Predavanje 5

OJLEROVA FUNKCIJA I OJLEROVA TEOREMA

Sada ćemo izvesti eksplicitnu formulu koja daje vrednosti Ojlerove funkcije $\varphi(n)$, polazeći od pretpostavke da je broj $n > 1$ dat u kanoničkom obliku

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \tag{5.1}$$

i to u užem smislu, dakle uz uslov da je $\alpha_i > 0$ za sve $1 \leqslant i \leqslant k$.

Teorema 5.1. *Neka je $n > 1$ prirodan broj dat u kanoničkom obliku* (5.1)*. Tada je*

$$\varphi(n) = \prod_{i=1}^{k} (p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n \cdot \prod_{\substack{p \mid n \\ p \text{ prost}}} \left(1 - \frac{1}{p}\right).$$

Tvrđenje ove teoreme će biti direktna posledica sledeće dve leme.

Lema 5.2. *Za svaki prost broj p i $\alpha \geqslant 1$ važi $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.*

Dokaz. Za prirodan broj $m < p^\alpha$ važi $(m, p^\alpha) = 1$ ako i samo ako je $(m, p) = 1$, odnosno, ako i samo ako $p \nmid m$. Dakle, $\varphi(p^\alpha)$ je broj svih elemenata skupa $\{0, 1, \dots, p^\alpha - 1\}$ koji nisu deljivi sa p, a što je očito $p^\alpha - \lfloor p^\alpha / p \rfloor = p^\alpha - p^{\alpha-1}$. □

Za kompleksnu funkciju $f : \mathbb{Z} \to \mathbb{C}$ jedne celobrojne promenljive (ovakve funkcije se ponekad zovu i *aritmetičke*) kažemo da je *multiplikativna* ako za sve $a, b \in \mathbb{Z}$ takve da je $(a, b) = 1$ važi

$$f(ab) = f(a)f(b).$$

Osim u slučaju kada je funkcija f konstantna nula-funkcija, imamo da je $f(1) = 1$ i $f(-1) \in \{1, -1\}$ (iz tog razloga su zanimljivi jedino pozitivni argumenti, budući da za $a > 0$ važi $f(-a) = f(-1)f(a)$).

Lema 5.3. *Ojlerova funkcija je multiplikativna.*

Dokaz. Pretpostavimo da su $a, b \in \mathbb{Z}^+$ takvi da je $(a, b) = 1$. Posmatraćemo najpre onaj redukovani sistem ostataka $r_1, \dots, r_{\varphi(a)}$ po modulu a koji je sadržan u standardnom potpunom sistemu ostataka po tom modulu, dakle, u skupu $\{0, 1, \dots, a - 1\}$. Imajući u vidu Tvrđenje 4.7, tada su svi brojevi manji od ab koji su uzajamno prosti sa a upravo oni koji su nabrojani u sledećoj tablici:

$$\begin{array}{rrcrcr}
r_1 & r_2 & \dots & r_i & \dots & r_{\varphi(a)} \\
a + r_1 & a + r_2 & \dots & a + r_i & \dots & a + r_{\varphi(a)} \\
\vdots & \vdots & & \vdots & & \vdots \\
ka + r_1 & ka + r_2 & \dots & ka + r_i & \dots & ka + r_{\varphi(a)} \\
\vdots & \vdots & & \vdots & & \vdots \\
(b-1)a + r_1 & (b-1)a + r_2 & \dots & (b-1)a + r_i & \dots & (b-1)a + r_{\varphi(a)}
\end{array}$$

Da bi neki broj (zapravo, ostatak po modulu ab) iz ove tablice bio uzajamno prost sa ab potrebno je i dovoljno da bude uzajamno prost sa b, imajući u vidu Lemu 3.6.

Posmatrajmo sada proizvoljnu kolonu ove tablice, na primer, i-tu kolonu: $r_i, a + r_i, \ldots, (b-1)a + r_i$. Ovaj niz se sastoji od b različitih brojeva. Oni su nekongruentni po modulu b; zaista, $ka + r_i \equiv \ell a + r_i \pmod{b}$ povlači da $b \mid (k - \ell)a$, tj. da $b \mid k - \ell$ (pošto je $(a, b) = 1$). Budući da je $|k - \ell| < b$, sledi da mora biti $k = \ell$. Prema tome, po Tvrđenju 4.5, svaka kolona prethodne tablice čini potpun sistem ostataka po modulu b. Iz tog razloga, svaka kolona sadrži tačno $\varphi(b)$ brojeva koji su uzajamno prosti sa b. Kako tih kolona ima $\varphi(a)$, zaključujemo da u posmatranoj tablici ima tačno $\varphi(a)\varphi(b)$ brojeva koji su uzajamno prosti sa ab. Međutim, po definiciji Ojlerove funkcije, taj broj je istovremeno jednak $\varphi(ab)$, pa željena jednakost $\varphi(ab) = \varphi(a)\varphi(b)$ sledi. □

Dokaz Teoreme 5.1 sada lako sledi iz zapažanja da, uz kanonički oblik (5.1) broja n, multiplikativno svojstvo Ojlerove funkcije daje da važi

$$\varphi(n) = \prod_{i=1}^{k} \varphi(p_i^{\alpha_i}).$$

Leonard Ojler (Leonhard Euler, 1707–1783) je 1736. dokazao tvrđenje u kome funkcija koja danas nosi njegovo ime igra centralnu ulogu i koje predstavlja uopštenje od ranije poznate "male" Fermaove teoreme.

Teorema 5.4 (Ojlerova teorema)**.** *Neka je $a \in \mathbb{Z}$ i $m > 0$ tako da je $(a, m) = 1$. Tada je*

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Dokaz. Neka je $r_1, \ldots, r_{\varphi(m)}$ neki redukovani sistem ostataka po modulu m. Po Tvrđenju 4.8, tada je i $ar_1, \ldots, ar_{\varphi(m)}$ takođe redukovan sistem ostataka po modulu m. To zapravo znači da je preslikavanje $\pi : \{1, \ldots, \varphi(m)\} \to \{1, \ldots, \varphi(m)\}$ definisano sa $\pi(i) = j$ ako i samo ako je $ar_i \equiv r_j \pmod{m}$ bijekcija, tj. permutacija skupa $\{1, \ldots, \varphi(m)\}$. Tako je

$$\begin{aligned} ar_1 &\equiv r_{\pi(1)} \pmod{m}, \\ &\vdots \\ ar_k &\equiv r_{\pi(k)} \pmod{m}, \end{aligned}$$

gde smo radi kraćeg zapisa označili $k = \varphi(m)$. Množeći ove kongruencije, dobijamo

$$a^{\varphi(m)} r_1 \cdots r_k \equiv r_{\pi(1)} \cdots r_{\pi(k)} \pmod{m},$$

pa pošto je $r_1 \cdots r_k = r_{\pi(1)} \cdots r_{\pi(k)}$ i $(r_1 \cdots r_k, m) = 1$, sledi da je

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

kao što se i tražilo. □

Posledica 5.5 (Mala Fermaova teorema)**.** *Neka je p prost broj i $a \in \mathbb{Z}$ takav da $p \nmid a$. Tada je*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Drugim rečima, za sve cele brojeve a važi $a^p \equiv a \pmod{p}$.

Dokaz. Sledi direktno iz Ojlerove teoreme, pošto je $\varphi(p) = p - 1$ za svaki prost broj p. □

Prethodna teorema nosi ime po Pjeru de Fermau (Pierre de Fermat, 1601–1665), francuskom pravniku, jednom od najznačajnijih i najuspešnijih matematičara-amatera svih vremena.