Prirodno-matematički fakultet, Univerzitet u Nišu, Srbija
http://www.pmf.ni.ac.yu/mii
Matematika i informatika 1 (1-2) (2008), 29-38

Euklidov algoritam

Radoslav Dimitrijević

U osnovi merenja je upoređivanje veličina iste vrste. Pri tome se ne ostaje na konstataciji da je neka veličina veća, manja ili jednaka drugoj, nego se utvrđuje tačan odnos prenošenjem jedne veličine na drugu veličinu. U procesu merenja ne upoređujemo samo veličine među sobom, već i sve veličine iste vrste upoređujemo sa jednom određenom, koju nazivamo jediničnom.

Ako je duž AB sadržana ceo broj n puta u nekoj duži PQ, broj n nazivamo **mernim brojem** duži PQ, uzimajući AB za jediničnu duž i pišemo $PQ = n \cdot AB$. Budući da raspolažemo ne samo racionalnim, već i iracionalnim brojevima, za svake dve duži možemo odrediti merni broj jedne, uzimajući drugu za jediničnu. Prema tome, za ma koje dve duži AB i PQ možemo pisati da je $PQ = x \cdot AB$, nezavisno od toga da li je x racionalan ili iracionalan broj.

Još u staroj grčkoj geometriji osobit značaj imao je pojam samerljivosti i nesamerljivosti veličina. U desetoj knjizi Euklidovih "Elemenata" uvodi se pojam samerlj ivih duži na sledeći način: Kaže se da su veličine **samerljive**, ako imaju zajedničku meru i da su **nesamerljive**, ako im se ne može odrediti zajednička mera.

To znači sledeće: ako su A i B dve samerljive veličine, tada postoji treća veličina C tako da je $A = mC$ i $B = nC$, pri čemu su m i n prirodni brojevi. No onda je $A : B = mC : nC = m : n$, odn. $A = \frac{m}{n}B$. Ako m/n označimo sa p, možemo reći da su veličine A i B samerljive ako postoji pozitivan racionalan broj p tako da je $A = pB$. Ukoliko ne postoji takav pozitivan racionalan broj, veličine A i B su nesamerljive.

Određivanje zajedničke mere dveju samerljivih duži u Euklidovim "Elementima" izvodi se Euklidovim algoritmom koji se sastoji u sledećem. Neka su AB i CD dve nejednake duži. Ukoliko se manja duž CD sadrži u većoj duži AB ceo broj puta, onda je duž CD zajednička

mera duži AB i CD. U protivnom, prenesimo manju duž CD na veću duž AB toliko puta dok ne preostane izvesna duž KD koja je manja od duži CD. Ako se duž KD sadrži ceo broj puta u duži CD, onda je duž KD zajednička mera duži AB i CD. U protivnom, prenesimo duž KD na duž CD toliko puta dok ne preostane duž LB koja je manja od duži KD. Ukoliko jednog trenutka dođemo do duži koja se ceo broj puta sadrži u prethodnoj, onda je tako dobijena duž zajednička mera duži AB i CD. U daljim razmatranjima videćemo da je opisanim algoritmom određena **najveća zajednička mera** duži AB i CD.

Ukoliko opisani algoritam ne dovodi do tražene duži, tada su duži AB i CD nesamerljive. Euklidov algoritam u tom slučaju ima beskonačno mnogo koraka. Na taj način možemo reći da Euklidovom algoritmu sa beskonačno koraka odgovara iracionalan broj koji je određen odnosom mernih brojeva posmatranih veličina. Da nesamerljivih duži ima, pokazuje primer kvadrata kod koga su stranica i dijagonala nesamerljive duži.

Ako svakoj veličini iste vrste pridružimo merni broj u odnosu na određen sistem merenja, određivanje zajedničke mere veličina svodi se na nalaženje zajedničkog delioca brojeva. Najveći zajednički delioc dva cela broja određuje se već opisanim Euklidovim algoritmom. U osnovi Euklidovog algoritma je sledeća teorema.

Teorema 1. *Neka su a i b nenegativni celi brojevi, pri čemu je $b \neq 0$. Tada su jednoznačno određeni celi brojevi q i r tako da je*

$$a = bq + r\,, \quad 0 \leqslant r < b\,. \tag{1}$$

Broj q nazivamo količnikom brojeva a i b, a r ostatkom pri deljenju broja a brojem b.

U gore opisanom postupku nalaženja zajedničke mere dveju duži, primenjujući Euklidov algoritam, prećutno smo koristili upravo navedenu teoremu u svakom koraku Euklidovog algoritma. Ovu teoremu učenici prvi put čuju već u petom razredu osnovne škole, da bi se sa njom ponovo susreli u prvom razredu srednje škole.

Dokaz : Posmatrajmo skup celih brojeva

$$\{a - kb : \ k \in \mathbb{N}_0\} \tag{2}$$

i izaberimo u njemu najmanji broj koji je prirodan ili eventualno nula. Na osnovu principa dobrog uređenja takav broj postoji. Neka je to broj $a - qb$. Označimo ga sa r. Tada je $a = qb + r$, gde je $0 \leqslant r < b$. Zaista, ako bi bilo $r \geqslant b$, tada bi i broj $a - (q+1)b$, koji je manji od $a - qb$, bio prirodan ili jednak nuli, što je u kontradikciji sa činjenicom da je $a - qb$ najmanji broj u skupu (2). Time smo dokazali egzistenciju brojeva q i r.

Dokažimo jedinstvenost ovih brojeva. Pretpostavimo da postoji još jedan par (q_1, r_1) celih brojeva tako da je $a = q_1 b + r_1$, $0 \leqslant r_1 < b$. Oduzimanjem poslednje jednakosti od jednakosti (1) dobijamo da je

$$0 = (q - q_1)b + (r - r_1)\,, \tag{3}$$

odakle sledi da $b \,|\, r - r_1$. Kako je $|r - r_1| < b$, to je $r - r_1 = 0$, odn. $r = r_1$, pa je sada zbog (3) $q = q_1$, čime je teorema dokazana.

Neka su a i b nenegativni celi brojevi od kojih je bar jedan veći od nule. Broj k je **zajednički delitelj** brojeva a i b ako $k \,|\, a$ i $k \,|\, b$. Najveći pozitivan ceo broj koji je delitelj brojeva a i b naziva se **najveći zajednički delitelj** brojeva a i b i označava se sa (a, b). Određivanje najvećeg zajedničkog delioca u osnovnoj školi, ali i u srednjim školama, radi se tako da se za zadate brojeve najpre nađe faktorizacija istih, da bi se odatle odredio najveći zajednički delioc. Ovakav metod je dosta neefikasan, jer je često određivanje faktorizacije zamašan posao koji je teško uraditi u vremenski razumnom roku. Isti problem još više dolazi do izražaja kada su u pitanju polinomi i određivanje najvećeg zajedničkog delioca dva polinoma. U tom slučaju neophodno je najpre odrediti nule zadatih polinoma, što u najvećem broju slučajeva predstavlja nerešiv problem. Međutim, najveći zajednički delioc dva polinoma se i u ovom slučaju veoma jednostavno određuje Euklidovim algoritmom koji je potpuno analogan Euklidovom algoritmu za određivanje najvećeg zajedničkog delioca celih brojeva.

Sam Euklidov algoritam sastoji se u uzastopnoj primeni tvrđenja iskazanog u Teoremi 1. Neka su a i b zadati celi brojevi, pri čemu je $a > b$. Tada su, na osnovu Teoreme 1., jednoznačno određeni nenegativni celi

brojevi q_i i r_i, $1 \leqslant i \leqslant k+1$, tako da je

$$\begin{aligned}
a &= q_1 b + r_1\,, & 0 < r_1 < b\,;\\
b &= q_2 r_1 + r_2\,, & 0 < r_2 < r_1\,;\\
r_1 &= q_3 r_2 + r_3\,, & 0 < r_3 < r_2\,;\\
&\cdots & \cdots\\
r_{k-3} &= q_{k-1} r_{k-2} + r_{k-1}\,, & 0 < r_{k-1} < r_{k-2}\,;\\
r_{k-2} &= q_k r_{k-1} + r_k\,, & 0 < r_k < r_{k-1}\,;\\
r_{k-1} &= q_{k+1} r_k + 0\,, & (r_{k+1} = 0)\,.
\end{aligned}$$

Niz gornjih jednakosti nazivamo Euklidovim algoritmom dužine n za brojeve a i b. Reč algoritam podrazumeva konačnu automatsku proceduru za izračunavanje nekog objekta.

Brojevi $r_1, r_2, \ldots, r_{k-1}, r_k$ u Euklidovom algoritmu čine opadajući niz prirodnih brojeva manjih od b, što znači da se gore opisani postupak mora završiti posle konačnog broja koraka. Koristeći ovu činjenicu i prethodnu teoremu lako se dokazuje da za svaka dva cela broja postoji jedinstven Euklidov algoritam.

Sada možemo iskazati teoremu koja daje odgovor na pitanje određivanja najvećeg zajedničkog delioca dva broja.

Teorema 2. *Najveći zajednički delioc celih brojeva a i b, $b \neq 0$, je broj $(a, b) = r_k$, gde je r_k poslednji pozitivan ostatak dobijen primenom Euklidovog algoritma na prirodne brojeve a i b.*

Dokaz : Da dokažemo teoremu, pokazaćemo da su zadovoljena sledeća dva tvrđenja:

(a) $r_k \,|\, a$ i $r_k \,|\, b$;
(b) ako $d \,|\, a$ i $d \,|\, b$, tada $d \,|\, r_k$.

Zaista, iz poslednje jednakosti Euklidovog algoritma sledi da $r_k \,|\, r_{k-1}$. Na osnovu toga i pretposlednje jednakosti zaključujemo da $r_k \,|\, r_{k-2}$. Nastavljajući ovaj postupak dobijamo da $r_k \,|\, r_{k-3}$,..., $r_k \,|\, b$, a onda iz prve jednakosti sledi da $r_k \,|\, a$, čime smo dokazali da je uslov (a) zadovoljen.

Da dokažemo da je i uslov (b) zadovoljen, pretpostavimo da je d prirodan broj koji deli brojeve a i b. Tada iz prve jednakosti Euklidovog algoritma odmah sledi da $d \,|\, r_1$, iz druge da $d \,|\, r_2$,...,$d \,|\, r_{k-1}$, i konačno, iz pretposlednje jednakosti sledi da $d \,|\, r_k$, čime je teorema dokazana.

Primer 1. Da bi smo ilustrovali efikasnost, ali i jednostavnost Euklidovog algoritma za određivanje najvećeg zajedničkog delioca dva broja, odredimo $(936, 588)$.

Rešenje : Prema Euklidovom algoritmu imamo sledeći niz:

$$\begin{aligned} 936 &= 1 \cdot 588 + 348\,, \\ 588 &= 1 \cdot 348 + 240\,, \\ 348 &= 1 \cdot 240 + 108\,. \\ 240 &= 2 \cdot 108 + 24 \\ 108 &= 4 \cdot 24 + 12 \\ 24 &= 2 \cdot 12\,. \end{aligned}$$

Dakle, $(936, 588) = 12$.

Vratimo se ponovo Euklidovom algoritmu i napišimo ostatke na sledeći način:

$$\begin{aligned} r_1 &= a - q_1 b\,, \\ r_2 &= b - q_2 r_1\,, \\ r_3 &= r_1 - q_3 r_2\,, \\ &\cdots \\ r_{k-1} &= r_{k-3} - q_{k-1} r_{k-2}\,, \\ r_k &= r_{k-2} - q_k r_{k-1}\,. \end{aligned}$$

Vidimo da se u ovom nizu, počev od trećeg, svaki član izražava pomoću svoja dva prethodnika kao celobrojna linearna kombinacija. Ako sada pođemo od poslednjeg člana r_k u navedenom nizu, zaključujemo da se on može izraziti kao linearna kombinacija brojeva a i b sa celobrojnim koeficijentima:

$$r_k = ax + by\,, \quad x\,, y \in \mathbb{Z}\,.$$

Time smo dokazali sledeću teremu.

Teorema 3. *Ako su a i b celi brojevi, tada jednačina*

$$ax + by = (a, b) \tag{4}$$

ima bar jedno celobrojno rešenje.

Ovu teoremu možemo lepo iskoristiti za rešavanje diofantskih jednačina oblika $ax + by = (a, b)$. Pokažimo to na sledećem primeru.

Primer 2. Naći bar jedno celobrojno rešenje jednačine $936x + 588y = 12$.

Rešenje: Kako je $(936, 588) = 12$, za rešavanje zadate jednačine primenićemo proceduru navedenu nakon Primera 1.

$$\begin{aligned} 12 &= 108 - 4 \cdot 24 = \\ &= 108 - 4(240 - 2 \cdot 108) = \\ &= 9 \cdot 108 - 4 \cdot 240 = \\ &= 9(348 - 240) - 4 \cdot 240 = \\ &= 9 \cdot 348 - 13 \cdot 240 = \\ &= 9 \cdot 348 - 13(588 - 348) = \\ &= 22 \cdot 348 - 13 \cdot 588 = \\ &= 22(936 - 588) - 13 \cdot 588 = \\ &= 22 \cdot 936 - 35 \cdot 588\,. \end{aligned}$$

Jedno celobrojno rešenje zadate jednačine je $x = 22$, $y = -35$.

Neka je sada f proizvoljan delioc brojeva a i b. Tada su $\frac{a}{f}$ i $\frac{b}{f}$ celi brojevi, pa je zbog (4)

$$\frac{a}{f}\,x + \frac{b}{f}\,y = \frac{(a,b)}{f}\,,$$

odakle sledi da je izraz na desnoj strani poslednje jednakosti ceo broj. No to onda znači da $f \mid (a, b)$, čime smo dokazali sledeće tvrđenje.

Teorema 4. *Najveći zajednički delioc dvaju brojeva deljiv je svakim drugim zajedničkim deliocem tih brojeva.*

U prethodnom izlaganju videli smo značaj Teoreme 1. Navedimo na kraju ovog dela još jedan divan primer primene ove teoreme.

Teorema 5. *Neka je b ceo broj veći od 1. Tada se svaki pozitivan ceo broj m na jedinstven način može prikazati u obliku*

$$m = a_n b^n + a_{n-1} b^{n-1} + \cdots + a_0\,, \tag{5}$$

gde je $0 < a_n < b$ i $0 \leqslant a_i < b$, za $i = 0, 1, \ldots, n-1$.

Dokaz : Za dato $m \in \mathbb{Z}$ i $b > 1$ na osnovu Teoreme 1. postoje jedinstveno određeni celi brojevi q_0 i a_0 za koje važi

$$m = q_0 b + a_0\,, \qquad 0 \leqslant a_0 < b\,.$$

Očigledno je $q_0 \geqslant 0$. Ako je $q_0 = 0$ teorema je dokazana. Ako je q_0 pozitivan broj, deljenjem q_0 sa b dobijamo

$$q_0 = q_1 b + a_1, \qquad 0 \leqslant a_1 < b\,,$$

gde su q_1 i a_1 prema Teoremi 1. jedinstveno određeni celi brojevi. Nastavljajući ovaj postupak dobijamo

$$\begin{array}{lll}
m = q_0 b + a_0\,, & 0 \leqslant a_0 < b\,, & q_0 > 0\,,\\
q_0 = q_1 b + a_1\,, & 0 \leqslant a_1 < b\,, & q_1 > 0\,,\\
q_1 = q_2 b + a_2\,, & 0 \leqslant a_2 < b\,, & q_2 > 0\,,\\
\quad\cdots & \cdots & \cdots\\
q_{n-2} = q_{n-1} b + a_{n-1}\,, & 0 \leqslant a_{n-1} < b\,, & q_{n-1} > 0\,,\\
q_{n-1} = q_n b + a_n\,, & 0 \leqslant a_n < b\,, & q_n = 0\,.
\end{array}$$

Kako je $m > q_0 > q_1 > \cdots > 0$ sledi da je na ovaj način jednoznačno određen ceo pozitivan broj q_{n-1} koji je manji od broja b. Iz poslednje jednakosti imamo da je $a_n = q_{n-1}$, pa je koeficijent a_n pozitivan broj.

Zamenom dobijamo da je

$$\begin{aligned}
m \;&= q_0 b + a_0 =\\
&= (q_1 b + a_1) b + a_0 = q_1 b^2 + a_1 b + a_0 =\\
&\cdots\cdots\cdots\\
&= (q_{n-1} b + a_{n-1}) b^{n-1} + \cdots + a_1 b + a_0 =\\
&= q_{n-1} b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0 =\\
&= a_n b^n + a_{n-1} b^{n-1} + \cdots + a_1 b + a_0\,.
\end{aligned}$$

Dobijena reprezentacija broja m je jedinstvena, jer su koeficijenti a_i, $i = 0, 1, \ldots, n$, na osnovu Teoreme 1. jednoznačno određeni.

Ako su zadovoljeni uslovi Teoreme 4., tada za broj m predstavljen u obliku (5) kažemo da je napisan u brojevnom sistemu za osnovu b. Broj **b** je **baza** ili **osnova** datog brojevnog sistema, a sam broj m zapisujemo u obliku

$$(a_n a_{n-1} \cdots a_0)_b\,.$$

Primer 3. Dokazati da se svaki prirodan broj na jedinstven način može predstaviti kao zbir različitih stepena broja 2.

Rešenje : Na osnovu dokazane teoreme, svaki prirodan broj m može se na jedinstven način napisati kao

$$m = a_n \cdot 2^n + a_{n-1} \cdot 2^{n-1} + \cdots + a_1 \cdot 2^1 + a_0 \cdot 2^0 \,,$$

gde su $a_n, \ldots, a_1, a_0 \in \{0, 1\}$.

Da bi smo izložili Euklidov algoritam za polinome, uvedimo najpre neke pojmove i oznake.

Označimo sa $\mathbb{N}_1 = \mathbb{N}_0 \cup \{-\infty\}$ skup na kome je uređenje definisano kao ekstenzija uređenja na $\mathbb{N}_0$, pri čemu je $-\infty$ najmanji element u tom skupu. Funkciju max dodefinišimo tako da je maksimum praznog skupa jednak $-\infty$. Operacija sabiranja na $\mathbb{N}_1$ je proširenje operacije $+$ sa $\mathbb{N}$ tako da $-\infty + x = -\infty$.

Neka je $n \in \mathbb{N}_1$ i $(a_n)_{n\in\mathbb{N}}$ niz brojeva takav da je $n = \max\{i : a_i \neq 0\}$. Izraz $p(x) = \sum_{i\leqslant n} a_i x^i$ nazivamo **polinomom stepena n sa nizom koeficijenata** $(a_n)_{n\in\mathbb{N}_0}$. 0 je polinom stepena $-\infty$ sa nizom koeficijenata $(0)_{i\in\mathbb{N}_0}$. Polinome stepena 0 nazivamo konstantnim polinomima ili konstantama. Sa $R[x]$ označimo skup polinoma nad poljem realnih brojeva, odn. polinome sa koeficijentima iz skupa realnih brojeva. Sa $st(p)$ označavamo stepen polinoma $p \in R[x]$.

Kao i za cele brojeve, tako i za polinome važi teorema koja je u osnovi Euklidovog algoritma.

Teorema 6. *Neka su $p, s \in R[x]$, $s \neq 0$. Tada postoje jedinstveni polinomi $q, r \in R[x]$ tako da je*

$$p = qs + r \,, \qquad st(r) < st(s) \,.$$

Dokaz : Dokažimo najpre egzistenciju polinoma q i r. Dokaz izvodimo transfinitnom indukcijom po $st(p)$. Pretpostavimo da je tvrđenje dokazano za sve polinome stepena manjeg od n. Dokažimo da tvrđenje važi za polinom p stepena n. Neka je $st(p) < st(s)$. Tada je $p = 0 \cdot s + p$ i $st(p) < st(s)$, dakle $q = 0$ i $r = s$ zadovoljavaju uslove teoreme. Neka je sada $st(p) \geqslant st(s)$, i neka je $p(x) = \sum_{i\leqslant n} a_i x^i$ i $s(x) = \sum_{i\leqslant m} b_i x^i$. Neka je $u = \frac{a_n}{b_m} x^{n-m} \cdot s$. Tada je $st(u) = (n-m) + m = n$. Vodeći koeficijent

polinoma u je $\frac{a_n}{b_m} \cdot b_m = a_n$. Stoga je $st(p-u) < n$. Zato, na osnovu indukcijske hipoteze, postoje polinomi q_1 i r tako da je $p-u = s \cdot q_1 + r$ i $st(r) < st(s)$. Otuda je

$$p = u+(p-u) = \left(\frac{a_n}{b_m}x^{n-m}\right)\cdot s+q_1 s+r = \left(\frac{a_n}{b_m}x^{n-m}+q_1\right)\cdot s+r = qs+r\,.$$

Polinomi $q = \frac{a_n}{b_m}x^{n-m}+q_1$ i r zadovoljavaju uslove tvrđenja.

Dokažimo jedinstvenost. Neka je $p = qs + r = q_1 s + r_1$ i $0 \leqslant st(r), st(r_1) < st(s)$. Tada je $s(q-q_1) = r - r_1$. Kako je $st(r_1 - r) \leqslant \max\{st(r), st(r_1)\} < st(s)$, to je $st(s(q-q_1) < st(s)$. Prema formuli za stepen proizvoda, $st(s) + st(q-q_1) < st(s)$. No onda je $st(q-q_1) < 0$. Dakle, $st(q-q_1) = -\infty$, tj. $q - q_1 = 0$, odn. $q = q_1$. Kako je $q = q_1$, to je $r = r_1$.

Neka su $p, s \in R[x]$, $p, s \neq 0$. Označimo sa $D(p,s) = \{t \in R[x] : t \,|\, p\,,\ t \,|\, s\}$. Polinom $d \in R[x]$ je **najveći zajednički delioc** polinoma p i s ako $d \in D(p,s)$ i ako za svako $t \in D(p,s)$, $t \,|\, d$. Najveći zajednički delioc polinoma p i s označavamo sa (p,s).

Kako iz $t \,|\, d$ sledi $t \,|\, ad$ za ma koju ne-nula konstantu a, najveći zajednički delioc polinoma nije jedinstveno određen. Kako se oni sadrže jedan u drugom, razlikuju se do na umnožka konstantom. Jednoznačnosti radi, za najveći zajednički delioc se u tom slučaju može definisati onaj polinom iz te klase čiji je najstariji član jednak jedinici.

Niz jednakosti

$$\begin{aligned}
p &= sq_1 + r_1\,, & 0 < st(r_1) < st(s)\,,\\
s &= r_1 q_2 + r_2\,, & 0 < st(r_2) < st(r_1)\,,\\
r_1 &= r_2 q_3 + r_3\,, & 0 < st(r_3) < st(r_2)\,,\\
&\cdots & \cdots\\
r_{n-2} &= r_{n-1}q_n + r_n\,, & 0 < st(r_n) < st(r_{n-1})\,,\\
r_{n-1} &= r_n q_{n+1}\,.
\end{aligned}$$

nazivamo Euklidovim algoritmom dužine n za polinome p i s.

Kao i za cele brojeve, i za polinome važe teoreme analogne već navedenim teoremama za brojeve. Dokazi ovih teorema zasnovani su na Teoremi 6..

Teorema 7. *Za svaka dva polinoma $p, s \in R[x]$, $s \neq 0$, postoji jedinstven Euklidov algoritam, pri čemu je $(p,s) = r_n$, gde je r_n poslednji ostatak u Euklidovom algoritmu koji je različit od nula polinoma.*

Teorema 8. *Za svaka dva polinoma $p, s \in R[x] \setminus \{0\}$ postoje polinomi $u, v \in R[x]$ tako da je $pu + sv = (p, s)$.*

Na kraju navedimo za polinome dva primera u kojima se koristi Euklidov algoritam.

Primer 4. Odrediti najveći zajednički delioc polinoma $p_1(x) = x^4 + 2x^3 + 3x^2 + 2x + 1$ i $p_2(x) = x^4 + x^3 + 2x^2 + x + 1$.

Rešenje: Euklidov algoritam za polinome $p_1(x)$ i $p_2(x)$ izražen je sledećim jednakostima:

$$\begin{aligned} &x^4 + 2x^3 + 3x^2 + 2x + 1 = (x^4 + x^3 + 2x^2 + x + 1) \cdot 1 + x^3 + x^2 + x\,, \\ &x^4 + x^3 + 2x^2 + x + 1 = (x^3 + x^2 + x) \cdot x + x^2 + x + 1\,, \\ &x^3 + x^2 + x = (x^2 + x + 1) \cdot x\,. \end{aligned}$$

Najveći zajednićki delioc polinoma $p_1(x)$ i $p_2(x)$ je polinom $x^2 + x + 1$.

Primetimo da za zadate polinome važe faktorizacije $p_1(x) = (x^2 + x + 1)^2$, $p_2(x) = (x^2 + x + 1)(x^2 + 1)$ koje nije baš najednostavnije odrediti.

Primer 5. Dati su polinomi $p_1(x) = 3x^3 - 2x^2 + x + 2$ i $p_2(x) = x^2 - x + 1$. Odrediti polinome $q_1(x)$ i $q_2(x)$ tako da je

$$p_1(x)q_2(x) + p_2(x)q_1(x) = 1\,.$$

Rešenje: Euklidov algoritam za polinome $p_1(x)$ i $p_2(x)$ dat je sledećim jednakostima:

$$\begin{aligned} &3x^3 - 2x^2 + x + 2 = (3x + 1)(x^2 - x + 1) + (-x + 1)\,, \\ &x^2 - x + 1 = (-x + 1)(-x) + 1\,. \end{aligned}$$

Najveći zajdnički delioc polinoma $p_1(x)$ i $p_2(x)$ je 1, pa su oni uzajimno prosti. Stoga zadatu jednačinu možemo rešiti primenom Euklidovog algoritma iz koga dobijamo da je

$$\begin{aligned} &= x^2 - x + 1 + x(-x + 1) = \\ &= x^2 - x + 1 + x[(3x^3 - 2x^2 + x + 2) - (3x + 1)(x^2 - x + 1)] = \\ &= (3x^3 - 2x^2 + x + 2) \cdot x + (x^2 - x + 1)(-3x^2 - x + 1)\,, \end{aligned}$$

pa je $q_1(x) = -3x^2 - x + 1$, a $q_2(x) = x$.

Adresa autora:

Prirodno-matematički fakultet, Univerzitet u Nišu