OZADJE RAZŠIRJENEGA EVKLIDOVEGA ALGORITMA

Naj bosta m in n pozitivni celi števili. Radi bi poiskali njun največji skupni delitelj d. Množico skupnih (pozitivnih) deliteljev števil m in n označimo z D,

$$D = \{k \in \mathbb{Z} \; ; \; k > 0 \wedge k|m \wedge k|n\},$$

množico vseh pozitivnih celoštevilskih linearnih kombinacij števil m in n pa z L,

$$L = \{s \cdot m + t \cdot n \; ; \; s \in \mathbb{Z} \wedge t \in \mathbb{Z} \wedge s \cdot m + t \cdot n > 0\}.$$

Očitno nobena izmed množic D in L ni prazna. Gotovo $1 \in D$ in $m = 1 \cdot m + 0 \cdot n \in L$ ter tudi $n = 0 \cdot m + 1 \cdot n \in L$. Največje število iz D, $d = \max D$ je *največji skupni delitelj števil m in n*. Pišemo tudi $d = \gcd(m, n)$. Enostavno je videti, da obstaja tudi najmanjše število iz L, označimo ga z $\ell = \min L$.

Trditev. *Velja* $\max D = \min L$. *To pomeni, da* $\gcd(m, n)$ *lahko poiščemo tako, da poiščemo najmanjšo pozitivno celoštevilsko linearno kombinacijo števil m in n.*

Najprej premislimo:

(1) Če je $a \in D$ in $b \in L$, potem je $a \leq b$. Vsak element množice D je manjši ali enak od vsakega elementa iz množice L.

Naj bo a *poljuben* element množice D. Po definiciji je a strogo pozitiven in *deli* tako m kot n. Torej a deli tudi izraz $s \cdot m + t \cdot n$, če sta le s in t celi števili. Odtod sklepamo, da a deli vsako celoštevilsko linearno kombinacijo števil m in n. In če je takšna celoštevilska linearna kombinacija strogo pozitivna, potem nikakor ne more biti manjša od a-ja: (1) torej velja.

(2) Naj bosta $\ell_1, \ell_2 \in L$. Privzemimo še, da je $\ell_1 > \ell_2 > 0$ in tudi, da ℓ_2 *ne deli* ℓ_1. Potem obstaja $\ell_3 \in L$, za katerega velja $\ell_2 > \ell_3 > 0$.

Zapišimo ℓ_1 in ℓ_2 kot celoštevilski linearni kombinaciji m in n: $\ell_1 = s_1 \cdot m + t_1 \cdot n$ in $\ell_2 = s_2 \cdot m + t_2 \cdot n$.

Uporabimo izrek o deljenju naravnih števil. Pišemo lahko $\ell_1 = k \cdot \ell_2 + \ell_3$, pri čemer sta $k, \ell_3 \in \mathbb{Z}$ in je $0 < \ell_3 < \ell_2$, saj ℓ_2 ne deli števila ℓ_1. Zdaj je potrebno samo še izraziti ℓ_3 kot linearno kombinacijo števil m in n. Računajmo:

$$\begin{aligned}
\ell_3 &= \ell_1 - k \cdot \ell_2 \\
&= (s_1 \cdot m + t_1 \cdot n) - k(s_2 \cdot m + t_2 \cdot n) \\
&= (s_1 - k \cdot s_2)m + (t_1 - k \cdot t_2)n
\end{aligned}$$

Torej je tudi ℓ_3 pozitivna celoštevilska linearna kombinacija števil m in n in zato $\ell_3 \in L$. S tem smo pokazali pravilnost (2).

(3) Naj bo $\ell = \min L$, najmanjše število iz L. Tedaj ℓ deli *vse* druge elemente množice L.

Denimo, da ℓ ne deli elementa $\ell_0 \in L$, za katerega po definiciji velja $\ell_0 > \ell$. Z uporabo točke (2) lahko poiščemo element $x \in L$, za katerega velja $0 < x < \ell$. To je v protislovju z dejstvom, da je ℓ najmanjši element množice L in zato (3) drži.

Na koncu opazimo, da tudi $m, n \in L$. Po (3) ℓ *deli* tudi m in n. Zato $\ell \in D$ in po Po (1) velja $\ell = \max D$. S tem je zaključen tudi dokaz trditve.

■