Mr Ivan Lončar
Fakultet organizacije i informatike
V a r a ž d i n

UDK 511
Stručni rad

A L G O R I T M I Z A L I N E A R N E D I O F A N T S K E J E D N A D Ž B E

Skup $D = \{0, \pm 1, \pm 2, \ldots\}$ *ima važnu ulogu u različitim zadacima teorijske i primijenjene matematike.*

U primjeni se u tom smislu naročito ističu razni zadaci cjelobrojnog linearnog programiranja.

Linearne jednadžbe s cjelobrojnim koeficijentima za koje tražimo i cjelobrojna rješenja dolaze često u zadacima cjelobrojnog linearnog programiranja.

Cilj ovog rada je teorijska obrada algoritama rješavanja navedenih jednadžbi i programska realizacija takvih algoritama kao potprograma u programskom jeziku FORTRAN.

1. OSNOVNE DEFINICIJE

Definicija 1.1.

Neka je $D^n = D \times \ldots \times D$ Kartezijev produkt od n faktora koji su jednaki skupu D cijelih brojeva.

Svako preslikavanje $f: D^n \longrightarrow D$ nazivamo cjelobrojnom ili diofantskom funkcijom od n cjelobrojnih varijabli.

Često ćemo funkciju f pisati u obliku

$$y=f(x_1,x_2,\ldots,x_n);\ y,x_1,x_2,\ldots,x_n \in D. \qquad \ldots (1)$$

Definicija 1.2.

Za fiksirani $y \in D$ označavamo s $f^{-1}(y)$ skup svih $x \in D^n$, $x = (x_1,x_2,\ldots,x_n)$ za koje vrijedi

$$y = f(x) \qquad \ldots (2)$$

ili

$$y = f(x_1,x_n,\ldots,x_n) \qquad \ldots (3)$$

Uz fiksirani y nazivamo izraz (3) cjelobrojnom ili diofantskom*) jednadžbom.

---

*) *Diofant, grčki matematičar, oko 270. godine prije nove ere. Vidi (1).*

U izrazu (3) mogu načelno sudjelovati različite računske operacije. Zbog uvjeta cjelobrojnosti za varijable $y, x_1, x_2, \ldots, x_n$ jasno je da nema smisla da u izrazu (3) sudjeluju operacije različite od operacije zbrajanja, oduzimanja, množenja i potenciranja cjelobrojnim eksponentom. Navedene operacije su zatvorene u skupu D. Zbog toga ima smisla podjela izraza (3) na jednadžbe s više varijabli i na jednadžbe različitih stupnjeva.

Definicija 1.3.

Linearna diofantska jednadžba je svaki izraz oblika

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = b \qquad \ldots (4)$$

uz uvjet da su $a_1, a_2, \ldots, a_n, b$ cijeli brojevi, tj. elementi skupa D.

Sustav S linearnih diofantskih jednadžbi je skup linearnih diofantskih jednadžbi

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n &= b_2, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n &= b_m. \end{aligned} \qquad \ldots (5)$$

Primjer 1.
Jednadžba $3x_1 + 4x_2 = 5$ je linearna diofantska jednadžba s dvije varijable x_1 i x_2.

Primjer 2.
Jednadžba $x^2 + y^2 = z^2$ je diofantska jednadžba drugog stupnja (kvadratna) s tri varijable x, y i z.

2. NUŽDAN I DOVOLJAN UVJET RJEŠIVOSTI LINEARNE DIOFANTSKE JEDNADŽBE

Definicija 2.1.
Rješenje diofantske jednadžbe (4) je svaka uredjena n-torka $(x_1', y_2', \ldots, x_n') \in D^n$ za koju vrijedi numerička jednakost

$$y_1x_1' + \ldots + a_nx_n' = b \qquad \ldots (6)$$

Svaka diofantska jednadžba ne mora imati rješenje. Jednadžba $3x_1 + 6x_2 = 4$ ne može imati cjelobrojno rješenje (x_1, x_2) jer bi dijeljenjem jednadžbe s 3 dobili $x_1 + 2x_2 = 4/3$. Na lijevoj strani nalazi se cijeli broj, a na desnoj razlomljeni. Kontradikcija!

Ovaj nas primjer uvjerava da vrijedi

Lema 2.2.
Jednadžba (4) nema rješenja ako slobodni koeficijent b nije djeljiv s najvećom zajedničkom mjerom $M(a_1,\ldots,a_n)$koeficijenata $a_1,\ldots,a_n$.

Prirodno je dakle postaviti pitanje da li rješenje postoji ako je b djeljiv s $M(a_1,\ldots,a_n)$? Pokažimo da rješenje postoji, tj. da vrijedi

Lema 2.3.
Diofantska jednadžba (4) ima rješenje onda i samo onda kada je b djeljiv s $M(a_1,a_2,\ldots,a_n)$.

Nužnost je već dokazana. Dokažimo da je navedeni uvjet dovoljan. Uz fiksirane $a_1,\ldots,a_n$ označimo s $L(a_1,a_2,\ldots,a_n)$ skup svih brojeva oblika $a_1x_1 + \ldots + a_nx_n$ uz varijabilne cijele brojeve $x_1,\ldots,x_n$. Jasno je da $L(a_1,\ldots,a_n)$ sadrži pozitivne cijele brojeve, tj. prirodne brojeve. Neka je r najmanji prirodan broj skupa $L(a_1,\ldots,a_n)$. Tvrdimo sada da je $r=M(a_1,\ldots,a_n)$ jer bez utjecaja na općenitost možemo pretpostaviti da su $a_1,\ldots,a_n$ prirodni brojevi. Kada r ne bi bio jednak $M(a_1,\ldots,a_n)$, tada bi postojao a_i za koji vrijedi $a_i = rq_i + r_i, r_i \neq 0, r_i < r$. Kako je

$$r = a_1x_1 + \ldots + a_nx_n,$$

dobivamo

$$r_i=a_i-q_i(a_1x_1+\ldots+a_nx_n)= -q_ia_1x_1+\ldots+(a_i-q_ia_i)x_i+\ldots$$

Odatle bi slijedilo da je r_i element skupa $L(a_1,\ldots,a_n)$manji od r. To je naravno nemoguće jer je r najmanji prirodan broj sadržan u $L(a_1,\ldots,a_n)$. Odatle slijedi da jednadžba

$$a_1x_1 + \ldots + a_nx_n = M(a_1,\ldots,a_n) \qquad \ldots (7)$$

ima rješenje. To naravno znači da i jednadžba

$$\frac{a_1}{M}x_1 + \ldots + \frac{a_n}{M}x_n = 1 \qquad \ldots (8)$$

Množenjem s b uvjeravamo se da je $(bx_1/M,\ldots,bx_n/M)$ rješenje jednadžbe (4). Dokaz je gotov.

3. ALGORITMI

Lema 2.3. je egzistencijalne naravi, tj. ona osigurava egzistenciju rješenja jednadžbe (4), ali ne ukazuje na put efektivnog odredjivanja barem jednog rješenja. U ovoj točki posvećujemo pažnju pitanjima matematičkih i programskih algoritama za odredjivanje rješenja. Kao pripremu iznosimo Euklidov algoritam za odredjivanje najveće zajedničke mjere $M(a,b)$ cijelih brojeva a i b. Lema 2.3. ukazuje na važnost mjere $M(a,b)$ kod diofantskih jednadžbi.
Neka su a i b cijeli brojevi. Bez utjecaja na općenitost možemo pretpostaviti da su a i b prirodni brojevi i da je $b > a$.

Izvršimo li nepotpuno dijeljenje, imamo

$$b = aq_1 + r_1 \qquad \ldots (9)$$

$$r_1 < a . \qquad \ldots (10)$$

Iz relacije (9) lako zaključujemo da svaki broj c, koji dijeli brojeve a i b, dijeli takodjer brojeve a i r_1. Vrijedi i obrat! Time smo dokazali da vrijedi

Lema 3.1.
Iz relacije (9) slijedi da je $M(a,b) = M(a,r_1)$.

Jasno je da se može dogoditi da bude $r_1 = 0$, tj. da vrijedi relacija

$$b = aq_1 \qquad \ldots (11)$$

Lema 3.2.
Iz relacije (11) slijedi da je $M(a,b) = a$.

Očito je da će biti lakše odrediti $M(a,r_1)$ nego $M(a,b)$ jer se radi o manjim brojevima. Odatle je jasno da će se postupak relacije (9) primjenjivati tako dugo dok ne dodjemo do vrlo malih brojeva ili pak do situacije relacije (11). Izvršimo li dakle nepotpuno dijeljenje a sa r_1, imamo

$$a = r_1q_2 + r_2 \qquad \ldots (12)$$

$$r_2 < r_1 \qquad \ldots (13)$$

Nastavljajući tako imat ćemo općenito

$$r_n = r_{n+1}q_{n+2} + r_{n+2} \qquad \ldots (14)$$

$$r_{n+2} < r_{n+1} \qquad \ldots (15)$$

Relacije (10), (13) i (15) pokazuju da ostaci dijeljenja padaju, a odatle slijedi da ćemo za konačno mnogo dijeljenja doći do ostatka nula. Tada ćemo imati situaciju relacije (11) a time i mjeru brojeva a i b.

Primjer 3.
Za brojeve a=246 i b=322 imamo ovo verižno Euklidovo dijeljenje:

322:246 = 1
246: 76 = 3
18:4=4
4:2 = 2
Ø

Dakle je M(322;246) = 2.

Za potrebe programiranja na elektroničkim računskim mašinama koristit ćemo često ocjenu broja potrebnih dijeljenja u Euklidovom algoritmu.

Lema 3.3.
Neka su a i b dva prirodna broja i a b. Broj nepotpunih dijeljenja u algoritmu Euklida nije veći od peterostrukog broja znamenaka broja a prikazanog u dekadskom sustavu.

Dokaz se nalazi u djelu (5). Najveći broj dijeljenja potreban je tada kada su a i bi susjedni članovi Finonačijevog niza, tj. niza koji se zadaje rekurzivnom jednakošću

$$u_{n+2} = u_{n+1} + u_n \qquad \text{... (16)}$$

uz početne uvjete $u_1 = u_2 = 1$.

Prethodne jednakosti omogućavaju prikaz broja $\frac{b}{a}$ u obliku verižnog razlomka. Naime iz (9) slijedi

$$\frac{b}{a} = q_1 + \frac{r_1}{a}$$

a iz (12) je

$$\frac{a}{r_1} = q_2 + \frac{r_2}{r_1}.$$

Uvrštavanje u prethodnu jednakost i nastavljanje daje

$$\frac{b}{a} = q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3 + \dots + \cfrac{1}{q_n}}} \qquad \text{... (17)}$$

Definicija 3.4.
Razlomak (17) nazivamo verižni razlomak, a razlomke q_1, $q_1 + \frac{1}{q_2}$, $q_1 + \cfrac{1}{q_2 + \cfrac{1}{q_3}}$, ... zovemo prva, druga, treća itd. aproksimacija razlomka (17).

Ako u aproksimacijama razriješimo višestruke razlomke, možemo ih prikazati u obliku

$$\frac{P_k}{Q_k} \qquad \text{... (18)}$$

Brojnici P_k i nazivnici Q_k imaju niz interesantnih svojstava. Neka od njih dajemo u slijedećoj lemi. Dokaz se nalazi u djelu (2).

Lema 3.5.
Brojnici P_n i nazivnici Q_n aproksimacija zadovoljavaju slijedeće jednakosti:

$$P_n = P_{n-1}\, q_n + P_{n-2}, \qquad \text{... (19)}$$

$$Q_n = Q_{n-1}\, q_n + Q_{n-2}, \qquad \text{... (20)}$$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^n, \qquad \text{... (21)}$$

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^{n+1} q_n \qquad \text{... (22)}$$

Početni uvjeti za relacije (19) i (20) su $P_o=Q_1=1, Q_o=0$ i $P_1=q_1$. Takodjer se jednostavno indukcijom dokazuje da su P_n i Q_n relativno prosti brojevi, tj. $M(P_n, Q_n) = 1$.

Uzme li se u obzir da će za neki k razlomak (18) biti jednak $\frac{b}{a}$, možemo reći da nam prikazivanje pomoću verižnih razlomaka može poslužiti za skraćivanje razlomaka.

Za nas je mnogo važnije da za relativno proste a i b relacija (21) daje

$$aQ_{n-1} - bP_{n-1} = (-1)^n \qquad \text{... (23).}$$

Množenje s $(-1)^n$ daje relaciju

$$aQ_{n-1}(-1)^n + bP_{n-1}(-1)^{n-1} = 1 \qquad \text{... (24)}$$

Jednakost (24) pokazuje da jednadžba

$$ax + by = 1 \qquad \dots (25)$$

ima rješenje

$$x = (-1)^n Q_n,$$
$$y = (-1)^{n-1} P_{n-1} \qquad \dots (26)$$

Množimo li rješenja (26) brojem c, možemo dobiti rješenje jednadžbe

$$ax + by = c \qquad \dots (27)$$

za relativno proste brojeve a i b.

Dokažimo na kraju da jednadžba (27) ima beskonačno mnogo rješenja ako ima barem jedno rješenje.

Ako postoji barem jedno rješenje (x_o, y_o) jednadžbe (27), tada mora biti

$$ax_o + by_o = c \qquad \dots (28)$$

Oduzimanje jednakosti (28) od (27) daje $a(x-x_o) = -b(y-y_o)$. Kako a i b imaju najveću zajedničku mjeru M(a,b)=1, to dijeljenjem s brojem a uvidjamo da je $(y-y_o)$:a cijeli broj. Označimo li ga sa u, dobivamo $y-y_o=au$. Uvrštavanje u posljednju jednakost daje $x - x_o = -bu$. Dakle, sva su rješenja dana relacijama

$$x = x_o - bu,$$
$$y = y_o + au \qquad \dots (29)$$

Kako je u slobodan parametar, to ćemo iz (29) moći dobiti beskrajno mnogo rješenja. Izraze (29) nazivamo parametarsko ili opće rješenje jednadžbe (27). Rješenje (x_o, y_o) nazivamo posebno rješenje. Jednakosti (26) daju jedno posebno rješenje jednadžbe(25).

U nastavku ove točke nalaze se potprogrami EUKLID i DIOFMA. Potprogram EUKLID je programska realizacija Euklidovog algoritma za ulazne prirodne brojeve M i N. Izlazne veličine su najveća zajednička mjera NZM i najmanji zajednički višekratnik NZV.ITER je brojač nepotpunih dijeljenja. DIOFMA odredjuje posebno rješenje IXO,IYO za jednadžbu MX+NY=K primjenjujući relacije (26).

```
      SUBROUTINE EUKLID(M,N,NZM,NZV,ITER)
      M1=M
      N1=N
      ITER=0
    5 KVOC=M1/N1
      ITER=ITER+1
      IOSTAT=M1-N1=KVOC
      IF(IOSTAT)1,1,2
    1 NZM=N1
      NZV=M*N/NZM
      RETURN
    2 M1=N1
      N1=IOSTAT
      GO TO 5
      END
      SUBROUTINE DIOFMA(M,N,K,IXO,IYO,M1,N1,K1,*)
      CALL EUKLID(M,N,NZM,NZV,ITER)
      CALL EUKLID(NZM,K,NZM1,NZV1,ITER1)
      M1=M/NZM1
      N1=N/NZM1
      K1=K/NZM1
      CALL EUKLID(M1,N1,NZM,NZV,ITER)
      IOST=K1-(K1/NZM)*NZM
      IF(IOST)10,30,10
   10 WRITE(6,15)
   15 FORMAT(T10,'JEDNADŽBA NEMA CJELOBROJNOG RJEŠENJA')
      RETURN1
   30 M1=M1/NZM
      N1=N1/NZM
      K1=K1/NZM
      IDIVN=M1
      IDIVZ=N1
      IP0=0
      IY0=1
      IP1=1
      IQ1=0
      ITER=1
   25 IQ=IDIVN/IDIVZ
      IOST=IDIVN-IQ*IDIVZ
      IPN=IP1*IQ+IP0
      IQN=IQ1*IQ+IQ0
      IF(IOST),40,70,40
   40 IDIVN=IDIVZ
      IDIVZ=IOST
```

```
      IPO=IP1
      IP1=IPN
      IQO=IQ1
      IQ1=IQN
      ITER=ITER+1
      GO TO 25
   70 IF(ITER-(ITER/2)*2)100,80,100
   80 IXO=IQ1*K1
      IYO=-IP1*K1
   82 WRITE(6,85)IXO,N1,IYO,M1
   85 FORMAT(T30,'PARAMETARSKO RJESENJE'//T43,'X=',I10,'+ ',I10,'*U'
     * /T4 3,'Y = ',I10,'- ', I10,'* U')
      RETURN
  100 IXO=-IQ1*K1
      IYO=IP1*K1
      GO TO 82
      END

      GLAVNI PROGRAM POKUS TESTIRA EUKLID I DIOFMA
      M=26532
      N=7816
      CAL EUKLID(M,N,NZM,NZV,ITER)
      WRITE(6,10)NZM,ITER
   10 FORMAT(T10,'MJERA = ',I10//T10,'BROJ ITERACIJA = ', I10)
      M=26
      N=7
      K=106
      CALL DIOFMA (M,N,K,IXO,IYO,M1,N1,K1,&20)
   20 STOP
      END
```

Potprogram MJERA je višestruka primjena potprograma EUKLID u skladu sa slijedećom lemom.

Lema 3.6.
Ako su $a_1,a_2,\ldots,a_n$ prirodni brojevi, tada vrijedi relacija

$$M(a_1,a_2,\ldots,a_n)=M(a_1,M(a_2,\ldots,M(a_{n-1},a_n))).$$

Prirodni brojevi nalaze se u cjelobrojnoj matrici MAT potprograma MJERA, a višestruko pozivanje potprograma EUKLID vrši se pomoću DO petlje koja počinje instrukcijom DO 1Ø I=1,N.

Potprogram GMJERA zasniva se na generalizaciji Euklidovog algoritma.

Lema 3.7.
Neka su $a_1, a_2, \ldots, a_n$ prirodni brojevi i a_1 najmanji medju njima. Neka su

$$a_2 = a_1 q_2 + r_2,$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$a_n = a_1 q_n + r_n$$

relacije nepotpunog dijeljenja, tada je

$$M(a_1, a_2, \ldots, a_n) = M(a_1, r_2, \ldots, r_n).$$

Dokaz je jednostavan i sličan dokazu leme 3.1.

```
   SUBROUTINE MJERA (N,MAT,NZM,IZLAZ)
   DIMENSION MAT(N)
   POTPROGRAM ZA NZM N BROJEVA IZ MATRICE MAT.
   M=MAT(1)
   DO 10 I=1,N
   N1=MAT(I)
   CALL EUKLID(M,N1,NZM,NZV,ITER)
   M=NZM
10 CONTINUE
   IF(IZLAZ-1)15,20,15
20 WRITE(6,25)NZM
25 FORMAT(T10,'NAJVEĆA ZAJEDNIČKA MJERA NZM = ',I10)
15 RETURN
   END

   SUBROUTINE GMJERA(N,MAT,NZM,IZLAZ)
   DIMENSION MAT(N)
 5 DO 6 I=1,N
   IF(MAT(I))7,6,7
 7 NZM=MAT(I)
   GO TO 8
 6 CONTINUE
   GO TO 25
 8 DO 10 I=1,N
   IF(MAT(I))11,10,11
11 IF(NZM-MAT(I))10,10,15
15 NZM=MAT(I)
10 CONTINUE
```

```
      DO 20 I=1,N
      IQ=MAT(I)/N
   20 MAT(I)=MAT(I)-IQ*NZM
   25 IBROJ=0
      IF(MAT(I))30,35,30
   35 IBROJ=IBROJ+1
   30 CONTINUE
      IF(IBROJ-N)5,40,5
   40 IF(IZLAZ-1)45,50,45
   50 WRITE(6,55)NZM
   55 FORMAT(T10,'NAJVEĆA ZAJEDNIČKA MJERA NZM ',I10)
   45 RETURN
      END

C     GLAVNI PROGRAM POKUS1 TESTIRA MJERA I GMJERA
      DIMENSION MAT(5)
      DATA MAT/273,1564,262,1115,6565/
      CALL MJERA (5,MAT,NZM,1)
      CALL GMJERA(5,MAT,NZM,1)
      STOP
      END
```

Prethodni postupak možemo tretirati na drugi način ovako:
Za jednadžbu $a_1x_1 + a_2x_2 = b$, konkretno $26x_1 + 29x_2 = 5$ odaberimo varijablu s najmanjim po apsolutnoj vrijednosti koeficijentom. U našem slučaju to je varijabla x_1. Izrazimo je pomoću x_2,

$$x_1 = \frac{5-29x_2}{26} = -x_2 + \frac{5-3x_2}{26}.$$

Da bi uz cijeli x_2 varijabla x_1 bila cijeli broj, mora razlomak

$$u = \frac{5-3x_2}{26}$$

biti cijeli broj. Dobivamo jednadžbu

$$3x_2 + 26u = 5.$$

Važno je sada uočiti da smo umjesto jedne jednadžbe $26x_1+29x_2= 5$ dobili dvije nove, i to:

$$x_1 + x_2 - u = 0$$
$$3x_2 + 26u = 5.$$

Isti postupak sada provodimo s jednadžbom $3x_2 + 26u = 5$. Opet odabiremo varijablu s najmanjim koeficijentom. To je varijabla x_2. Imamo

$$x_2 = -8u + 1 + \frac{-2u+2}{3}$$

Odatle slijedi

$$x_2 = -8u + 1 + v$$

$$3_v = -2u + 2.$$

Na kraju iz posljednje jednadžbe slijedi

$$u = 1 - v - \frac{v}{2}$$

Konačno vidimo da mora $z = v/2$ biti cijeli broj, tj. $v = 2z$. Sada se moramo vraćati unatrag i izraziti sve uvedene parametre u,v i varijable x_1 i x_2 izraziti pomoću parametra z.

Za parametar u imamo $u=1 - 3z$. Na temelju toga je $x_2 = -8u+1+v=$ $=-8(1-3z)+1+2z=-7+26z$. Odatle za x_1 slijedi: $x_1 =-x_2 + u =$ $= +7-26z+1-3z$ ili $x_1 = 8 - 29z$.

Varijable x_1, x_2 izražene su pomoću parametra z. Dobiveno je parametarsko rješenje. Vidimo da je ideja jednostavna i uspješna, ali je treba na neki način algoritmizirati.

Ova metoda rješavanja poznata je iz vremena prije naše ere (vidi djela (1) i (7)).

Dokažimo sada lemu koja nam omogućava algoritmizaciju.

Lema 3.8.
Svaka linearna diofantska jednadžba ekvivalentna je sistemu od dvije diofantske jednadžbe. Prva od njih dobije se tako da koeficijenti uz varijable budu kvocijenti dobiveni dijeljenjem koeficijenata polazne jednadžbe s koeficijentom one varijable koja ima najmanji po apsolutnoj vrijednosti koeficijent, dok druga jednadžba ima kao koeficijente ostatke navedenog dijeljenja. U svakoj od ovih jednadžbi dolazi novo uvedeni parametar, u prvoj s koeficijentom +1,a u drugoj s koeficijentom koji je jednak negativnoj odabranoj apsolutnoj vrijednosti.

Dokaz. Neka je zadana jednadžba (4) i neka je a_i koeficijent koji ima najmanju apsolutnu vrijednost. Bez utjecaja možemo pretpostaviti da je a_i pozitivan. Izvršimo li nepotpuno dijeljenje svih koeficijenata s koeficijentom a_i, možemo (4) pisati

$$(a_i q_1 + r_1)x_1 + \ldots + a_i x_i + \ldots + (a_i q_n + r_n) = a_i q + r$$

ili

$$a_i(q_1x_1 + \dots + x_i + \dots + q_nx_n) + (r_1x_1 + \dots r_{i-1}x_{i-1} + r_{i+1}x_{i+1} + \dots) = a_iq + r.$$

Dijeljenjem s a_i uvidjamo da zbog zahtjeva cjelobrojnosti mora biti razlomak

$$\frac{r_1x_1 + \dots + r_nx_n - r}{a_i}$$

cijeli broj koji ćemo označiti s u_1 ili u_i ako su već neki parametri uvedeni. Na taj način iz prethodne jednadžbe slijede dvije:

$$q_1x_1 + \dots + x_i + \dots + q_nx_n + u = q$$

$$r_1x_1 + \dots\dots\dots\dots\dots + r_nx_n - a_iu = r.$$

Dokaz je gotov.

Za jednadžbu $45x_1 - 32x_2 + 7x_3 = 9$ opisani postupak izgleda ovako:

$$\begin{array}{rcl} 45x_1 - 32x_2 + 7x_3 & = & 9 \\ \hline x_3 + 6x_1 - 4x_2 + u_1 & = & 1 \\ 3x_1 - 4x_2 - 7u_1 & = & 2 \\ \hline \end{array}$$

Primijenimo li lemu 3.8. na posljednju jednadžbu, imamo

$$\begin{aligned} x_3 + 6x_1 - 4x_2 + u_1 &= 1 \\ x_1 - x_2 - 2u_1 + u_2 &= 0 \\ - x_2 - u_1 - 3u_2 &= 2. \end{aligned}$$

U posljednjoj jednadžbi najmanja apsolutna vrijednost koeficijenta jednaka je jedinici pa nema smisla dalje primjenjivati lemu 3.8.

Gausova eliminacija varijabli daje sustav

$$\begin{aligned} x_3 \qquad + 11u_1 - 12u_2 &= 5 \\ x_1 \qquad - u_1 + 4u_2 &= -2 \\ x_2 + u_1 + 3u_2 &= -2. \end{aligned}$$

Odatle dobivamo opće rješenje u parametarskom obliku:

$$x_1 = -2 + u_1 - 4u_2$$
$$x_2 = -2 - u_1 - 3u_2$$
$$x_3 = 5 - 11u_1 + 12u_2.$$

Uzmemo li da su svi parametri jednaki nuli, dobivamo posebno rješenje $x_1=-2, x_2=-2, x_3=5$.

Programska realizacija ove ideje nalazi se u potprogramu DIOF1. Matrica MAT služi za pohranjivanje koeficijenata varijabli i parametara, a matrica MAT1 za pohranjivanje desnih strana jednadžbi. Matrica MAT2 memorira poredak varijabli koje se nalaze na dijagonali matrice MAT.

4. DIOFANTSKE JEDNADŽBE I KONGRUENCIJE

U svim analizama rješivosti diofantskih jednadžbi važnu ulogu ima djeljivost cijelih brojeva. Zbog toga u ovoj točki želimo formalizirati pojam djeljivosti. Ujedno ćemo postići svodjenje pretraživanja beskonačnog skupa rješenja na konačan podskup a time omogućiti primjenu elektroničkog računala.

Definicija 4.1.
Za dva cijela broja kažemo da su kongruenti u odnosu na cijeli broj m ako je njihova razlika djeljiva brojem m, tj. $a = b \pmod m$ onda i samo onda kada je $a-b=qm$.

Lako je dokazati da je relacija $\equiv \pmod m$ jedna relacija ekvivalencije na skupu D, tj. da je refleksivna, simetrična i tranzitivna. Vrijedi naime ova jednostavna lema.

Lema 4.2.

Za cijele brojeve a i b u odnosu na svaki modul m vrijedi:

a) refleksivnost, tj. $a \equiv a \pmod m$,

b) simetričnost, tj. $a \equiv b \pmod m \longrightarrow b \equiv a \pmod m$ i

c) tranzitivnost, tj. $a \equiv b \pmod m$ i $b \equiv c \pmod m \longrightarrow a \equiv c \pmod m$.

Iz ove leme na poznati način slijedi da relacija kongruencije s obzirom na bilo koji modul m rastavlja skup D na razrede ili klase modulo m.

Definicija 4.3.
Razred ili klasa broja a modulo m je maksimalan skup brojeva b za koje vrijedi $b \equiv a \pmod m$.

Razred broja a modul m označavamo s $[a]$.

Lako je ustanoviti da brojevi 0,1,...,m-1 nisu dva po dva kongruentni modulo m te prema tome pripadaju raznim razredima. S druge strane za svaki broj b zbog poznatog nepotpunog dijeljenja možemo pisati b=qm+r slijedi da je $b \equiv r(\mathrm{mod}\ m)$. Ostatak r je manji od m pa je dakle svaki broj b kongruentan jednom od brojeva 0,1,2,..., m-1.

Definicija 4.4.
Brojeve 0,1,2,...,m-1 zovemo potpuni sistem ostataka mod m a one od njih koji su relativno prosti s m zovemo reducirani sistem ostataka.

Lema 4.5.
Potpuni sistem ostataka mod m je m-člani skup, pa prema tome i razreda mod m ima točno m.

Što se tiče kardinalnog broja reduciranog sistema ostataka možemo reći da je jednak Euler-ovom indikatoru $\varphi(m)$ u skladu s definicijom.

Definicija 4.6.
Euler-ov indikator $\varphi(m)$ broja m je broj svih brojeva a koji su manji od m i relativno prosti s m, tj. za koje vrijedi M(a,m)=1.

Ako je poznata faktorizacija broja $m = p_1^{n_1} \dots p_i^{n_i} \dots p_k^{n_k}$,

$$(m) = m\ (1 - p_1^{-1}) \dots (1-p_i^{-1})\ \dots\ (1 - p_k^{-1}).$$

Jasno je da je za prim broj p $\varphi(p) = p-1$.

Potprogram EULER odredjuje indikator $\varphi(m)$ pod nazivom IFIM koristeći potprogram EUKLID, jer bi upotreba gornje formule zahtijevala faktorizaciju brojeva što nije jednostavan zadatak.

Potprogram FAKTOR je jednostavan potprogram za faktorizaciju zasnovan na pretraživanju i dijeljenju.

Slijedeća lema pokazuje značaj broja $\varphi(m)$.

Lema 4.7.
Za svaki cijeli broj a i modul m,M(a,m)=1, vrijedi kongruencija

$$a^{\varphi(m)} \equiv 1\ (\mathrm{mod}\ m).$$

Specijalno je dakle za svaki cijeli broj a relativno prost s prim brojem p ispunjava kongruencija

$$a^{p-1} \equiv 1 (\mathrm{mod}\ p).$$

Spomenimo na kraju kongruenciju koja karakterizira prim brojeve.

Lema 4.8.
Prirodni broj p je prim onda i samo onda kada je ispunjena kongruencija

$$(p-1)! + 1 \equiv 0 \pmod{p}.$$

```
   SIBROUTINE FAKTOR (M,MAT,IBROJ,IZLAZ)
   DIMENSION MAT(M)
   IBROJ=0
   N=M
   DO 10 I=1, M-1
   CALL VILSON(I,IPRIM,0)
   IF(IPRIM)15,10,15
15 IQ=N/I
   IOST=N-IQ*I
   IF(IOST)10,20,10
20 IBROJ=IBROJ+1
   MAT(IBROJ)=I
   N=IQ
   GO TO 15
10 CONTINUE
   IF(IZLAZ)30,40,30
40 RETURN
30 IF(IBROJ)45,60,45
60 WRITE(6,65)M
65 FORMAT(T10,'BROJ M = ',I10,' JE PRIMBROJ')
   GO TO 40
45 WRITE(6,70)M
70 FORMAT(T10,'BROJ M = ',I10,'IMA FAKTORE:'/)
   DO 75 I=1,IBROJ
75 WRITE(6,80)I,MAT(I)
80  FORMAT(T15,I2,', FAKTOR ',I5)
   END

   SUBROUTINE KONGR(M,N,L.IX,*)
   POTPROGRAM ZA KONGRUENCIJU MX=N(MOD L)
   DO 10 I=0,L
   IY=M*I-N
   IF(IY)15,20,20
15 IY=-IY
20 IQ=IY/L
   IOST=IY-IQ*L
```

```
   IF(IOST)10,30,10
30 IX=I
   RETURN
10 CONTINUE
   END

   SUBROUTINE EULER (M,IFIM)
   IFIM=0
   DO 10 I=1,M
   CALL EUKLID(I,M,NZM)
   IF(NZM-1)10,30,10
30 IFIM=IFIM+1
10 CONTINUE
   RETURN
   END

   SUBROUTINE VILSON (M,IPRIM,IZLAZ)
   IFAKT=1
   DO 10 I=1,M-1
   IFAKT=IFAKT*I
   IQ=IFAKT/M
   IOST=IFAKT-IQ*M
   IFAKT=IOST
10 CONTINUE
   IFAKT=IFAKT+1
   IQ=IFAKT/M
   IOST=IFAKT-IQ*M
   IF(IOST)15,20,15
15 IPRIM = Ø
   IF(IZLAZ)25,30,25
30 RETURN
25 WRITE(6,35)M
35 FORMAT(T10,'BROJ M= ',I10,' NIJE PRIMBROJ')
   GO TO 30
20 IPRIM=1
   IF(IZLAZ)40,30,40
40 WRITE(6,45)M
45 FORMAT(T10,'BROJ M = ',I10,' JE PRIMBROJ')
   RETURN
   END
```

```
  GLAVNI PROGRAM
  DIMENSION MAT(10)
  N=10
  CALL VILSON(37,IPRIM,1)
  CALL VILSON(49,IPRIM,1)
  CALL FAKTOR(215,MAT,IBROJ,1)
  CALL KONGR(5,4,7,IBROJ&5)
5 CALL EULER(17,IFIM)
  WRITE(6,7)IFIM
7 FORMAT(T10,'IFIM= ', I10)
  STOP
  END

      SUBROUTINE DIOF1(N,M1,N1,KOEFV,KOEFS,MAT,MAT1,MAT2,ITER,*,*)
      DIMENSION KOEFV(N),MAT(M1,N1),MAT1(M1),MAT2(N1)
      DO 10 I=1,N
      MAT2(I)=I
   10 MAT(1,I)=KOEFV(I)
      MAT1(1)=KOEFS
C     POČETAK PROCEDURE EUKLIDOVOG DIJELJENJA
      ITER=0
   15 ITER=ITER+1
C     TRAŽENJE VARIJABLE S NAJMANJIM PO APS.VRIJEDNOSTI KOEFICIJENTOM
      IX=IABS(MAT(ITER,1))
      DO 20 I=1,N1
      IY=IABS(MAT(ITER,I))
      IF(IY)20,20,30
   30 IF(IX-IY)20,20,31
   31 IX=IY
      IRED=I
   20 CONTINUE
      IF(IX)25,25,34
   25 IF(MAT1(ITER))33,26,33
   33 WRITE(6,32)
   32 FORMAT(T10,'JEDNADŽBA NEMA CJELOBROJNO RJEŠENJE')
      RETURN1
   26 GO TO 300
C     PREMJEŠTANJE VARIJABLE
   34 IF(IX-1)25,45,35
   45 IF(IRED-N1)35,35,87
   35 DO 40 I=1,M1
      IZ=MAT(I,IRED)
      MAT(I,IRED)=MAT(I,ITER)
   40 MAT(I,ITER)=IZ
```

```
      K=MAT2(IRED)
      MAT2(IRED)=MAT2(ITER)
      MAT2(ITER)=K
C     TRANSFORMACIJA JEDNADŽBE I FORMIRANJE NOVE JEDNADŽBE
      DO 50 I=1,M1
      IF(MAT(ITER,I))55,50,65
   55 IQ=-MAT(ITER,I)/IX
      MAT(ITER,I)=-IQ
      IOST=TABS(MAT(ITER,I))-IX*IQ
      MAT(ITER+1,I)=-IOST
      GO TO 50
   65 IQ=MAT(ITER,I)/IX
      MAT(ITER,I)=IQ
      IOST=MAT(ITER,I)=IX*IQ
      MAT(ITER+1,I)=IOST
   50 CONTINUE
      MAT(ITER+1,N+ITER)=-IX
      MAT(ITER,ITER+N)=1
      IF(MAT1(ITER))70,80,90
   70 IQ=TABS(MAT1(ITER))-IX*IQ
      MAT1(ITER)=-IQ
      MAT1(ITER+1)=-IOST
      GO TO 100
   80 MAT1(ITER+1)=0
      ITER1=ITER
      GO TO 100
   50 IQ=MAT1(ITER)/IX
      IOST=MAT1(ITER)-IX*IQ
      MAT1(ITER)=IQ
      MAT1(ITER+1)=IOST
C     ELIMINACIJA
   87 IF(MAT(ITER,ITER))81,89,89
   81 DO 82 I=1,N1
   82 MAT(ITER,I)=-MAT(ITER,I)
   89 DO 91 I=1,M1
      IK=MAT(I,ITER)
      IF(I-ITER)92,91,92
   92 DO 93 J=1,N1
   93 MAT(I,J)=MAT(I,J)-MAT(ITER,J)*IK
      MAT1(I)=MAT1(I)-MAT1(ITER)=IK
   91 CONTINUE
      IF(IX)100,300,100
  100 IF(ITER-M1)15,150,150
  150 WRITE(6,155)M1
  155 FORMAT(T10,'POTREBNO JE VIŠE OD',I5,'PARAMETARA,POVEĆAJ DI-
     *MENZIJU MATRICE MAT1.')
```

```
      RETURN2
C     IZLAZ
  300 IF(ITER-N)310,350,350
  350 ITER1=N
  310 DO 315 I=1,ITER1
      DO 320 J=1,N1
      K=MAT2(J)
      IF(I-K)320,325,320
  320 CONTINUE
      IF(ITER-N)325,335,335
  325 WRITE(6,326)K
  326 FORMAT(T20,'K(',I2,') = ')
      DO 330 J=ITER+1,N
  330 WRITE(6,331)MAT(I,J),MAT2(J)
  331 FORMAT(T30,I10,'*X(',I2,')')
  335 DO 340 J=1,ITER
  340 WRITE(6,341)MAT(I,N+J),J
  341 FORMAT(T30,I10,'*U(',I2,')')
  315 CONTINUE
      RETURN
      END

      DIMENSION KOEFV(2),MAT(10,10),MAT1(10),MAT2(10)
      KOEFV(1)=25
      KOEFV(2)=27
      CALL DIOF1(2,10,10,KOEFV,33,MAT,MAT1,MAT2,ITER,&1,&1)
    1 STOP
      END
```

Generalizacija ideje koja je realizirana u potprogramu DIOF1 je ideja ugradjena u potprogram DIOFAN koji se može primijeniti na sustave diofantskih jednadžbi. Ovaj se potprogram temelji na unimodularnim transformacijama matrice sistema. Time se matrica dovodi na Smitovu formu matrice, vidi djelo 4.

Potprogram je snabdjeven velikim brojem komentara C pa ga nećemo posebno opisivati.

Na kraju skrenimo pažnju na djela 8 i 9 u kojima se nalaze ocjene potrebnog broja operacija za pojedine algoritme.

```
      SUBROUTINE DIOFAN(ULAZ,M,N,A,B,IZLAZ,REDAK,STUPAC,Y,Z,*)
      DIMENSION A(M,N),REDAK(M,N),STUPAC(M,N),B(M),Y(M),Z(N)
      POTPROGRAM ZA CJELOBROJNO RJEŠENJE SUSTAVA S CJELOBRO.KOEFI_
      CIJENTIMA;ULAZ=1 AKO POTP.UČITAVA PODATKE A INAČE ULAZ=0;
      IZLAZ=1 AKO SE TISKA PARAMET.RJEŠENJE A INAČE IZLAZ=0
C     A(M,N)=MATRICA KOEF.VARIJABLI SUSTAVA S M JEDNADŽBI I N VA-
C     RIJABLI.
C     B(M)=MATRICA DESNIH STRANA SUSTAVA A*X=B.
C     REDAK=MATRICA KOJA U POČETKU JEDINIČNA I MEMORIA SVE OPERACI-
C     JE S RECIMA MATRICE A.
C     STUPAC=MATRICA ANALOGNA MATRICI REDAK ALI ZA MEMORIRANJE
C     OPERACIJA SA STUPCIMA MATRICE A.Y=PARAMETARSKA MATRICA.(CJE-
C     LOBROJNA).
C     M,N=DEFINIRANI U GLAVNOM PROGRAMU KAO I IZLAZ
C1    INICIJALIZACIJA MATRICA REDAK I STUPAC
      DO 10 I=1,M
   10 REDAK(I,I)=1
      DO 20 I=1,N
   20 STUPAC(I,I)=1
C2    UČITAVANJE
      IF(ULAZ-1)50,30,50
   30 DO 35 I=1,M
      DO 35 J=1,N
   35 READ(5,40)A(I,J)
   40 FORMAT(F15.0)
      DO 45I=1,M
   45 READ(5,40)B(I)
C3    PROCEDURA ZA SMITOVU FORMU CJELOBROJNE MATRICE
   50 IRANG=0
  111 IF(IRANG-M)60,60,500
   60 IF(IRANG-N)110,110,500
  110 IRANG=IRANG+1
C4    TRAŽENJE NAJMANJEG PO APOSLUT.VRIJED.ELEMENTA MATRICE A
  112 X=ABS(A(IRANG,IRANG))
      DO 113 I=IRANG,M
      DO 114 J=IRANG,N
      IF(ABS(A(I,J)))115,114,115
  115 X=ABS(A(I,J))
  114 CONTINUE
  113 CONTINUE
      IR=IRANG
      IS=IRANG
      DO 120 I=IRANG,M
      DO 125 J=IRANG,N
      IF(ABS(A(I,J)))124,125,124
```

```
  124 IF(X-ABS(A(I,J)))125,130,130
  130 X=ABS(A(I,J))
      IR=I
      IS=J
  125 CONTINUE
  120 CONTINUE
      IF(X)140,145,140
   15 IRANG =IRANG-1
      GO TO 500
C9    PERMUTACIJA REDAKA
  140 DO 150 I=1,N
      X=A(IRANG,I)
      A(IRANG,I)=A(IR,I)
      A(IR,I)=X
      IF(M-I)150,151,151
  151 X=REDAK(IRANG,I)
      REDAK(IRANG,I)=REDAK(IR,I)
      REDAK(IR,I)=X
  150 CONTINUE
C     PERMUTACIJA STUPACA
      DO 160 J=1,M
      X=A(J,IS)
      A(J,IS)=A(J,IRANG)
      A(J,IRANG)=X
      IF(N-J)160,161,161
  161 X=STUPAC(J,IS)
      STUPAC(J,IS)=STUPAC(J,IRANG)
      STUPAC(J,IRANG)=X
  160 CONTINUE
C6    TRANSFORMACIJA REDAKA
      IF(IRANG-M)165,195,195
  165 DO 170 I=IRANG+1,M
      KVOC=IFIX(A(I,IRANG))/IFIX(A(IRANG,IRANG))
      DO 180 J=1,N
  180 A(I,J)=A(I,J)-KVOC*A(IRANG,J)
      DO 185 J=1,M
  185 REDAK(I,J)=REDAK(I,J)-KVOC*REDAK(IRANG,J)
  170 CONTINUE
C7    TRANSFORMACIJA STUPACA
  195 IF(IRANG-N))196,201,201
  196 DO 190 J=IRANG+1,N
      KVOC=IFIX(A(IRANG,J))/IFIX(A(IRANG,IRANG))
      DO 200 I=1,M
```

```
  200 A(I,J)=A(I,J)-KVOC*A(I,IRANG)
      DO 205 I=1,N
  205 STUPAC(I,J)=STUPAC(I,J)-KVOC*STUPAC(I,IRANG)
  190 CONTINUE
C8    ISPITIVANJE DA LI SU NULE U RETKU
  201 IF(IRANG-N)202,203,203
  202 DO 210 I=IRANG+1,N
      IF(A(IRANG,I))112,210,112
  210 CONTINUE
C9    ISPITIVANJE DA LI SU NULE U STUPCU
  203 IF(IRANG-M)204,500,112
  204 DO 220 I=IRANG+1,M
      IF(A(I,IRANG))112,220,112
  220 CONTINUE
      GO TO 111
C10   ISPITIVANJE NUŽNIH I DOVOLJNIH UVJETA ZA EGZISTENCIJU CJE-
C11   LOBROJNOG RJEŠENJA,MNOŽENJE MATRICE REDAK S MATRICOM B.
  500 DO 520 J=1,M
      S=0
      DO 530 K=1,M
  530 S=S+REDAK(J,K)*B(K)
  520 Y(J)=S
C12   ISPITIVANJE DJELJIVOSTI U VEZI S UVJETOM A)
      OD 540 I=1, IRANG
      KVOC=IFIX(Y(I))/IFIX(A(I,I))
      KOST=Y(I)-KVOC*IFIX(A(I,I))
      IF(KOST)600,545,600
  545 Y(I)=KVOC
  540 CONTINUE
      GO TO 700
  600 WRITE(6,610)
  610 FORMAT(T20,'SUSTAV NEMA CJELOBROJNOG RJEŠENJA'//)
      RETURN1
C13   ISPITIVANJE UVJETA B
  700 IF(IRANG-M)710,800,800
  710 DO 720 I=IRANG+1,M
      IF(Y(I))600,720,600
  720 CONTINUE
C14   MNOŽENJE MATRICE STUPAC I MATRICE Y.NAKON TOGA Z SADRŽI
C15   KONSTANTNE DIJ.ZA X DOK STUPAC-MATRICA SAD.KOEF.PAR.DIJELA.
  800 DO 810 I=1,N
      S=0
      DO 820 J=1,IRANG
  820 S=S+STUPAC(I,J)*Y(J)
  810 Z(I)=S
```

```
C16    ELEMENTI I-TOG RETKA MATRICE STUPAC ZA I>IRANG SU KOEFICI-
C17    JENTI PARAMETARA Y=(I)
C18    IZVJEŠTAJI
       IF(IZLAZ-1)850,830,850
   850 RETURN
   830 IF(IRANG-N)860,900,900
   860 WRITE(6,865)
   865 FORMAT(T30,'SUSTAV IMA SLIJEDEĆE PARAMETARSKO RJEŠENJE:'/
      *T25,53(1H*)/T25,53(1H*)///)
       DO 870 I=1,N
       WRITE(6,875)I,Z(I)
   875 FORMAT(T40,'X(',I2,') = ',F1).0/)
       DO 880 J=IRANG+1,N
   880 WRITE(6,885)STUPAC(I,J),J
   885 FORMAT((50,'+(',F10.0,')*Y(',I2,')'/)
       WRITE(6,890)
   890 FORMAT(T40,30(1H*)///)
   870 CONTINUE
       RETURN
   900 WRITE(6,995)
   995 FORMAT(T40,'SUSTAV IMA JEDINSTVENO RJEŠENJE'/T35,41(1H*)/
      *T35,41(1H*)//)
       DO 996 I=1,N
   996 WRITE(6,875)I,Z(I)
       RETURN
       NED

   GLAVNI PROGRAM CJEL TESTIRA DIOFAN
   DIMENSION  A(3,5),REDAK(3,3),STUPAC(5,5),B(3),Y(3),Z(5)
   DATA A(1,1),A(1,2),A(1,3),A(1,4),A(1,5)/1.,1.,1.,-4.,1./
   DATA A(2,1),A(2,2),A(2,3),A(2,4),A(2,5)/.,1.,1.,3.,-2./
   DATA A(3,1),A(3,2),A(3,3),A(3,4),A(3,5)/2.,0.,2.,-1.,-1./
   DATA B/-6.,2.,8./
   ULAZ=0
   IZLAZ=1
   M=3
   N=5
   CALL DIOFAN(ULAZ,M,N,A,B,IZLAZ,REDAK,STUPAC,Y,Z,&10)
10 STOP
   END
```

```
SUSTAV IMA SLIJEDEĆE PARAMETARSKO RJEŠENJE:
********************************************

       X( 1) =           16.
             +(           5.)*Y( 4)
             +(          -1.)*Y( 5)
       ******************************

       X( 2) =           -6.
             +(           0.)*Y( 4 )
             +(           0.)*Y( 5)
       ******************************

       X( 3) =            0.
             +(           0.)*Y( 4)
             +(           1.)*Y( 5)
       ******************************

       X( 4) =            0.
             +(           1.)*Y(4)
             +(           0.)*Y( 5)
       ******************************

       X( 5) =            0.
             +(           0.)*Y( 4)
             +(           1.)*Y( 5)
       ******************************
```

L I T E R A T U R A :

1. *I.G.Bašmakova,Diofant i diofantovi uravnenija,Moskva,1972.*
2. *A.A.Buhštab,Teorija čisel,Moskva,1966.*
3. *M.A.Frumkin, Primenije modul'noj arifmetiki k postrojeniju algoritmov dlja rešenija sistem linejnyh uravnenij,Dokl. AN SSSR,1976,tom 229,no 5,1067-1070.*
4. *A.Kofman,A.Anri-Laborder,Metody i modeli issledovanija operacij, Moskva 1977.*
5. *A.I.Markuševiĉ, Vozvratnyje posledovatel'nosti,Moskva, 1975.*
6. *I.M.Vinigradov, Osnovy teorii čisel, Moskva 1972.*
7. *A.I.Volodskij, Ariabhata, Moskva, 1977.*
8. *M.Matijasevič, Diofantovi množestva, UMN,tom XXVII,5(167), 1972, 185-222.*
9. *M.A.Frumkin,Stepenye algoritmy v teorii sistem linejnyh diofantovyh uravnenij, Soobšćenija Mos.mat,obšćestva, 1975.*

Primljeno: 1979-10-4

Lončar I. Algorithms for Linear Diophantine Equations

SUMMARY

The paper contains algorithms for diophantine equations. The algorithms are expressed in FORTRAN programming language and take the form of subroutines.

In determining the solutions of a system of diophantine equations, the most important role is played by the subprograms DIOF1 and DIOFAN. These subprograms are in turn supported by the auxiliary subprograms EUKLID, DIOFMA, MJERA and FAKTOR.