Dodatek B

Evklidov algoritem

S pomočjo Evklidovega algoritma poiščemo največji skupni delitelj dveh naravnih (ali celih) števil. Če sta a in b dve celi števili, potem lahko a delimo z b in to zapišemo $a = sb + r$, kjer je r ostanek pri deljenju in velja $0 \leq r < |b|$.

Evklidov algoritem: Imamo dani dve neničelni celi števili a in b; denimo, da je $|a| \geq |b|$. Potem z deljenjem poiščemo taka cela števila $s_1, s_2, \ldots$ in $r_1, r_2, \ldots$, da velja

$$\begin{array}{rcl} a &=& s_1 b + r_1 \\ b &=& s_2 r_1 + r_2 \\ r_1 &=& s_3 r_2 + r_3 \\ r_2 &=& s_4 r_3 + r_4 \\ & \vdots & \end{array}$$

in $|b| > r_1 > r_2 > r_3 > \cdots \geq 0$. Algoritem se ustavi, ko je $r_k = 0$. Ker je naravnih števil manjših od $|b|$ končno mnogo, se bo algoritem zagotovo ustavil v končno korakih. Denimo, da je k-tem koraku $r_k = 0$ in $r_{k-1} \neq 0$. Potem je r_{k-1} največji skupni delitelj a in b. Kako to dokažemo? Poglejmo si nekaj zadnjih korakov Evklidovega algoritma:

$$\begin{array}{rcl} r_{k-2} &=& s_k r_{k-1} \\ r_{k-3} &=& s_{k-1} r_{k-2} + r_{k-1} \\ r_{k-4} &=& s_{k-2} r_{k-3} + r_{k-2} \ . \end{array}$$

Iz prve od teh enakosti sledi, da r_{k-1} deli r_{k-2}. Potem iz druge enakosti sledi, da r_{k-1} deli r_{k-3} in iz tretje, da r_{k-1} deli r_{k-4}. Zgornji sklep ponavljamo, dokler ne dobimo, da r_{k-1} deli tako b kot tudi a. Torej je r_{k-1} skupni delitelj

a in b. Obratno, če je q skupni delitelj a in b, potem deli r_1, kar vidimo iz prve enakosti v Evklidovem algoritmu. Iz druge enakosti dobimo, da q deli r_2, itd. Tako sledi, da q deli r_{k-1} in je zato r_{k-1} res največji skupni delitelj a in b. Pišemo tudi $d(a,b) = r_{k-1}$, oziroma samo $d = d(a,b)$.

Zgled B.1 Poiščimo največji skupni delitelj števil 144 in 40:

$$\begin{array}{rcl} 144 &=& 3 \cdot 40 + 24 \\ 40 &=& 1 \cdot 24 + 16 \\ 24 &=& 1 \cdot 16 + 8 \\ 16 &=& 2 \cdot 8 + 0 \end{array}$$

Torej je največji skupni delitelj 144 in 40 enak 8. $\square$

S pomočjo Evklidovega algoritma lahko poiščemo taki celi števili p in q, da je $p \cdot a + q \cdot b = d$, kjer je d največji skupni delitelj a in b. Kako to naredimo? Iz prve enakosti v algoritmu dobimo

$$r_1 = a - s_1 b \ .$$

Potem iz druge enakosti sledi

$$r_2 = -s_2 a + (1 + s_1) b \ .$$

Nadaljujemo z vstavljanjem $r_2, r_3, \ldots$, dokler iz predzadnje enakosti ne dobimo zveze

$$r_{k-1} = pa + qb$$

za neki celi števili p in q.

Zgled B.2 Izrazimo 8 v obliki $p \cdot 144 + q \cdot 40$. Računajmo:

$$\begin{array}{rcl} 24 &=& 144 - 3 \cdot 40 \\ 16 &=& 40 - (144 - 3 \cdot 40) = -144 + 4 \cdot 40 \\ 8 &=& (144 - 3 \cdot 40) + 144 - 4 \cdot 40 = 2 \cdot 144 - 7 \cdot 40 \ . \end{array}$$

Torej je $p = 2$ in $q = -7$. $\square$

Definicija B.3 Rečemo, da sta celi števili a in b *tuji*, če je njun največji skupni delitelj enak 1. $\Diamond$

Če sta a in b tuji, potem obstajata taki celi števili p in q, da je $pa + qb = 1$.

Evklidov algoritem lahko uporabimo tudi za iskanje največjega skupnega delitelja dveh polinomov. Naj bo $K = \mathcal{O}[x]$ kolobar polinomov s koeficienti v komutativnem obsegu $\mathcal{O}$. Če sta $a(x)$ in $b(x)$ dva polinoma, potem lahko $a(x)$ delimo z $b(x)$ in dobimo

$$a(x) = s(x)b(x) + r(x) \ \ .$$

Pri tem je $0 \leq \operatorname{st} r < \operatorname{st} b$. Tu smo s $\operatorname{st} p$ označili stopnjo polinoma p.

V kolobarju K je največji skupni delitelj določen do neničelnega skalarnega faktorja natanko.

Zgled B.4 Poiščimo največji skupni delitelj polinomov $a(x) = x^4 - 3x^2 - 4$ in $b(x) = x^3 + 2x^2 - x - 2$ v $K = \mathbb{R}[x]$.
Velja:

$$\begin{aligned} x^4 - 3x^2 - 4 &= (x-2)(x^3 - 3x^2 - 4) + (2x^2 - 8) \\ x^3 + 2x^2 - x - 2 &= (\frac{1}{2}x + 1)(2x^2 - 8) + (3x - 6) \\ 2x^2 - 8 &= (\frac{2}{3}x - \frac{4}{3})(3x - 6) + 0 \ \ . \end{aligned}$$

Največji skupni delitelj je torej $3x - 6$. Lahko pa vzamemo $d(a,b) = x - 2$. Z vstavljanjem dobimo, da je

$$x - 2 = \left(-\frac{1}{6}x - \frac{1}{3}\right) a(x) + \left(\frac{1}{6}x^2 - \frac{1}{3}\right) b(x) \ \ . \qquad \square$$