\}$ $\forall k \in \{1, \ldots, M\}$ važi:*

$$(B_{jk} \bmod d) = 0.$$

Dokaz. Razmatraćemo sledeće slučajeve:

- (Slučaj $k = j$) Važi $B_{jk} = B_{jj} = B$. Pošto je $B \bmod d = 0$, sledi:

$$B_{jk} \bmod d = 0.$$

- (Slučaj $k > r$) Vrednost minora B_{jk} je jednaka vrednosti $r \times r$ minora (onog koji sadrži kolone $1, \ldots, j-1, j+1, \ldots, r, k$), a d je najveći zajednički delilac svih takvih minora. Zbog toga:

$$B_{jk} \bmod d = 0.$$

- (Slučaj $1 \leq k \leq r$ i $k \neq j$) Tada je $B_{jk} = 0$ (sledi iz Teoreme 1.3.4 jer B_{jk} ima dve kolone jednake). Zato

$$B_{jk} \bmod d = 0.$$

□

U nastavku ćemo definisati skup funkcija (Definicija 4.3.1), zatim pokazati da je to skup testera (Teorema 4.3.4), a u Teoremi 4.3.5 pokazati kompletnost ovog skupa testera. Sledeća teorema je neophodna za definisanje ovog skupa funkcija:

Teorema 4.3.3 *Ako je* $k \in \{r+1, \ldots, N\}$ *tada* $\exists\, m_{k1}, \ldots, m_{kr}, m_{kk} \in \mathbb{Z}$ *tako da je:*

$$\begin{array}{l} m_{k1}a_{11} + \ldots + m_{kr}a_{r1} + m_{kk}a_{k1} = 0 \\ m_{k1}a_{12} + \ldots + m_{kr}a_{r2} + m_{kk}a_{k2} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ m_{k1}a_{1M} + \ldots + m_{kr}a_{rM} + m_{kk}a_{kM} = 0 \end{array}.$$

Dokaz. Pošto je $r = rang(A)$, to znači da matrica A ima r linearno nezavisnih vrsta (kolona), pa je onda skup vektora nad poljem $\mathbb{Q}$ $\{(a_{11}, \ldots, a_{1M}), \ldots, (a_{r1}, \ldots, a_{rM}), (a_{k1}, \ldots, a_{kM})\}$ linearno zavisan. Zbog toga, postoje $q_1, \ldots, q_r, q_k \in \mathbb{Q}$ takvi da:

$$q_1(a_{11}, \ldots, a_{1M}) + \ldots + q_r(a_{r1}, \ldots, a_{rM}) + q_k(a_{k1}, \ldots, a_{kM}) = (0, \ldots, 0).$$

Neka je $q_i = \frac{n_i}{d_i}$, gde $d_i, n_i \in \mathbb{Z}$ i $d_i \neq 0$. Tada imamo:

$$\frac{n_1}{d_1}(a_{11}, \ldots, a_{1M}) + \ldots + \frac{n_r}{d_r}(a_{r1}, \ldots, a_{rM}) + \frac{n_k}{d_k}(a_{k1}, \ldots, a_{kM}) = (0, \ldots, 0) \Big/ d_1 \cdots d_r d_k$$

Definišemo $m_{ki} = n_i d_k \prod_{j=1, j\neq i}^{r} d_j \in \mathbb{Z}$ za svako $i \in \{1, \ldots, r\}$ i $m_{kk} = n_1 d_1 \cdots d_r \in \mathbb{Z}$.
Prethodni izraz je ekvivalentan sledećem:

$$m_{k1}(a_{11}, \ldots, a_{1M}) + \ldots + m_{kr}(a_{r1}, \ldots, a_{rM}) + m_{kk}(a_{k1}, \ldots, a_{kM}) = (0, \ldots, 0).$$

Zbog toga je

$$\begin{array}{l} m_{k1}a_{11} + \ldots + m_{kr}a_{r1} + m_{kk}a_{k1} = 0 \\ m_{k1}a_{12} + \ldots + m_{kr}a_{r2} + m_{kk}a_{k2} = 0 \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ m_{k1}a_{1M} + \ldots + m_{kr}a_{rM} + m_{kk}a_{kM} = 0 \end{array}$$

što je i trebalo pokazati.

□

Definicija 4.3.1 *Definišemo sledeće funkcije:*

(i) *Funkcije* $g_k : \mathbb{Z}^N \longrightarrow \mathbb{Z}_d$ *gde* $k \in \{1, \ldots, r\}$, *kao što sledi:*

$$g_k(y_1, \ldots, y_N) = A_{1k}y_1 - A_{2k}y_2 + \ldots + (-1)^{r-1}A_{rk}y_r \bmod d$$

(ii) *Funkcije* $f_k : \mathbb{Z}^N \longrightarrow \mathbb{Z}$ *gde* $k \in \{r+1, \ldots, N\}$:

$$f_k(y_1, \ldots, y_N) = m_{k1}y_1 + \ldots + m_{kr}y_r + m_{kk}y_k$$

gde $m_{k1}, \ldots, m_{kr}, m_{kk} \in \mathbb{Z}$ *ispunjavaju uslove Teoreme 4.3.3.*

Sada dokazujemo da su funkcije iz prethodne definicije testeri.

Teorema 4.3.4 *Važi sledeće:*

(i) *Ako je* $k \in \{1, \ldots, r\}$, *funkcija* g_k *je tester u* $\mathbb{Z}_d$ *matrice* A.

(ii) *Ako je* $k \in \{r+1, \ldots, N\}$, *funkcija* f_k *je tester u* $\mathbb{Z}$ *matrice* A.

Dokaz.

(i) Imamo da je:

$$g_k(y_1, \ldots, y_N) = A_{1k}y_1 - A_{2k}y_2 + \ldots + (-1)^{r-1}A_{rk}y_r \bmod d.$$

Zbog toga, funkcija g_k ispunjava uslove (i) i (ii) iz Definicije 3.3.1. Prema Teoremi 4.3.1, važi:

$$g_k(a_{11}, \ldots, a_{N1}) = A_{1k}a_{11} - A_{2k}a_{21} + \ldots + (-1)^{r-1}A_{rk}a_{r1} \bmod d = B_{k1}$$

$$g_k(a_{12}, \ldots, a_{N2}) = A_{1k}a_{12} - A_{2k}a_{22} + \ldots + (-1)^{r-1}A_{rk}a_{r2} \bmod d = -B_{k2}$$

$$\ldots$$

$$g_k(a_{1M}, \ldots, a_{NM}) = A_{1k}a_{1M} + \ldots + (-1)^{r-1}A_{rk}a_{rM} \bmod d = (-1)^{M+1}B_{kM}$$

Zbog Teoreme 4.3.2 sledi:

$$g_k(a_{11}, \ldots, a_{N1}) = g_k(a_{21}, \ldots, a_{N2}), \ldots, g_k(a_{1M}, \ldots, a_{NM}) = 0.$$

To znači da funkcija g_k ispunjava i uslov (iii) iz Definicije 3.3.1. Dakle, g_k je tester.

(ii) Imamo da je:

$$f_k(y_1, \ldots, y_N) = m_{k1}y_1 + \ldots + m_{kr}y_r + m_{kk}y_k$$

Zbog toga, funkcija f_k ispunjava uslove (i) i (ii) iz Definicije 3.3.1. Pošto je funkcija f definisana tako da $m_{k1}, \ldots, m_{kr}$ i m_{kk} zadovoljavaju uslove Teoreme 4.3.3, imamo da je:

$$f_k(a_{11}, \ldots, a_{N1}) = f_k(a_{21}, \ldots, a_{N2}), \ldots, f_k(a_{1M}, \ldots, a_{NM}) = 0.$$

To znači da funkcija f_k zadovoljava uslov (iii) iz Definicije 3.3.1, pa je f_k tester.

□

Pre nego što pokažemo da je $\{g_1, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ kompletan skup testera, dokazaćemo sledeću lemu:

Lema 4.3.1 *Neka* $y_1, \ldots, y_n \in \mathbb{Z}$. *Ako*

$g_1(y_1, \ldots, y_N) = \ldots = g_r(y_1, \ldots, y_N) = f_{r+1}(y_1, \ldots, y_N) = \ldots = f_N(y_1, \ldots, y_N) = 0$

onda sistem (3.1) ima rešenje koje odgovara $\frac{B}{d}(y_1, \ldots, y_N)$.

Dokaz. Uzimajući $k \in \{1, \ldots, r\}$, definišemo:

$$x_k^* = \frac{(-1)^{k+1} A_{1k} y_1 + \ldots + (-1)^{k+r} A_{rk} y_r}{d}$$

Važi sledeće:

(i) Pošto $\forall k \in \{1, \ldots, r\}\ 0 = g_k(y_1, \ldots, y_N) = A_{1k} y_1 - A_{2k} y_2 + \ldots + (-1)^{r-1} A_{rk} y_r \bmod d$, sledi da $\forall k \in \{1, \ldots, r\}\ x_k^* \in \mathbb{Z}$.

(ii) Sledeće, pokazaćemo da $(x_1^*, \ldots, x_r^*, 0, \ldots, 0)$ zadovoljava prvih r jednačina sistema (3.1) koji odgovara $\frac{B}{d}(y_1, \ldots, y_N)$.
Zaista, x_k^* možemo izraziti kao:

$$x_k^* = \frac{\begin{vmatrix} a_{11} & \ldots & a_{1,k-1} & y_1 & a_{1,k+1} & \ldots & a_{1r} \\ a_{21} & \ldots & a_{2,k-1} & y_2 & a_{2,k+1} & \ldots & a_{2r} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & \ldots & a_{r,k-1} & y_r & a_{r,k+1} & \ldots & a_{rr} \end{vmatrix}}{d}$$

$$= \frac{B \cdot \begin{vmatrix} a_{11} & \ldots & a_{1,k-1} & y_1 & a_{1,k+1} & \ldots & a_{1r} \\ a_{21} & \ldots & a_{2,k-1} & y_2 & a_{2,k+1} & \ldots & a_{2r} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & \ldots & a_{r,k-1} & y_r & a_{r,k+1} & \ldots & a_{rr} \end{vmatrix}}{Bd}$$

$$= \frac{B \cdot \begin{vmatrix} a_{11} & \ldots & a_{1,k-1} & \frac{By_1}{d} & a_{1,k+1} & \ldots & a_{1r} \\ a_{21} & \ldots & a_{2,k-1} & \frac{By_2}{d} & a_{2,k+1} & \ldots & a_{2r} \\ \vdots & & \vdots & \vdots & \vdots & & \vdots \\ a_{r1} & \ldots & a_{r,k-1} & \frac{By_r}{d} & a_{r,k+1} & \ldots & a_{rr} \end{vmatrix}}{\begin{vmatrix} a_{11} & \ldots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \ldots & a_{rr} \end{vmatrix}}$$

Na ovaj način, pomoću Kramerovog pravila, $(x_1^*, \ldots, x_r^*)$ je rešenje linearnog sistema jednačina:

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1r} \\ \vdots & \vdots & \ddots & \vdots \\ a_{r1} & a_{r2} & \ldots & a_{rr} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_r \end{bmatrix} = \begin{bmatrix} \frac{By_1}{d} \\ \vdots \\ \frac{By_r}{d} \end{bmatrix}$$

Zbog toga, $(x_1^*, \ldots, x_r^*, 0, \ldots, 0)$ zadovoljava prvih r jednačina sistema (3.1) koji odgovara $\frac{B}{d}(y_1, \ldots, y_N)$.

(iii) Sledeće, pokazaćemo da $(x_1^*, \ldots, x_r^*, 0, \ldots, 0)$ zadovoljava poslednjih $N - r$ jednačina sistema (3.1) koje odgovara $\frac{B}{d}(y_1, \ldots, y_N)$.
Neka je $k \in \{r+1, \ldots, N\}$.

$$0 = f_k(y_1, \ldots, y_N) = \frac{Bf_k(y_1, \ldots, y_N)}{d} = \frac{B(m_{k1}y_1 + \ldots + m_{kr}y_r + m_{kk}y_k)}{d}$$

$$= m_{k1}\frac{By_1}{d} + \ldots + m_{kr}\frac{By_r}{d} + m_{kk}\frac{By_k}{d}$$

Kao što smo videli u prethodnoj stavci, $(x_1^*, \ldots, x_r^*, 0, \ldots, 0)$ zadovoljava prvih r jednačina sistema (3.1) koji odgovara $\frac{B}{d}(y_1, \ldots, y_N)$. Zbog toga, imamo:

$$0 = m_{k1}(a_{11}x_1^* + \ldots + a_{1r}x_r^*) + \ldots + m_{kr}(a_{r1}x_1^* + \ldots + a_{rr}x_r^*) + m_{kk}\frac{By_k}{d}$$

$$= x_1^*(m_{k1}a_{11} + \ldots + m_{kr}a_{r1}) + \ldots + x_r^*(m_{k1}a_{1r} + \ldots + m_{kr}a_{rr}) + m_{kk}\frac{By_k}{d}$$

Kako je f_k definisano da zadovoljava uslove Teoreme 4.3.3, imamo:

$$0 = -(m_{kk}a_{k1}x_1^* + \ldots + m_{kk}a_{kr}x_r^*) + m_{kk}\frac{By_k}{d}$$

$$= -m_{kk}(a_{k1}x_1^* + \ldots + a_{kr}x_r^*) + m_{kk}\frac{By_k}{d}$$

Kako je $m_{kk} \neq 0$, $(x_1^*, \ldots, x_r^*, 0, \ldots, 0)$ zadovoljava k-tu jednačinu sistema (3.1) koji odgovara $\frac{B}{d}(y_1, \ldots, y_N)$:

$$a_{k1}x_1^* + \ldots + a_{kr}x_r^* = \frac{By_k}{d}$$

odakle sledi traženo.

□

U sledećoj teoremi dokazujemo da je $\{g_1, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ kompletan skup testera.

Teorema 4.3.5 *Skup $\{g_1, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ je kompletan skup testera matrice A. Odnosno:*
Sistem jednačina (3.1) ima rešenje koje odgovara $y_1, \ldots, y_N \in \mathbb{Z}$

$$\Leftrightarrow$$

$$g_1(y_1, \ldots, y_N) = \ldots = g_r(y_1, \ldots, y_N) = f_{r+1}(y_1, \ldots, y_N) = \ldots = f_N(y_1, \ldots, y_N) = 0.$$

Dokaz. $\Rightarrow$) Sledi direktno iz Teoreme 3.3.1.
$\Leftarrow$) Kako je d najveći zajednički delilac svih $r \times r$ minora matrice A, možemo pronaći $|B_1|, \ldots, |B_s|$, $r \times r$ minore matrice A, tako da:

$$d = \lambda_1 |B_1| + \ldots + \lambda_s |B_s|$$

Zbog Leme 4.3.1, $\exists\, x_{1i}, \ldots, x_{Mi} \in \mathbb{Z}$, $i \in \{1, \ldots, s\}$, takvi da:

$$A(x_{1i}, \ldots, x_{Mi})^T = \frac{|B_i|}{d}(y_1, \ldots, y_N)^T$$

Neka je $x_k^* = \lambda_1 x_{k1} + \ldots + \lambda_s x_{ks}$, gde $k \in \{1, \ldots, M\}$.
Sada ćemo pokazati da je $(x_1^*, \ldots, x_M^*)$ rešenje sistema (3.1) koje odgovara $(y_1, \ldots, y_N)$.

$$\begin{aligned} A(x_1^*, \ldots, x_M^*)^T &= \lambda_1 \frac{|B_1|}{d}(y_1, \ldots, y_N)^T + \ldots + \lambda_s \frac{|B_s|}{d}(y_1, \ldots, y_N)^T \\ &= (y_1, \ldots, y_N)^T \frac{\lambda_1 |B_1| + \ldots + \lambda_s |B_s|}{d} \\ &= (y_1, \ldots, y_N)^T \frac{d}{d} = (y_1, \ldots, y_N)^T \end{aligned}$$

□

4.4 Nalaženje kompletnog skupa testera

U prethodnom delu smo pokazali kako uvek možemo odrediti da li sistem linearnih Diofantovih jednačina ima rešenje koje odgovara $(y_1, \ldots, y_N)$ računajući kompletan skup testera. Ovaj skup testera možemo lako pronaći računajući Smitovu normalnu formu za matricu sistema A. Međutim, računanje Smitove normalne forme pomoću Gausovog postupka eliminacije nije lak posao i često dovodi do ogromnih računanja. Iako nam Teorema 4.3.5

pruža drugačiji način računanja kompletnog skupa testera, postupak računanja koji je opisan u dokazu ove teoreme uključuje veliko računanje. Naime, prvo je trebalo naći d, najveći zajednički delilac svih $r \times r$ minora matrice A. Ali, broj minora reda r matrice A je $\binom{N}{r} \cdot \binom{M}{r}$, što je nepolinomske složenosti. Uprkos tome, u ovom delu će postati očigledno da Teorema 4.3.5 može biti korisna za izbegavanje rada sa matricama ogromnih koeficijenata. Zaista, ovaj metod će biti baziran na operacijama vrsta i kolona matrice u prstenu $\mathbb{Z}_m$ umesto u prstenu $\mathbb{Z}$. Pošto su ulazne veličine matrice (njeni koeficijenti) u $\mathbb{Z}_m = \{0, 1, \ldots, m-1\}$ onda više nije moguć ogroman rast ulaznih veličina matrice.

4.4.1 Računanje kompletnog skupa testera za proizvoljnu matricu

Prema Teoremi 4.3.5, postoji kompletan skup testera definisan u $\mathbb{Z}$ i u $\mathbb{Z}_d$. Možemo pokušati pronaći testere definisane u $\mathbb{Z}$, pomoću Definicije 3.3.1. Na osnovu ove definicije, tester f u $\mathbb{Z}$ je oblika:

$$f(y_1, \ldots, y_N) = \alpha_1 y_1 + \ldots + \alpha_N y_N$$

gde $\alpha_1, \ldots, \alpha_N \in \mathbb{Z}$ i važi uslov (3.3).

Na ovaj način, svako rešenje $(\alpha_1, \ldots, \alpha_N)$ u (3.3) označava tester u $\mathbb{Z}$. Pošto je $rang(A) = rang(A^T) = r$, postoji $N - r$ linearno nezavisnih rešenja u (3.3) (uzimajući u obzir da radimo u polju $\mathbb{Q}$) koji daju $N - r$ testera u $\mathbb{Z}$. Bilo koji drugi tester u $\mathbb{Z}$ može se predstaviti kao linearna kombinacija ovih $N - r$ testera.

Na isti način, možemo lako pronaći testere u $\mathbb{Z}_m$, gde je m proizvoljan prirodan broj. Prema Definiciji 3.3.1, tester g u $\mathbb{Z}_m$ je oblika:

$$g(y_1, \ldots, y_N) = (\alpha_1 y_1 + \ldots + \alpha_N y_N) \bmod m$$

gde $\alpha_1, \ldots, \alpha_N \in \mathbb{Z}$, i važi sledeće:

$$\underbrace{\begin{bmatrix} a_{11} \bmod m & \ldots & a_{N1} \bmod m \\ \vdots & \ddots & \vdots \\ a_{1M} \bmod m & \ldots & a_{NM} \bmod m \end{bmatrix}}_{A^T \bmod m} \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix} \bmod m. \tag{4.1}$$

Nalaženjem skupa generatora rešenja (3.3) i skupa generatora rešenja (4.1) (gde je $m = d$ najveći zajednički delilac svih $r \times r$ minora matrice A), dobijamo kompletan skup testera za matricu A.

Iako određivanje vrednosti d može dovesti do komplikovanog računa, sledeća teorema daje rezultat pomoću kojeg bismo lakše izračunali kompletan skup testera.

Teorema 4.4.1 *Neka je $r = rang(A)$. Neka je d najveći zajednički delilac svih $r \times r$ minora matrice A. Neka $m \in \mathbb{N}$ takav da $d \,|\, m$.*

Postoji kompletan skup testera u $\mathbb{Z}$ i $\mathbb{Z}_m$.

Dokaz. Neka je $\{g_1, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ kompletan skup testera matrice A tako da su $g_1, \ldots, g_r$ testeri definisani u $\mathbb{Z}_d$, i $f_{r+1}, \ldots, f_N$ testeri definisani u $\mathbb{Z}$. Kako $d \,|\, m$, imamo da je $m = d \cdot k$ za neko $k \in \mathbb{N}$.
Neka su testeri g_i, $i \in \{1, \ldots, r\}$, definisani na sledeći način:

$$g_i(y_1, \ldots, y_N) = \alpha_{i1}y_1 + \ldots + \alpha_{iN}y_N \bmod d$$

Definišemo funkcije g_i^* na sledeći način:

$$g_i^*(y_1, \ldots, y_N) = k \cdot (\alpha_{i1}y_1 + \ldots + \alpha_{iN}y_N) \bmod m$$

Pošto je $g_i(y_1, \ldots, y_N) = 0 \Leftrightarrow g_i^*(y_1, \ldots, y_N) = 0$, onda je skup funkcija $\{g_1^*, \ldots, g_r^*, f_{r+1}, \ldots, f_N\}$ kompletan skup testera matrice A.

□

U prethodnoj teoremi, kompletan skup testera matrice A smo odredili tako što smo našli generatorni skup rešenja za (3.3) i generatorni skup rešenja za (4.1), gde je m umnožak od d (m čak može biti i minor reda r matrice A). U Teoremi 1.5.5 pokazali smo kako se svaka matrica može transformisati u stepenastu matricu za koju lako određujemo rang. Na taj način, matricu A^T možemo transformisati u sledeću stepenastu matricu B^T :

$$B^T = \begin{bmatrix} a_1 & c_{12} & c_{13} & \ldots & c_{1,r-2} & c_{1,r-1} & c_{1r} & \ldots & c_{1n} \\ 0 & a_2 & c_{23} & \ldots & c_{2,r-2} & c_{2,r-1} & c_{2r} & \ldots & c_{2n} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & a_{r-1} & c_{r-1,r} & \ldots & c_{r-1,N} \\ 0 & 0 & 0 & \ldots & 0 & 0 & b_1 & \ldots & b_{N-r+1} \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 & 0 & \ldots & 0 \end{bmatrix}$$

gde je $\forall i \in \{1, \ldots, r-1\}$ $a_i \neq 0$ i $b_1 \neq 0$. Za matricu B^T lako određujemo $rang(B) = rang(A)$, i umnožak od d,

$$m = NZD(a_1a_2 \cdots a_{r-1}b_1, a_1a_2 \cdots a_{r-1}b_2, \ldots, a_1a_2 \cdots a_{r-1}b_{N-r+1})$$

$= a_1 a_2 \cdots a_{r-1} \cdot NZD(b_1, \ldots, b_{N-r+1})$

Osim toga, pomoću matrice B^T lako dobijamo testere matrice A u $\mathbb{Z}$. Testere u $\mathbb{Z}_m$ dobijamo pronalaženjem generatornog skupa rešenja (4.1). U sledećem delu ćemo proučavati kako da dobijemo ovaj generatorni skup rešenja.

Primer 4.4.1 Posmatrajmo sledeću matricu:

$$A = \begin{bmatrix} 1 & 3 & 3 \\ 2 & 0 & -1 \\ 2 & -1 & 1 \\ 2 & 1 & -1 \end{bmatrix}$$

Gausovim postupkom eliminacije, transformišemo matricu A^T u trougaonu matricu B^T:

$$\underbrace{\begin{bmatrix} 1 & 2 & 2 & 2 \\ 3 & 0 & -1 & 1 \\ 3 & -1 & 1 & -1 \end{bmatrix}}_{A^T} \sim \begin{bmatrix} 1 & 2 & 2 & 2 \\ 0 & -6 & -7 & -5 \\ 0 & -7 & -5 & -7 \end{bmatrix} \sim \begin{bmatrix} 1 & 2 & 2 & 2 \\ 0 & -6 & -7 & -5 \\ 0 & 0 & \frac{19}{6} & -\frac{7}{6} \end{bmatrix} \sim$$

$$\sim \underbrace{\begin{bmatrix} 1 & 2 & 2 & 2 \\ 0 & -6 & -7 & -5 \\ 0 & 0 & 19 & -7 \end{bmatrix}}_{B^T}$$

Prvu vrstu matrice A^T pomnožimo sa -3 i dodamo drugoj i trećoj vrsti. U sledećem koraku drugu vrstu pomnožimo sa $-\frac{7}{6}$ i dodamo trećoj vrsti. U poslednjem koraku, treću vrstu pomnožimo sa 6. Pomoću matrice B^T, određujemo rang matrice A ($rang(B^T) = rang(A^T) = rang(A) = 3$) i umnožak od d ($m = 1 \cdot 6 \cdot NZD(19, 7) = 6$).
Da bismo pronašli generatorni skup testera u $\mathbb{Z}$, rešavamo sledeći sistem jednačina:

$$\underbrace{\begin{bmatrix} 1 & 2 & 2 & 2 \\ 0 & -6 & -7 & -5 \\ 0 & 0 & 19 & -7 \end{bmatrix}}_{B^T} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Odnosno:

$$\begin{aligned} \alpha_1 + 2\alpha_2 + 2\alpha_3 + 2\alpha_4 &= 0 \\ -6\alpha_2 - 7\alpha_3 - 5\alpha_4 &= 0 \\ 19\alpha_3 - 7\alpha_4 &= 0 \end{aligned}$$

Ako stavimo da je $\alpha_4 = a$, gde je $a = 19 \cdot t$ i t je proizvoljan ceo broj (a je ovakvog oblika jer radimo sa celobrojnim matricama, a rešenja sistema su takođe celi brojevi), onda je rešenje sistema:

$$RS = \Big\{ \Big(-\frac{4}{19} \cdot a, -\frac{24}{19} \cdot a, \frac{7}{19} \cdot a, a \Big) \Big| \, a = 19 \cdot t, \, t \in \mathbb{Z} \Big\}.$$

Kako je $rang(A) = 3$, onda je $N - rang(A) = 4 - 3 = 1$. To znači da se baza generatornog skupa testera u $\mathbb{Z}$ sastoji od jednog testera. Ako uzmemo da je $t = 1$, onda je tester u $\mathbb{Z}$ oblika:

$$f(y_1, \ldots, y_N) = -4y_1 - 24y_2 + 7y_3 + 19y_4$$

Primer 4.4.2 Posmatrajmo sledeću matricu:

$$A = \begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 3 \\ 0 & 2 & 2 & 2 \end{bmatrix}$$

Gausovim postupkom eliminacije, transformišemo matricu A^T u trougaonu matricu B^T:

$$\underbrace{\begin{bmatrix} 2 & 1 & 1 & 0 \\ 1 & 0 & 1 & 2 \\ 3 & 1 & 2 & 2 \\ 5 & 2 & 3 & 2 \end{bmatrix}}_{A^T} \sim \begin{bmatrix} 1 & 0 & 1 & 2 \\ 2 & 1 & 1 & 0 \\ 3 & 1 & 2 & 2 \\ 5 & 2 & 3 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & -4 \\ 0 & 1 & -1 & -4 \\ 0 & 2 & -2 & -8 \end{bmatrix} \sim \underbrace{\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & -4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}}_{B^T}$$

U matrici A^T najpre zamenimo prvu i drugu vrstu. U sledećem koraku prvu vrstu novodobijene matrice pomnožimo sa -2 i dodamo drugoj vrsti, sa -3 i dodamo trećoj i sa -5 i dodamo četvrtoj vrsti. Konačno, drugu vrstu pomnožimo sa -1 i dodamo trećoj, a sa -2 i dodamo četvrtoj vrsti. Dobili smo matricu B^T ranga 2. Umnožak od d je $m = 1 \cdot NZD\{1, -1, -4\} = 1$. Dakle, generatorni skup testera u $\mathbb{Z}$ čine dva testera, a dobijamo ih rešavajući sledeći sistem jednačina:

$$\begin{bmatrix} 1 & 0 & 1 & 2 \\ 0 & 1 & -1 & -4 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix} \cdot \begin{bmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \\ \alpha_4 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \\ 0 \end{bmatrix}$$

Odnosno:

$$\begin{aligned} \alpha_1 + \alpha_3 + 2\alpha_4 &= 0 \\ \alpha_2 - \alpha_3 - 4\alpha_4 &= 0 \\ 0 &= 0 \\ 0 &= 0 \end{aligned}$$

Ako uzmemo da je $\alpha_3 = a$ i $\alpha_4 = b$, gde su a i b proizvoljni celi brojevi, onda je rešenje sistema:

$$RS = \{(-a - 2b, a + 4b, a, b) | a, b \in \mathbb{Z}\}.$$

Baza ovog generatornog skupa testera je $\{(-3, 5, 1, 1), (-2, 4, 0, 1)\}$. Rešenje $\alpha_1 = -3$; $\alpha_2 = 5$; $\alpha_3 = 1$; $\alpha_4 = 1$ odgovara sledećem testeru u $\mathbb{Z}$:

$$f_1(y_1, \ldots, y_N) = -3y_1 + 5y_2 + y_3 + y_4,$$

a rešenje $\alpha_1 = -2$; $\alpha_2 = 4$; $\alpha_3 = 0$; $\alpha_4 = 1$ odgovara:

$$f_2(y_1, \ldots, y_N) = -2y_1 + 4y_2 + y_4.$$

4.4.2 Računanje testera u $\mathbb{Z}_m$

U ovom delu proučavamo kako odrediti testere matrice A po modulu m (gde je m proizvoljan prirodan broj).

Najpre, razmotrićemo slučaj kada je A dijagonalna matrica.

Lema 4.4.1 *Neka je $A = diag(a_1, \ldots, a_r, 0, \ldots, 0)$ dijagonalna matrica tipa $N \times M$.*
Neka su g_i, $i \in \{1, \ldots, N\}$, sledeći testeri definisani u $\mathbb{Z}_m$:

$$g_i(y_1, \ldots, y_N) = k_i \cdot y_i \bmod m$$

gde

$$k_i = \begin{cases} 0, & 1 \leq i \leq r \text{ i } NZD(a_i, m) = 1 \\ \frac{m}{NZD(a_i, m)}, & 1 \leq i \leq r \text{ i } NZD(a_i, m) \neq 1 \\ 1, & r + 1 \leq i \leq N \end{cases}$$

Tada važi:

$$\{g_1, \ldots, g_N\} \text{ je generatorni skup testera matrice } A \text{ u } \mathbb{Z}_m$$

gde

- *g_i je definisana na sledeći način ($1 \leq i \leq r$ i $NZD(a_i, m) \neq 1$) :*

$$g_i(y_1, \ldots, y_N) = \frac{m}{NZD(a_i, m)} y_i \bmod m$$

- *g_i je definisana na sledeći način ($r + 1 \leq i \leq N$) :*

$$g_i(y_1, \ldots, y_N) = y_i \bmod m.$$

Dokaz. Neka je f tester u $\mathbb{Z}_m$. Prema definiciji testera,

$$f = \alpha_1 y_1 + \ldots + \alpha_r y_r + \alpha_{r+1} y_{r+1} + \ldots + \alpha_N y_N \bmod m$$

je tester matrice A u $\mathbb{Z}_m$ ako i samo ako:

$$\underbrace{\begin{bmatrix} a_1 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ 0 & a_2 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & a_r & 0 & \ldots & 0 \\ 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 0 & 0 & \ldots & 0 \end{bmatrix}}_{A^T} \cdot \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_r \\ \alpha_{r+1} \\ \vdots \\ \alpha_N \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \\ \vdots \\ 0 \end{bmatrix} \bmod m$$

Odnosno, imamo da je:

$$a_1\alpha_1 = 0 \bmod m$$
$$a_2\alpha_2 = 0 \bmod m$$
$$\ldots$$
$$a_r\alpha_r = 0 \bmod m$$

U slučaju da je $1 \leq i \leq r$ i $NZD(a_i, m) = 1$, imamo da je $a_i\alpha_i = 0 \bmod m$, i zato je:

$$\alpha_i = 0 \bmod m$$

U slučaju da je $1 \leq i \leq r$ i $NZD(a_i, m) \neq 1$, imamo da $\exists\, \beta_i \in \mathbb{Z}_m$ tako da:

$$\alpha_i = \beta_i \cdot \frac{m}{NZD(a_i, m)} \bmod m = \beta_i k_i \bmod m$$

Zbog toga je:

$$f = \sum_{i=1}^{r} \beta_i k_i y_i + \sum_{i=r+1}^{N} \alpha_i y_i = \sum_{i=1}^{r} \beta_i g_i + \sum_{i=r+1}^{N} \alpha_i g_i$$

Dakle, tester f smo izrazili kao linearnu kombinaciju testera g_i.

□

Lema 4.4.2 *Ako je A matrica tipa $N \times M$ nad prstenom $\mathbb{Z}$, onda možemo pronaći $N \times N$ matricu, L, i $M \times M$ matricu, R, i dijagonalnu matricu, D, tako da:*

$$A \bmod m = LDR \bmod m$$

Pored toga, $L \bmod m$ i $R \bmod m$ su invertibilne matrice u $\mathbb{Z}_m$.

Dokaz. Na osnovu Teoreme 2.3.2 o Smitovoj normalnoj formi, matricu A možemo napisati kao $A = LDR$, gde je L invertibilna $N \times N$ matrica, R invertibilna $M \times M$ matrica, i D je dijagonalna matrica. Zbog toga je

$$A \mod m = (LDR) \mod m = (L \mod m) \cdot (D \mod m) \cdot (R \mod m)$$

Pored toga, pošto su L i R invertibilne matrice, $L \cdot L^{-1} = I = R \cdot R^{-1}$, sledi:

$$(L \mod m) \cdot (L^{-1} \mod m) = (L \cdot L^{-1} \mod m) = I \mod m = I,$$

$$(R \mod m) \cdot (R^{-1} \mod m) = (R \cdot R^{-1} \mod m) = I \mod m = I.$$

□

Teorema 4.4.2 *Neka je A matrica tipa $N \times M$ takva da je $A \bmod m = LDR \bmod m$, gde su L i R invertibilne matrice i $D = (a_1, \ldots, a_r, 0, \ldots, 0)$ je dijagonalna matrica.*
Neka su g_i^*, $i \in \{1, \ldots, N\}$, sledeći testeri definisani u $\mathbb{Z}_m$:

$$g_1^*(\mathbf{y}) = k_1(1, 0, 0, \ldots, 0) \cdot L^{-1}\mathbf{y}^T \mod m$$

$$g_2^*(\mathbf{y}) = k_2(0, 1, 0, \ldots, 0) \cdot L^{-1}\mathbf{y}^T \mod m$$

$$\ldots$$

gde

$$k_i = \begin{cases} 0, & 1 \leq i \leq r \text{ i } NZD(a_i, m) = 1 \\ \frac{m}{NZD(a_i,m)}, & 1 \leq i \leq r \text{ i } NZD(a_i, m) \neq 1 \\ 1, & r+1 \leq i \leq N \end{cases}$$

Tada je $\{g_1^*, \ldots, g_N^*\}$ generatorni skup testera matrice A u $\mathbb{Z}_m$.

Dokaz. Imamo da je:
$g^*(\mathbf{y}) = \mathbf{z} \cdot \mathbf{y}^T \bmod m$ je tester matrice A u $\mathbb{Z}_m \Leftrightarrow$
$\mathbf{z} \cdot A = \mathbf{0} \bmod m \Leftrightarrow$
$\mathbf{z} \cdot LDR = \mathbf{0} \bmod m \Leftrightarrow$
$\mathbf{w} \cdot DR = \mathbf{0} \bmod m$, gde $\mathbf{w} = \mathbf{z}L \Leftrightarrow$
$g(\mathbf{y}) = \mathbf{w} \cdot \mathbf{y}^T \bmod m$ je tester matrice D.
Odnosno, uzimajući tester $g(\mathbf{y}) = \mathbf{w} \cdot \mathbf{y}^T \bmod m$ matrice D u $\mathbb{Z}_m$, dobijamo tester $g^*(\mathbf{y}) = \mathbf{w}L^{-1}\mathbf{y}^T \bmod m$ matrice A u $\mathbb{Z}_m$.
Zbog toga je $\{g_1, \ldots, g_N\}$ je generatorni skup testera matrice D u $\mathbb{Z}_m$, gde:
$g_1(\mathbf{y}) = \mathbf{w}_1\mathbf{y} \bmod m$, gde $\mathbf{w}_1 = k_1(1, 0, 0, \ldots, 0)$
$g_2(\mathbf{y}) = \mathbf{w}_2\mathbf{y} \bmod m$, gde $\mathbf{w}_2 = k_2(0, 1, 0, \ldots, 0)$

...
Skup $\{g_1^*, \ldots, g_N^*\}$ je generatorni skup testera matrice A u $\mathbb{Z}_m$, gde:

$$g_1^*(\mathbf{y}) = k_1(1,0,0,\ldots,0) \cdot L^{-1}\mathbf{y}^T \bmod m$$
$$g_2^*(\mathbf{y}) = k_2(0,1,0,\ldots,0) \cdot L^{-1}\mathbf{y}^T \bmod m$$
$$\ldots$$

□

Primer 4.4.3 Posmatrajmo matricu A iz Primera 4.4.1:

$$A = \begin{bmatrix} 1 & 3 & 3 \\ 2 & 0 & -1 \\ 2 & -1 & 1 \\ 2 & 1 & -1 \end{bmatrix}$$

U Primeru 4.4.1, izračunali smo da je $m = 6$ i našli smo matricu B^T:

$$B^T = \begin{bmatrix} 1 & 2 & 2 & 2 \\ 0 & -6 & -7 & -5 \\ 0 & 0 & 19 & -7 \end{bmatrix} = \underbrace{\begin{bmatrix} 1 & 0 & 0 \\ 2 & -6 & 0 \\ 2 & -7 & 19 \\ 2 & -5 & -7 \end{bmatrix}^T}_{B}$$

Računajući Smitovu normalnu formu matrice B, možemo izračunati testere matrice A definisane u $\mathbb{Z}_6$ (matrice A i B imaju iste testere):

$$\underbrace{\left[\begin{array}{ccc} 1 & 0 & 0 \\ 2 & 0 & 0 \\ 2 & -1 & 1 \\ 2 & 1 & -1 \end{array}\right.}_{B \bmod 6} \underbrace{\left.\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right]}_{E_4 \bmod 6} \to \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & -1 & 1 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right] \to$$

$$\left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 2 & 0 & 0 & 0 & 1 & 0 & 0 \\ 2 & -1 & 0 & 0 & 0 & 1 & 0 \\ 4 & 0 & 0 & 0 & 0 & 1 & 1 \end{array}\right] \to \left[\begin{array}{ccc|cccc} 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -2 & 1 & 0 & 0 \\ 0 & -1 & 0 & -2 & 0 & 1 & 0 \\ 0 & 0 & 0 & -4 & 0 & 1 & 1 \end{array}\right] \to$$

$$\underbrace{\left[\begin{array}{ccc} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{array}\right.}_{D \bmod 6} \underbrace{\left.\begin{array}{cccc} 1 & 0 & 0 & 0 \\ -2 & 0 & 1 & 0 \\ -2 & 1 & 0 & 0 \\ -4 & 0 & 1 & 1 \end{array}\right]}_{L^{-1} \bmod 6}$$

Imamo da je $k_1 = 0$; $k_2 = 0$; $k_3 = 1$; $k_4 = 1$. Dakle,

$g_1(y_1, y_2, y_3, y_4) = g_2(y_1, y_2, y_3, y_4) = 0$
$g_3(y_1, y_2, y_3, y_4) = (0, 0, 1, 0)L^{-1}(y_1, y_2, y_3, y_4)^T \bmod 6 = -2y_1 + y_2 \bmod 6$
$g_4(y_1, y_2, y_3, y_4) = (0, 0, 0, 1)L^{-1}(y_1, y_2, y_3, y_4)^T \bmod 6 = -4y_1 + y_3 + y_4 \bmod 6$

Primer 4.4.4 U Primeru 4.4.2, posmatrali smo matricu:

$$A = \begin{bmatrix} 2 & 1 & 3 & 5 \\ 1 & 0 & 1 & 2 \\ 1 & 1 & 2 & 3 \\ 0 & 2 & 2 & 2 \end{bmatrix}$$

i izračunali da je $m = 1$ što znači da je $d = 1$ i da postoji kompletan skup testera matrice A definisanih u $\mathbb{Z}$. U Primeru 4.4.2 smo pronašli testere f_1 i f_2 u $\mathbb{Z}$, što znači da oni čine kompletan skup testera matrice A.

4.4.3 Računanje testera u $\mathbb{Z}_p$

U slučaju da je m prost broj p, možemo i lakše i mnogo brže pronaći testere sistema (4.1) u $\mathbb{Z}_m = \mathbb{Z}_p$.

Već smo pokazali da svako rešenje $(\alpha_1, \ldots, \alpha_N)$ u (4.1) predstavlja tester u $\mathbb{Z}_p$. Kada je $m = p$ prost broj, $\mathbb{Z}_p$ je polje i možemo dobiti $N - rang(A^T \bmod p)$ linearno nezavisnih rešenja sistema (4.1) koji daju nezavisne testere u $\mathbb{Z}_p$. U prethodnoj glavi smo pokazali da su r testera od ovih $N - r$ testera u $\mathbb{Z}_p$ izvedeni iz testera u $\mathbb{Z}$, koji se smatraju beskorisnim, i zato nam nisu potrebni za građenje kompletnog skupa testera.

Sumirajući sve, lako pronalazimo testere u $\mathbb{Z}$ i $\mathbb{Z}_p$, gde je p prost broj. U sledećoj teoremi, pokazujemo kako, uz neke uslove, možemo dobiti kompletan skup testera u $\mathbb{Z}$ i u nekim specijalnim poljima, $\mathbb{Z}_p$.

Teorema 4.4.3 *Neka je $r = rang(A)$. Neka je d najveći zajednički delilac svih $r \times r$ minora matrice A.*

(i) *Ako je $d = p_1 \cdots p_q$, gde su $p_1, \ldots, p_q$ različiti prosti brojevi, onda postoji kompletan skup testera matrice A definisanih u prstenima $\mathbb{Z}, \mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_q}$.*

(ii) *Ako postoji $r \times r$ minor matrice A koji ima vrednost p, gde je p prost broj, onda postoji kompletan skup testera matrice A definisan u prstenima $\mathbb{Z}$ i $\mathbb{Z}_p$.*

(iii) *Ako postoji $r \times r$ minor matrice A koji ima vrednost 1, onda postoji kompletan skup testera matrice A definisan u $\mathbb{Z}$.*

(iv) *Ako je* $r = rang(A) = N$ *i postoji* $N \times N$ *minor matrice* A *vrednosti* 1, *onda sistem (3.1) uvek ima rešenje bez obzira na* $(y_1, \ldots, y_N)$.

Dokaz.

(i) Na osnovu Teoreme 4.3.5, postoji kompletan skup testera definisan u $\mathbb{Z}_d$ i $\mathbb{Z}$. Prema Kineskoj teoremi o ostacima, $\mathbb{Z}_d \simeq \mathbb{Z}_{p_1} \times \cdots \times \mathbb{Z}_{p_q}$. Zato, svaki tester definisan u $\mathbb{Z}_d$ može se prikazati kao q testera definisanih u $\mathbb{Z}_{p_1}, \ldots, \mathbb{Z}_{p_q}$, redom.

(ii) Kako $d \,|\, p$, prema Teoremi 4.4.1, postoji kompletan skup testera definisan u $\mathbb{Z}_p$ i $\mathbb{Z}$.

(iii) Zbog Teoreme 4.3.5, $\{g_1, \ldots, g_r, f_{r+1}, \ldots, f_N\}$ je kompletan skup testera, gde su $g_1, \ldots, g_r$ testeri u $\mathbb{Z}_d$ a $f_{r+1}, \ldots, f_N$ testeri u $\mathbb{Z}$. Pošto postoji $r \times r$ minor matrice A vrednosti 1, imamo da je $d = 1$. Kako je $g_i(y_1, \ldots, y_N) = \alpha_1 y_1 + \ldots + \alpha_N y_N \bmod 1 = 0$, $\{g_1, \ldots, g_r\}$ su beskorisni testeri. Dakle, $\{f_{r+1}, \ldots, f_N\}$ je kompletan skup testera definisanih u $\mathbb{Z}$.

(iv) Zbog Teoreme 4.3.5 (kako je $r = N$), $\{g_1, \ldots, g_N\}$ je kompletan skup testera u $\mathbb{Z}_d$. Kako postoji $r \times r$ minor matrice A vrednosti 1, imamo da je $d = 1$. Pošto je $g_i(y_1, \ldots, y_N) = \alpha_1 y_1 + \ldots + \alpha_N y_N \bmod 1 = 0$, prema Teoremi 4.2.2, imamo da sistem (3.1) ima rešenje koje odgovara $y_1, \ldots, y_N$.

□

Primer 4.4.5 U Primeru 3.5.2 posmatrali smo matricu:

$$A = \begin{bmatrix} -3 & 2 & 2 \\ 2 & -3 & 2 \\ 2 & 2 & -3 \end{bmatrix}$$

Zaključili smo da nema korisnih testera u $\mathbb{Z}$ i pronašli testere u $\mathbb{Z}_5$:

$$f_5^1(z_1, z_2, z_3) = (4z_1 + z_2) \bmod 5,$$

$$f_5^2(z_1, z_2, z_3) = (3z_1 + z_2 + z_3) \bmod 5.$$

Kako je $rang(A) = 2$ i postoji minor reda 2×2, $\begin{vmatrix} -3 & 2 \\ 2 & -3 \end{vmatrix} = 5$, a 5 je prost broj, na osnovu Teoreme 4.4.3 (ii) zaključujemo da je $\{f_5^1, f_5^2\}$ kompletan skup testera.

Primer 4.4.6 U Primeru 3.5.1 posmatrajući matricu:

$$\begin{bmatrix} 2 & -2 & 1 \\ 1 & 1 & -2 \\ -3 & 1 & 1 \end{bmatrix}$$

pronašli smo jedan tester

$$f(z_1, z_2, z_3) = z_1 + z_2 + z_3$$

u $\mathbb{Z}$, $rang(A) = 2$ i postoji minor 2×2, $\begin{vmatrix} 2 & 1 \\ -3 & 1 \end{vmatrix} = 5$, a 5 je prost broj, pa osnovu Teoreme 4.4.3 (ii) sledi da postoji kompletan skup testera u $\mathbb{Z}$ i $\mathbb{Z}_5$. Računamo testere u $\mathbb{Z}_5$:

$$\underbrace{\begin{bmatrix} 2 & 1 & 1 \\ 3 & 1 & 1 \\ 1 & 3 & 1 \end{bmatrix}}_{A^T \bmod 5} \sim \begin{bmatrix} 1 & 3 & 1 \\ 3 & 1 & 1 \\ 2 & 1 & 2 \end{bmatrix} \sim \begin{bmatrix} 1 & 3 & 1 \\ 0 & -8 & -2 \\ 0 & -5 & 0 \end{bmatrix}$$

Kako je $rang(A \bmod 5) = 3$, dimenzija vektorskog prostora W_5 jednaka je nuli, odakle sledi da nema korisnih testera u $\mathbb{Z}_5$. Dakle, kompletan skup testera je $\{f\}$.

Primer 4.4.7 Posmatrajmo sledeći sistem linearnih Diofantovih jednačina:

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= y_1 \\ x_2 + 2x_3 + 3x_4 &= y_2 \\ x_3 + 2x_4 + 3x_5 &= y_3 \\ &\dots \\ x_N + 2x_{N+1} + 3x_{N+2} &= y_N \end{aligned}$$

Imamo da je:

$$A = \begin{bmatrix} 1 & 2 & 3 & 0 & 0 & \dots & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & \dots & 0 & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 & 2 & 3 \end{bmatrix}_{N \times (N+2)}$$

Sledeći minor matrice A reda $N \times N$ je vrednosti 1:

$$\begin{vmatrix} 1 & 2 & 3 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 2 & 3 & 0 & \dots & 0 & 0 \\ 0 & 0 & 1 & 2 & 3 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & 0 & \dots & 0 & 1 \end{vmatrix} = 1^N$$

Dakle, $rang(A) = N$ i zbog (iv) u Teoremi 4.4.3, sledi da uvek postoji rešenje sistema bez obzira na vrednosti $y_1, \ldots, y_N$, tj. kompletan skup testera matrice sistema je prazan.

4.5 Doprinosi metoda zasnovanog na testerima

U drugoj glavi ovoga rada pokazali smo kako egziztenciju rešenja sistema linearnih Diofantovih jednačina možemo ispitati računanjem Smitove normalne forme za matricu sistema. U ostatku ovoga rada bavili smo se metodom zasnovanim na linearnim funkcijama koje smo nazvali testeri. U praksi, pitanje koje se samo nameće, kada imamo dva različita metoda, koji metod je bolji? Za koji metod je računaru potrebno manje vremena za izvršavanje i samim tim manje prostora u memoriji računara? U sledećoj tabeli prikazana su poređenja ova dva metoda na matricama tipa $N \times M$ sa, random izabranim, celim koeficijentima iz skupa $\{1, 2, \ldots, 1000\}$. (Videti [7])

Metod baziran na	$N=M=5$	$N=M=20$	$N=M=30$	$N=M=50$
Smitovoj formi	0.016 s	10 min 37 s	50 min 12 s	6h 11 min
testerima	0.016 s	8 min 56 s	40 min 43 s	4h 27 min

Možemo videti da metod baziran na testerima daje bolji rezultat.

Definišimo sledeći rekurzivan niz matrica $A(n, x)$ gde je x ceo broj:

$$A(1, x) = \begin{bmatrix} 1 & x \\ x & -1 \end{bmatrix}$$

Matricu $A(n+1, x)$ definišemo induktivno tako što dodamo 2 vrste i 1 kolonu tako što kopiramo poslednju vrstu i kolonu prethodne matrice ali sa 4 nova elementa:

$$A(n+1, x) = \begin{bmatrix} A(n, x) & & \mathbf{a} \\ \mathbf{b} & (-1)^n & (-1)^{n+1} \\ \mathbf{b} & 0 & (-1)^n \end{bmatrix}$$

Dakle,

$$A(n+1, x) = \left[\begin{array}{cc|c|c|cc} 1 & x & x & x & x & \ldots \\ x & -1 & -1 & -1 & -1 & \ldots \\ \hline x & 1 & -1 & -1 & -1 & \ldots \\ x & 0 & 1 & 1 & 1 & \ldots \\ \hline x & 0 & -1 & 1 & 1 & \ldots \\ x & 0 & 0 & -1 & -1 & \ldots \\ \hline x & 0 & 0 & 1 & -1 & \ldots \\ x & 0 & 0 & 0 & 1 & \ldots \end{array}\right]$$

U sledećoj tabeli poredimo metode na matricama $A(n, x)$. (Videti [7])

Metod baziran na	$x = 4; n = 3$	$x = 4; n = 20$	$x = 4; n = 100$
Smitovoj formi	2.164 s	3 min 22 s	1h 23 min
testerima	2.026 s	30.245 s	28 min 39 s
	$x = 4; n = 256$ - 4 h 48 min		

Kao što se može videti, metod baziran na testerima i u ovom slučaju se pokazao boljim i bržim u smislu vremena izvršavanja operacija, i čak uspešnim za računanje matrica većih dimenzija za koje je primena drugog metoda zasnovanog na Smitovoj normalnoj formi nemoguća.

Zaključak

10. Hilbertov problem iz 1900. godine, da li postoji algoritam koji bi za svaku Diofantovu jednačinu odlučivao da li ona ima rešenja, rešen je negativno 1970. godine. Međutim, upravo zbog toga Diofantove jednačine i jesu fascinantno polje istraživanja u teoriji brojeva. Sistemi linearnih Diofantovih jednačina, iako teški za rešavanje, jer rešenja tražimo isključivo u skupu celih brojeva, posebno su važni u poljima celobrojnog linearnog programiranja i u rešavanju nekih zagonetki [10]. Do sada su pronađeni razni algoritmi za traženje minimalnih rešenja sistema oblika $Ax = 0$, gde je $x > 0$ [1, 3, 15, 19].

U ovom radu bavili smo se ispitivanjima egzistencije sistema linearnih Diofantovih jednačina. Najpre smo, ispitivanja vršili računanjem Smitove normalne forme za matricu sistema pomoću klasičnog metoda zasnovanog na Gausovom postupku eliminacije. Međutim, iako pomoću takvog oblika sistema lako dolazimo do rešenja, samo svođenje matrice na dijagonalni oblik predstavlja komplikovan posao. Naime, za matrice sistema velikih dimenzija memorija potrebna za njihovo izvršavanje premašuje memoriju jednog procesora.

Koristili smo i jednu novu metodu zasnovanu na linearnim funkcijama u $\mathbb{Q}$ i $\mathbb{Z}_p$, gde je p prost broj, koje smo nazvali testeri, pomoću kojih smo prvo pokazivali nepostojanje rešenja ovih sistema. Ali, neka pitanja su ostala otvorena. Ako sistem nema rešenja da li uvek postoji tester pomoću kojeg bismo to pokazali? I da li postoji konačan skup testera za svaki sistem pomoću kojeg možemo zaključiti da sistem linearnih Diofantovih jednačina ima rešenje? Na ova pitanja odgovorili smo pozitivno. Priču smo proširili na traženje testera i u skupu $\mathbb{Z}_m$, gde m nije prost broj. Dokazali smo da za svaku matricu sistema postoji kompletan skup testera. Proučavali smo vezu između ovog skupa i minora matrice sistema i naveli algoritam za računanje kompletnog skupa testera zasnovanog na ovoj vezi. Novi algoritam uspostavio se uspešnijim, jer tražeći testere u $\mathbb{Z}_m$ izbegli smo račun sa ogromnim koeficijentima matrice, što je upravo i predstavljao glavni problem kod svođenja matrice na Smitovu normalnu formu, i na kraju zaključili da je metod zasnovan na testerima bolji.

Literatura

[1] Chou T.-W.J., Collins G.E., Algorithms for the solution of systems of linear Diophantine equations. SIAM J. Comput. 11, 687–708 (1982)

[2] Fang, X.G., Havas,G., On the worst-case complexity of integer gausian elimination. In: Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation ISSAC, pp. 28–31. ACM Press, New York (1997)

[3] Filgueiras M., Tomás A.P., A fast method for finding the basis of non-negative solutions to a linear Diophantine equation. J Symbol. Comput. 19, 507–562 (1995)

[4] G. Frobenius, Theorie der linearen Formen mit ganzen Coefficienten, Jour. fur Math., 86 (1878) 146–208.

[5] G. Frobenius und L. Stickelberger, Uber Gruppen von Vertauschbaren Elementen, J. de Crelle LXXXVI, (1879) 217

[6] I. Heger, Denkschriften Acad. Wiss. Wien (Math. Nat.), 14 II (1858) 1-122.

[7] Hernando A., De Ledesma L., On the existence of solutions in systems of linear Diophantine equations, RACSAM, 105:223 (2011)

[8] A. Hernando, L. De Ledesma, L.M. Laita, A system simulating representation change phenomena while problem solving, Mathematics and Computers in Simulation 78 (2008) 89–106.

[9] Hernando A., De Ledesma L., Laita L.M., Showing the non-existence of solutions in systems of linear Diophantine equations. Math. Compute. Simul. 79, 3211–3220 (2009)

[10] Hernando, A., New methods for proving the impossibility to solve problems through reduction of problem spaces. Ann. Math. Artif. Intell. (2009)

[11] Ch. Hermite, Œuvres, t. I, Gauthier–Villars, Paris, 1905.

[12] N. Jacobson, Basic Algebra I, W.H. Freeman and Co.,San Francisco, 1974.

[13] R. Kannan and A. Bachem, Polynomial time algorithms to compute Hermite and Smith normal forms of an integer matrix, SIAM J. Computing, 8 (1979) 499–507.

[14] Lazebnik F., On Systems of linear Diophantine equations. Math. Mag. 69, 261–266 (1996)

[15] Pottier L., Minimal solutions of linear diophantine solutions: bounds and algorithms. Lect. Notes Comput. Sci. 488, 162–173 (1986)

[16] Smith H.J.S., On systems of linear indeterminate equations and congruences. Philos. Trans. R. Soc. Lond. 151, 293–326 (1861)

[17] Z. Stojaković, I. Bošnjak, Elementi linearne algebre, Novi Sad, 2010.

[18] Z. Stojaković, D. Herceg, Linearna algebra i analitička geometrija, Novi Sad, 2005.

[19] Tomás A.P., Filgueiras M., An algorithm for solving systems of linear Diophantine equations in naturals. Lect. Notes Comput. Sci. 1323, 3–84 (1997)

[20] G. Vojvodić, Predavanja iz algebre, Univerzitet u Novom Sadu, Novi Sad, 2007.

Biografija

Đorđe Dragić je rođen 23.1.1993. godine u Vlasenici, Republika Srpska. Osnovnu školu ,,Vuk Karadžić" završava 2008. godine kao nosilac Vukove diplome. Potom, u SŠC ,,Milorad Vlačić" u Vlasenici upisuje opšti smer gimnazije, koju završava 2012. godine kao nosilac Vukove diplome i učenik generacije.
Studije Prirodno-matematičkog fakulteta u Novom Sadu, smer Diplomirani profesor matematike, upisuje iste godine, i uspešno ih završava jula 2016., prosekom 9,55. Master akademske studije smer Master profesor matematike upisuje na istom fakultetu. Položio je sve ispite predviđene planom i programom sa prosečnom ocenom 9.50 i time stekao uslov za odbranu ovog master rada.
Tokom studija bio je stipendista Fonda za mlade talente ,,Dositeja". Zaposlen je na Fakultetu tehničkih nauka u Novom Sadu pri katedri za matematiku, kao saradnik u nastavi.

Novi Sad, oktobar 2018.

Đorđe Dragić

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR
Identifikacioni broj:
IBR
Tip dokumentacije: Monografska dokumentacija
TD
Tip zapisa: Tekstualni štampani materijal
TZ
Vrsta rada: Master rad
VR
Autor: Đorđe Dragić
VR
Mentor: dr Petar Đapić
MN
Naslov rada: Ispitivanja egzistencije rešenja sistema linearnih Diofantovih jednačina
NR
Jezik publikacije: srpski (latinica)
JP
Jezik izvoda: srpski/engleski
JI
Zemlja publikovanja: Srbija
ZP
Uže geografsko područje: Vojvodina
UGP
Godina: 2018.
GO
Izdavač: Autorski reprint
IZ
Mesto i adresa: Departman za matematiku i informatiku, Prirodno-matematički fakultet, Univerzitet u Novom Sadu, Trg Dositeja Obradovića 4, Novi Sad
MA
Fizički opis rada: (4, 85, 20, 0, 0, 0, 0)
(broj poglavlja, strana, literalnih citata, tabela, slika, grafika, priloga)

FO
Naučna oblast: Matematika
NO
Naučna disciplina: Algebra
ND
Predmetna odrednica/Ključne reči: Linearne Diofantove jednačine, Smitova normalna forma, testeri
PO
UDK:
Čuva se: Biblioteka Departmana za matematiku i informatiku Prirodno-matematičkog fakulteta u Novom Sadu
ČU
Važna napomena:
VN
Izvod: U ovom master radu bavimo se ispitivanjima egzistencije rešenja sistema linearnih Diofantovih jednačina. U prvom delu rada je data teorijska osnova koja je potrebna za razumevanje gradiva. Nakon toga pokazujemo kako se pomoću Smitove normalne forme matrice sistema ispituje njihova egzistencija. U nastavku rada, definišemo testere, posebne klase linearnih funkcija, i objašnjavamo njihov značaj za pokazivanje da određeni sistemi nemaju rešenja. Na kraju, govorimo o kompletnom skupu testera za svaki sistem i njegovoj vezi sa egzistencijom rešenja familije sistema linearnih Diofantovih jednačina.
IZ
Datum prihvatanja teme od strane NN veća: 03.09.2018.
DP
Datum odbrane:
DO
Članovi komisije:
KO
Predsednik: dr Ivica Bošnjak, vanredni profesor Prirodno-matematičkog fakulteta, Univerziteta u Novom Sadu
Mentor: dr Petar Đapić, vanredni profesor Prirodno-matematičkog fakulteta, Univerziteta u Novom Sadu
Član: Siniša Crvenković, redovni profesor Prirodno-matematičkog fakulteta u penziji, Univerziteta u Novom Sadu

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCE
KEY WORDS DOCUMENTATION

Accession number:
ANO
Identification number:
INO
Document type: Monograph
DT
Type of record: Printed text
TR
Contents Code: Master's thesis
CC
Author: Đorđe Dragić
AU
Mentor: Petar Đapić, Ph. D.
MN
Title: Study of the existence of solutions for a systems of Diophantine linear equations
TI
Language of abstract: English
LA
Country of publication: Republic of Serbia
CP
Locality of publication: Vojvodina
LP Publication year: 2018.
PY
Publisher: Author's reprint
PU
Publ. place: Department of Mathematics and Informatics, Faculty of Science, Trg Dositeja Obradovića 4, Novi Sad
PP
Physical description: 4 chapters/85 pages/20 refences
PD
Scientifictield: Mathematics
SF
Scientific discipline: Algebra

SD
Subject/Key words: Linear Diophantine equations, Smith normal form, testers
SKW
Holding data: Library of Department of Mathematics and Inforatics, Faculty of Science, University of Novi Sad
HD
Note:
N
Abstract: The main topic of this Master's Thesis is study of the existence of solutions for a systems of Diophantine linear equations. The first part of the paper exposes theoretical basis essential for understanding of the material. Further, application of Smith's normal forms of the system matrix for solution existence examination is demonstrated. After that, special class of linear function, testers, are defined and their significance of indicating that some systems do not have solution is explained. Lastly, we are talking about a complete set of testers for each system and its relationship with the existence of a solution of the family of the linear Diophantine equations.
AB
Accepted by the Scientific Board on: 03/09/2018
ASB
Defended:
DE
Thesis defend board:
DB
President: Ivica Bošnjak, Ph.D., associate professor, Faculty of Science, University of Novi Sad
Member: Petar Đapić, Ph.D., associate professor, Faculty of Science, University of Novi Sad, mentor
Member: Siniša Crvenković, Ph.D., full professor, Faculty of Science, University of Novi Sad