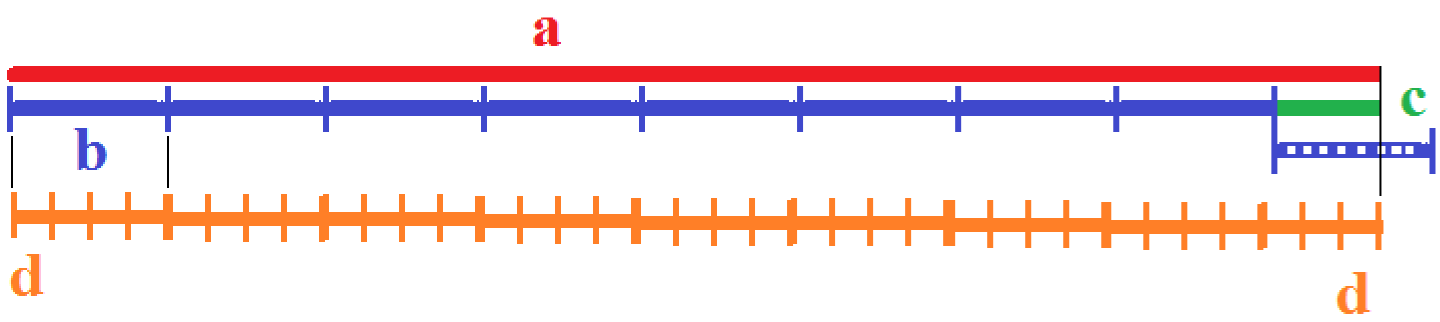
Maradékos osztás, *lnko*, összemérhetőség, Euklideszi algoritmus szakaszokkal

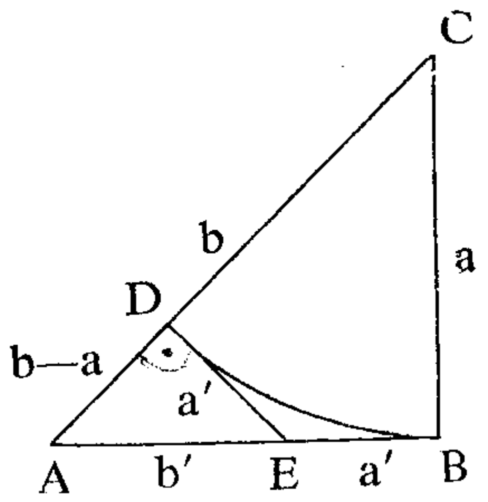


$a = b * k + c$, $c < b$ $(k=8)$

$lnko(a,b) = d$

$a , b , c , d \in R$

Ezt a módszert EUKLEIDÉSZ a VII. könyv elején számokra alkalmazza a legnagyobb közös osztó meghatározása céljából, a X. könyv elején pedig tetszőleges mennyiségekre, hogy megállapítsa, van-e közös mérték, s ha igen, úgy azt meghatározza. Ha azonban ezt a módszert összemérhetetlen mennyiségekre alkalmazzuk, akkor a folyamat minden határon túl folytatódik.



64. ábra

Ha pl. a egy négyzet oldala, b pedig az átlója, akkor a-t egyszer tudjuk levonni b-ből (lásd a 64. ábrát). A

$$b-a = AD = DE = EB = a'$$

maradékot megint levonhatjuk $a = AB$-ből, akkor $b' = AE$ marad. Most azonban a' és b' ismét egy kisebb oldal négyzete, illetve átlója

Waerden: 208.old.

$$lnko(94542, 24981) = \mathbf{?}$$

$$\begin{aligned}
(94542) &= (24981) \cdot 3 + (19599) \\
(24981) &= (19599) \cdot 1 + (5382) \\
(19599) &= (5382) \cdot 3 + (3453) \\
(5382) &= (3453) \cdot 1 + (1929) \\
(3453) &= (1929) \cdot 1 + (1524) \\
(1929) &= (1524) \cdot 1 + (405) \\
(1524) &= (405) \cdot 3 + (309) \\
(405) &= (309) \cdot 1 + (96) \\
(309) &= (96) \cdot 3 + (21) \\
(96) &= (21) \cdot 4 + (12) \\
(21) &= (12) \cdot 1 + (9) \\
(12) &= (9) \cdot 1 + (3) \\
(9) &= (3) \cdot 3 + (0)
\end{aligned}$$

$$lnko(94542, 24981) = 3$$

$$lnko(94542, 24981) = \textbf{?}$$

$$\begin{aligned}
(94542) &= (24981) \cdot 3 + (19599) \\
(24981) &= (19599) \cdot 1 + (5382) \\
(19599) &= (5382) \cdot 3 + (3453) \\
(5382) &= (3453) \cdot 1 + (1929) \\
(3453) &= (1929) \cdot 1 + (1524) \\
(1929) &= (1524) \cdot 1 + (405) \\
(1524) &= (405) \cdot 3 + (309) \\
(405) &= (309) \cdot 1 + (96) \\
(309) &= (96) \cdot 3 + (21) \\
(96) &= (21) \cdot 4 + (12) \\
(21) &= (12) \cdot 1 + (9) \\
(12) &= (9) \cdot 1 + (3) \\
(9) &= (3) \cdot 3 + (0)
\end{aligned}$$

$$lnko(94542, 24981) = 3$$

XXI. századi alkalmazás: kódolás, hibajavítás, titkosírások, ...

Készítette: dr. Szalkai István, 2016.