EULERJEVA FUNKCIJA $\varphi(n)$

Definicija. Naj bo $n \in \mathbb{N}$. Število naravnih števil med 1 in n, ki so *tuja* n označimo s $\varphi(n)$:

$$\varphi(n) = |\{k \in \mathbb{N};\ 1 \leq k \leq n \wedge \perp kn\}|$$

Zgledi:

$$\begin{array}{ll} \varphi(4) = 2 & 1,\ \cancel{2},\ 3,\ \cancel{4} \\ \varphi(5) = 4 & 1,\ 2,\ 3,\ 4,\ \cancel{5} \\ \varphi(6) = 2 & 1,\ \cancel{2},\ \cancel{3},\ \cancel{4},\ 5,\ \cancel{6} \end{array}$$

Trditev 1. *Če je p praštevilo, potem je $\varphi(p) = p - 1$.*

Dokaz. Vsa števila med 1 in $p - 1$ so tuja številu p. □

Trditev 2. *Če je p praštevilo, potem je $\varphi(p^n) = p^n - p^{n-1}$.*

Dokaz. Med števili $1, \ldots, p^n$ so natančno večkratniki števila p tista števila, ki *niso* tuja številu p^n. To pa so natanko $1p, 2p, \ldots, p^{n-1}p$. Teh števil je natančno p^{n-1} in dokaz je pri koncu. □

Z $a \bmod k$ označimo ostanek pri deljenju števila a s številom k. Brez dokaza navedimo:

Pomožna trditev.
1. $k \perp ab \Leftrightarrow k \perp a \wedge k \perp b$
2. $k \perp a \Leftrightarrow k \perp a \bmod k$

Trditev 3. $a \perp b \Rightarrow \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$.

Dokaz. Števila med 1 in $a \cdot b$ zapišimo v tabelo.

$$\begin{array}{ccccc} 1 & 2 & 3 & \ldots & a \\ a+1 & a+2 & a+3 & \ldots & 2a \\ 2a+1 & 2a+2 & 2a+3 & \ldots & 3a \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ (b-1)a+1 & (b-1)a+2 & (b-1)a+3 & \ldots & ba \end{array}$$

Števila, ki so tuja produktu ab, morajo biti tuja a in tudi b. Števila v k-tem stolpcu so oblike $na + k$, $0 \leq n \leq b - 1$. Pri deljenju z a dajo vsa omenjena števila isti ostanek, namreč k, torej so bodisi *vsa* tuja a bodisi ni *nobeno* tuje a. Stolpcev, ki vsebujejo številu a tuja števila, je torej natančno $\varphi(a)$.

Pri deljenju z b pa dajejo števila v k-tem stolpcu same različne ostanke. Iz $n_1a + k \equiv n_2a + k (\bmod b)$ namreč sledi $b|(n_1 - n_2)a$, odtod pa $b|(n_1 - n_2)$, saj je $a \perp b$. Ker pa velja $0 \leq n_1, n_2 \leq b - 1$, je $-b + 1 \leq n_1 - n_2 \leq b - 1$. Torej velja $n_1 - n_2 = 0$ in zato $n_1 = n_2$. V vsakem stolpcu je natančno b števil, torej dajejo pri deljenju z b vseh b možnih ostankov.

V tabeli je torej $\varphi(a)$ stolpcev, katerih elementi so tuji a. V vsakem od teh stolpcev pa je $\varphi(b)$ števil, ki so tuji b. Števil, ki so tuja a in tudi b, je potemtakem $\varphi(a) \cdot \varphi(b)$.

Zaključek: $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$. □

S pomočjo Trditev 1, 2 in 3 lahko izračunamo vrednost Eulerjeve funkcije pri poljubnem naravnem številu, če le poznamo njegov praštevilski razcep.

Izrek. *Naj bo $n = p_1^{k_1} \cdot p_2^{k_2} \cdot \cdots \cdot p_m^{k_m}$ praštevilski razcep števila n, kjer so $p_1, p_2, \ldots, p_m$ različna praštevila. Potem je*

$$\varphi(n) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot \cdots \cdot (p_m^{k_m} - p_m^{k_m-1})$$

Zgledi:

$$\begin{array}{l} \varphi(720) = \varphi(16 \cdot 9 \cdot 5) = \varphi(16) \cdot \varphi(9) \cdot \varphi(5) = 8 \cdot 6 \cdot 4 = 192 \\ \varphi(1200) = \varphi(16 \cdot 3 \cdot 25) = \varphi(16) \cdot \varphi(3) \cdot \varphi(25) = 8 \cdot 2 \cdot 20 = 320 \end{array}$$