Статијата прв пат е објавена во списанието Математичко-физички лист на ДМФА на Хрватска во 1961

O jednom diofantskom problemu

Dr MIRKO STOJAKOVIĆ, Novi Sad

Mnogi problemi u algebri ili geometriji svode se na rešavanje nekog sistema jednačina ali se pri tom od svih uopšte mogućih rešenja tog sistema jednačina zadržavaju samo ona koja imaju neka unapred određena svojstva. Izdvajanje takvih rešenja nije uvek lak posao. Iz jedne vrste takvih problema razvila se posebna grana matematike — diofantska analiza. Čitav niz čuvenih problema matematike upravo je te prirode. Tako, na primer, ni danas se nezna da li jednakost $x^n+y^n=z^n$ ima ili nema rešenja u celim brojevima $x, y, z \neq 0$ za svaki prirodan broj n. Ta jednačina ima rešenja kad je $n = 2$ na primer $x = 5$, $y = 12$, $z = 13$, nema rešenja kad je $n = 3$, nema ih ni kad je $n = 4, 5, 6, \ldots$ ali se ne zna postoji li možda još neko n sem $n = 2$ kad ta jednačina opet ima rešenja u celim brojevima (različitim od nule). To je čuveni *Fermatov* problem. Ne manje slavan je i *Goldbahov* problem koji je uz to i jednostavniji po formulaciji: linearna jednačina $x + y = 2z$ ima rešenja u prostim brojevima x, y za svaki prirodan broj z. No koliko god da je to jednostavno kazati ne sledi da je to jednostavno i dokazati — i taj problem do danas nije rešen. Ispitane su takve jednačine za veoma velike vrednosti z (čak i do 9 000 000) i uvek su probanjem nađena rešenja u prostim brojevima ali to još nije dokaz ta tako mora biti za svako z. Ovi su primeri jednostavni ali su ograničenja »stroga«.

Ovde ćemo posmatrati linearnu jednačinu $Ax + By = C$ gde su A, B, C celi brojevi ali nećemo tražiti da rešenja budu prosti brojevi kao u Goldbahovom problemu nego »samo« da budu takođe celi brojevi.

Neka je, dakle, data jednačina

$$(1) \quad Ax + By = C$$

gde su $A \neq 0$, $B \neq 0$, C celi brojevi i neka se traže sva rešenja te jednačine u celim brojevima x, y.

Utvrdićemo uslove pod kojima takva rešenja uopšte postoje i navesti postupak kojim se do rešenja dolazi kad se utvrdi da ona postoje. Odvojićemo, znači problem *egzistencije rešenja od problema algoritma kojim se rešenja nalaze.*

Najpre ćemo problem uprostiti smanjivši broj pretpostavki pod kojima se jednačina (1) ima rešavati.

Pre svega, brojevi A, B, C u jednačini (1) mogu se smatrati uzajamno prostim to jest oni nisu sva tri deljivi jednim istim celim brojem D većim od 1. Jer ako je

$$(2) \quad A = A_1D, \; B = B_1D, \; C = C_1D$$

gde su i A_1, B_1 C_1 celi brojevi a D njihov najveći zajednički delitelj $\neq 1$ onda se jednačina (1) svodi na ekvivalentnu jednačinu

$$(3) \quad A_1x + B_1y = C_1$$

koja ima koeficijente uzajamno proste pa kako sva njena rešenja jesu rešenja jednačine (1) a važi i obrnuto, to je dovoljno posmatrati jednačinu (1) pod navedenom pretpostavkom.

Dalje, možemo uzeti da su A i B u jednačini (1) p o z i t i v n i brojevi. Jer, ako su A i B negativni brojevi množenjem cele jednačine sa -1 dobijamo novu ekvivalentnu jednačinu sa pozitivnim koeficijentima uz nepoznate. Ako je jedan od brojeva A, B pozitivan a drugi negativan, recimo $A < 0$ $B > 0$, onda se smenom $x = -u$ dobija jednačina sa pozitivnim koeficijentima uz nepoznate, pa ako je u rešenju u ceo broj biće i $-u$ odnosno x ceo broj i problem tom smenom ništa ne gubi.

Posmatrajmo, prema tome, jednačinu (1) pod pretpostavkom da su A, B prirodni brojevi i da A, B, C nemaju zajednički delitelj veći od 1. Uzmimo sad specijalni slučaj jednačina (1) kad je $C = 0$. Neka je dakle, najprije

$$(4) \quad Ax + By = 0.$$

Ako A i B imaju najveći zajednički delitelj $D \neq 1$, to jest ako je $A = A_1D$, $B = B_1D$ onda se jednačina (4) svodi na jednačinu

$$(5) \quad A_1x + B_1y = 0$$

gde su sad A_1, B_1 uzajamno prosti prirodni brojevi. Iz $A_1x = -B_1y$ sledi da x mora biti deljivo sa B_1 jer je proizvod A_1x deljiv sa B_1 a A_1 nije deljivo tim brojem. Dakle $x = mB_1$. Isto tako dobija se $y = nA_1$ gde su m, n neki celi brojevi. Tada se jednačina (5) svodi na

$$(6) \quad A_1B_1(m + n) = 0$$

pa mora biti $m + n = 0$ odnosno $m = -n$ i tako imamo

STAV 1. *Jednačina (4) ima rešenja i sva ona data su sa*

$$(7) \quad x = mB_1, \quad y = -nA_1$$

gde je m m a k o j i ceo broj.

Uzmimo sad još specijalni slučaj jednačine (1) u kome je $C = 1$. Neka je, dakle,

$$(8) \quad Ax + By = 1.$$

Ako A i B imaju najveći zajednički delitelj $D \neq 1$ to jest ako je $A = A_1D$, $B = B_1D$, tada se jednačina (8) svodi na

$$(9) \quad D(A_1x + B_1y) = 1$$

pa je leva strana deljiva sa D a desna to ne može biti i nikakve vrednosti za x, y u celim brojevima ne mogu tu ništa da poprave. Stoga u tom slučaju jednačina (8) n e m a rešenja u celim brojevima. Ako su pak A i B u jednačini (8) uzajamno prosti brojevi onda jednačina (8) i m a rešenja i to dokazujemo time što rešenje stvarno navodimo. Jedno od rešenja naći ćemo poznatim E u k l i d o v i m a l g o r i t m o m kojim se sračunava najveći zajednički delitelj za dva prirodna broja. Verižno deljenje koje se tu izvodi polazeći od brojeva A, B mora dovesti do ostatka 1 jer je to najveći zajednički delitelj dva uzajamno prosta broja A, B. Neka je dakle $A > B$ (> 0) i neka je pri deljenju broja A brojem B količinik k_1 a ostatak $D_1 < B$, to jest

$$(10) \quad A = k_1B + D_1 \; D_1 < B.$$

Postupak ponovimo sa B i D ako nije $D_1 = 1$ to jest neka je

$$(11) \quad B = k_2 D_1 + D_2, \quad D_2 < D_1.$$

Ako nije $D_2 = 1$ postupak ponovimo sa D_2 i D_1 to jest neka je

$$(12) \quad D_1 = k_3 D_2 + D_3, \quad D_3 < D_2.$$

Ako ni sad nije $D_3 = 1$ postupak možemo opet ponoviti. Jednom se kao ostatak mora dobiti 1 jer niz pozitivnih brojeva A, B, D_1, D_2, D_3 opada pa ako se produži mora da se završi sa 1. Da ne bismo opterećivali tekst a da bi suština postupka ipak bila jasna dovoljno je da uzmemo da je već $D_4 = 1$ to jest važi, recimo,

$$(13) \quad D_2 = k_4 D_3 + 1.$$

Jednačine (10), (11), (12) i (13) sadrže ostatke D_1, D_2, D_3 i kako tu ima četiri jednačine a tri veličine ove se mogu eliminisati. Zbilja idući unazad od jednačine (13) pa do (10) imamo redom

$$\begin{aligned} 1 &= D_2 - k_4 D_3 = D_2 - k_4 (D_1 - k_3 D_2) = D_2 (1 + k_3 k_4) - k_4 D_1 = (B - k_2 D_1)(1 + k_3 k_4) - k_4 D_1 = \\ &= B (1 + k_3 k_4) + D_1 (-k_2 - k_2 k_3 k_4 - k_4) = B (1 + k_3 k_4) + (A - k_1 B)(-k_2 - k_2 k_3 k_4 - k_4) = \\ &= A (-k_2 - k_2 k_3 k_4 - k_4) + B (1 + k_3 k_4 + k_1 k_2 + k_1 k_2 k_3 k_4 + k_1 k_4) = A x_1 + B y_1, \end{aligned}$$

gde su sa x_1, y_1 označeni izrazi u poslednjim dvema zagradama, to jest

$$(14) \quad A x_1 + B y_1 = 1,$$

pa je (x_1, y_1) jedno rešenje jednačine (8). I tako važi

STAV 2. *Jednačina*

$$Ax + By = 1$$

ima rešenja u celim brojevima onda i samo onda kad su A i B uzajamno prosti brojevi.

Sad tek možemo posmatrati opštu jednačinu (1) (naravno pod stalnom pretpostavkom da su A, B prirodni brojevi a A, B, C nemaju zajednički delitelj veći od 1. Pokazaćemo da važi

STAV. 3. *Jednačina*

$$(1) \quad Ax + By = C$$

ima rešenja u celim brojevima onda i samo onda kad su brojevi A, B uzajamno prosti.

Zbilja, ako brojevi A, B nisu uzajamno prosti nego je $A = A_1 D$, $B = B_1 D$, onda je $D(A_1 x + B_1 y) = C$ pa je leva strana deljiva sa D a desna nije što ne može biti ni za kakove cele brojeve x, y. Obrnuto, ako su A i B uzajamno prosti onda jednačina

$$(15) \quad Au + Bv = 1$$

prema stavu 2 ima rešenja i neka je jedno od njih (u_0, v_0). Onda je međutim (Cu_0, Cv_0) jedno rešenje jednačine (1) jer je $ACu_0 + BCv_0 = C(Au_0 + Bv_0) = C$. Da nađemo s v a rešenja jednačine (1), u slučaju kad ih ona uopšte ima, postupimo ovako: Iz $Ax + By = C$ i $ACu_0 + BCv_0 = C$ sledi oduzimanjem $A(x - Cu_0) + B(y - Cv_0) = 0$ a prema stavu 1 mora biti

$$x - Cu_0 = mB, \quad y - Cv_0 = -mA,$$

jer su A i B uzajamno prosti brojevi pa su uslovi za primenu stava 1 ispunjeni. Stoga važi

STAV 4. ***Sva rešenja jednačine $Ax + By = C$, u slučaju kad ih ona ima, data su sa***

$$x = Cu_0 + mB, \quad y = Cv_0 - mA,$$

gde je (u_0, v_0) *jedno rešenje jednačine* $Au + Bv = 1$ a $(mB, -mA)$ *opšte rešenje jednačine* $Az + Bw = 0$.

Primer 1. Jednačina $4x + 6y = 5$ nema rešenja jer brojevi 4 i 6 nisu uzajamno prosti.

Primer 2. Jednačina $4x + 5y = 6$ ima rešenja jer su brojevi 4 i 5 uzajamno prosti. Jedno rešenje jednačine $4u+5v = 1$ je $u_0 = 4$, $v_0 = -3$ a opšte rešenje jednačine $4z + 5w = 0$ je $z = 5m$, $w = -4m$ pa je opšte rešenje jednačine $4x+5y=6$ dato sa $x=6u_0+5m$, $y=6v_0-4m$ to jest $x=24+5m$, $c = -18 - 4m$, gde m može biti koji bilo ceo broj.

Primenimo sad nađene stavove na sledeći problem: ispitati kada su $m + n$ i mn uzajamno prosti brojevi, ako su m i n prirodni brojevi.

STAV 5. *Prirodni brojevi* m, n *uzajamno su prosti onda i samo onda kad su* $(m + n)$ *i* mn *uzajamno prosti brojevi.*

Zbilja, ako su $m+n$ i mn uzajamno prosti brojevi onda za podesno nađene cele brojeve x, y važi $(m+n)x+mny=1$ (Stav 2). Odatle sledi $mx+n(x+my)=1$ pa su m i n uzajamno prosti brojevi. Obrnuto, neka je $mx+ny=1$ (*) za neke cele brojeve x, y to jest neka su m, n uzajamno prosti brojevi, tada je redom

$$1 = mx + ny = m(x + zn) + n(y - zm) = (x + zn)(m + n) - (x + zn)n + (y - zm)n = \\ = (x + zn)(m + n) + [y - x - z(m + n)]n,$$

gde je z neki još neodređeni broj.

Uzimajući sad $z = y(y - x)$ dobijamo dalje

$$1=[x+y(y-x)n](m+n)+(y-x)(1-ym-yn)n$$

a kako po pretpostavci (*) važi $1-ny=mx$ biće poslednja jednakost

$$1=[x+y(y-x)n](m+n)+(y-x)(x-y)mn=(m+n)u+mnv$$

gde je stavljeno $u=x+(y-x)n$, $v=-(y-x)^2$ a veza $1=(m+n)u+mnv$ i kazuje da su $(m+n)$ i mn uzajamno prosti brojevi. Time je i stav 5 dokazan.