Az a alapú számrendszer számjegyei:

$$0, 1, 2, \ldots, a-1. \tag{1}$$

Ezek közül csak azok jöhetnek tekintetbe, amelyek *négyzete* velük megegyező számjegyre végződik. Megmutatjuk, hogy az ilyen jegyek mind meg is felelnek: az ilyenre végződő számok *minden hatványa* ugyanarra a jegyre végződik.

Legyen egy ilyen jegy b, vagyis a

$$b^2 - b = b(b-1) \tag{2}$$

különbség 0-ra végződik, osztható a-val. Másrészt a B szám a-alapú számrendszerbeli alakja végződjék b-re, vagyis $B-b$ is osztható a-val. Azt akarjuk megmutatni, hogy ekkor minden k természetes számra B^k, is b-re végződik, azaz $B^k - b$ is osztható a-val. Hogy a második feltételt kihasználhassuk, vonjunk le a különbségből és adjunk is hozzá b^k-t:

$$\begin{aligned} B^k - b = B^k - b^k + b^k - b = (B-b)\big(B^{k-1} + B^{k-2}b + \ldots + Bb^{k-2} + b^{k-1}\big) + \\ + b\big(b^{k-1} - 1\big) = (B-b)\big(B^{k-1} + B^{k-2}b + \ldots + Bb^{k-2} + b^{k-1}\big) + \\ + b(b-1)\big(b^{k-2} + \ldots + b + 1\big), \end{aligned}$$

és ez a feltételek szerint valóban osztható a-val.

Elegendő tehát azokat a b számjegyeket megkeresni, amelyekre a (2) alatti szám osztható a-val. A bal oldal két tényezőjének legnagyobb közös osztója a különbségüknek is osztója, ez viszont 1, tehát b és $b-1$ relatív prímek

Legyen a és b legnagyobb közös osztója a_1, az a, $b-1$ számpáré a_2. Ezek szintén relatív prímek – hiszen (az egységnél nagyobb) közös osztójuk a b, $b-1$ számpárnak is közös osztója lenne –, ezért az $a_1 a_2$ szorzat osztója a-nak.

Fordítva, a is osztója $a_1 a_2$-nek, tehát

$$a_1 a_2 = a. \tag{3}$$

Valóban, legyen az a alapszám törzstényezős felbontása

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}. \tag{4}$$

Ennek minden $p_i^{\alpha_i}$ alakú osztója ($i = 1, 2, \ldots, k$) a fentiek szerint vagy b-nek, vagy $b-1$-nek osztója (de csak az egyiküknek); ezért az első esetben a_1-nek osztója a $p_i^{\alpha_i}$ hatvány, a másodikban a_2-nek, így pedig mindenesetre osztója az $a_1 a_2$ szorzatnak. $i \neq j$ esetlen $p_i^{\alpha_i}$ és $p_j^{\alpha_j}$ relatív prímek, ezért az $a_1 a_2$ szorzat osztható a (4) jobb oldalán álló szorzattal, vagyis a-val, amint állítottuk.

Ezen az úton minden megfelelő b számjegyhez hozzárendeltük az a szám egy (3) alakú felbontását két tényezős szorzatra. Megmutatjuk, hogy minden, ilyen felbontáshoz egyértelműen tartozik egy b számjegy.

Ehhez meg kell keresnünk az a_1 számnak azt a

$$b = a_1 m$$

a-nál kisebb többszörösét, amelyre $b-1$ osztható a_2-vel, azaz amelyet a_2-vel osztva a maradék 1 Osszuk a

$$0,\ 1 \cdot a_1,\ 2 \cdot a_1,\ \ldots,\ (a_2 - 1) \cdot a_1 \tag{5}$$

számokat a_2-vel. Nem lehet, hogy ennek során kétszer ugyanazt a maradékot kapjuk, hiszen ilyen esetben ennek a két többszörösnek, ia_1-nek és különbsége, ja_1-nek, $(i<j)$ különbsége, $(j-i)a_1$ osztható volna a_2-vel. Azonban a_1 és a_2 relatív prímek, ezért a szorzat csak úgy lehetne a_2-vel osztható, ha $(j-i)$ osztható volna a_2-vel. Ámde $0 \leqq i < j < a_2$, így $0 < j - i < a_2$, ezért $j-i$ sem osztható a_2-vel, tehát az (5) alatti számok mondott osztási maradékai mind különbözők.

Az (5) alatt felsorolt többszörösök száma a_2. Másrészt az a_2-vel végzett osztás maradékai

$$0,\ 1,\ 2,\ \ldots,\ a_2 - 1 \tag{6}$$

számok lehetnek, tehát a lehetséges maradékok száma is a_2, így az (5) számok maradékai között minden maradék pontosan egyszer fordul elő. Nevezetesen az 1 maradék is egyszer fordul elő, tehát a választott (3) alakú felbontáshoz valóban egyértelműen hozzátartozik egy (2) alakú szorzat.

Ezek szerint feladatunk megoldásainak a száma egyenlő a (3) alakú felbontások számával. Egy (3) alakú felbontásban az a szám minden törzstényezője vagy a_1, vagy pedig a_2 osztója. A felbontásokat tehát úgy kapjuk meg, hogy a (4) alatti törzstényezőket két csoportba osztjuk. Ismeretes, hogy k különböző elemet 2^k-féleképpen oszthatunk két csoportba, feladatunk megoldásainak száma tehát 2^k, ahol k az a szám törzstényezőinek a száma. (Ebben természetesen benne van a $b=0$, és a $b=1$ triviális megoldás is; $b=0$ az $a_1 = 1$, $a_2 = a$ felbontásból, $b=1$ pedig az $a_1 = a$, $a_2 = 1$ felbontásból.)

Pl. $a = 105 = 3 \cdot 5 \cdot 7$ esetén $k=3$, a felbontások száma $2^k = 8$, és a megfelelő számjegyek: $b = 0,\ 1,\ 15,\ 21,\ 36,\ 70,\ 85,\ 91.$ – Példát láttunk az 1222. gyakorlatban is[1].

Martoni Viktor

[1] K. M. L. 38 (1969) 113. o.