A komplementer prímszita (CPS) tétel alkalmazása S.W. Golomb primfaktorizációs módszerére

Dénes Tamás

Budapest, 2001. április

S.W. Golomb "On factoring Jevons' number"[1] cikkében a Jevons szám faktorizációja kapcsán bemutat egy általános eljárást a két prímtényezős szorzatok prímtényezőinek meghatározására. Ha J jelöli a szorzatot, akkor a módszer alapötlete így írható le:

(1) $$J = p \cdot q = a^2 - b^2 = (a+b)(a-b)$$

ahol a és b természetes számok, p és q prímszámok.

Az (1) összefüggéshez igen egyszerűen számolható, hatékony algoritmust mutat be az a, b számok meghatározására. Az algoritmus lényeges lépései:

- Képezzük az $a_0 = \left[\sqrt{J}\right]$ kezdőértéket.
- Legyen $a_k = a_0 + k$, ahol k=1,2,3,...
- Képezzük az ${a_k}^2 - J$ sorozatot, amíg teljes négyzetet kapunk, azaz

(2) $${a_k}^2 - J = {b_k}^2$$

Ekkor tehát a_k , b_k természetes számok és így teljesül, hogy

(3) $$J = (a_k + b_k)(a_k - b_k)$$

Az eljáráshoz mindössze egy memóriára van szükség, amelyben az aktuális a_k értéket tároljuk. Így akár egy zsebszámológép segítségével elvégezhetők a számítások. Igen meggyőző, hogy a Jevons által 1870-ben megoldhatatlannak tartott feladat, a J=8.616.460.799 szám faktorizációja, S.W. Golomb módszerével $k=56$ lépésben célhoz vezet és megadja az a_{56}=92.880, b_{56}=3199 megoldást[2].

[1] CRYPTOLOGIA, vol. XX. Number 3. 1996. July

[2] ${a_{56}}^2 - {b_{56}}^2 = (a_{56} - b_{56})(a_{56} + b_{56}) = \underbrace{89681}_{p} \cdot \underbrace{96079}_{q} = 8.616.460.799 = J$

Más megközelítésben a Dénes T. C.P.S. tétel (Complementary Prime Sieve) szintén megadja bármely $6k \pm 1$ alakú összetett szám két tényezős prímfelbontását[3], amelynek alakja

(4) $$J = (6u \pm 1)(6v \mp 1) \qquad (u, v = 1,2,3, \ldots)$$

Ha tehát feltételezzük, hogy J-nek két prímtényezője van (lásd (1)), akkor fennáll:

(5) $$J = (a_k + b_k)(a_k - b_k) = (6u \pm 1)(6v \mp 1)$$

A két prímtényezőre vonatkozó feltétel miatt (5)-ből következik, hogy

(6) $$\begin{aligned} a_k + b_k &= 6u \pm 1 \\ a_k - b_k &= 6v \mp 1 \end{aligned}$$

A két egyenlet összeadásával adódik:

(7) $$2a_k = 6u + 6v \quad \Rightarrow \quad a_k = 3(u + v)$$

(7)-ből következik, hogy a_k mindig osztható 3-mal. Ha tehát az a_0 kezdőértéket úgy választjuk, hogy

(8) $$h \equiv \left\lceil \sqrt{J} \right\rceil \bmod 3 \quad \Rightarrow \quad a_0 = \left\lceil \sqrt{J} \right\rceil - h$$

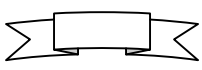
azaz a_0 osztható 3-mal, akkor a Golomb algoritmus szerint:

(9) $$a_k = a_0 + k$$

amely (7) és (8) alapján csak akkor teljesülhet, ha k osztható 3-mal. Így a rekurziós lépések számát harmadára csökkenthetjük, hiszen a $k=1,2,3, \ldots$ lépések helyett csak a $k=3,6,9, \ldots$ esetek kiszámítására van szükség.
A Jevons szám esetén tehát:

(10) $$\begin{aligned} a_0 &\xrightarrow{(8)} 92823 \qquad (h=1) \\ a_{19 \cdot 3} &= 92880 \end{aligned}$$

azaz *56* lépés helyett, *19* lépésben előáll a megoldás.



[3] A C.P.S. tételből kiderül, hogy ha J-nek két prímtényezője van, akkor mindig $6k \pm 1$ alakú. A Jevons szám esetében például: J=8.616.460.799= $6 \cdot 1.436.076.800 - 1$