1 Ojlerova funkcija

Definicija 1.1. Ojlerova funkcija je funkcija $\varphi : \mathbb{N} \to \mathbb{N}$ definisana sa $\varphi(n) = |\{m \in \{1, 2, \ldots, n\} : (m, n) = 1\}$ (broj prirodnih brojeva $\leqslant n$ koji su uzajamno prosti sa n).

Ova funkcija je multiplikativna, tj. važi $\varphi(mn) = \varphi(m)\varphi(n)$ ako je $(m, n) = 1$. Kao posledicu ovoga, pošto svaki prirodan broj ima jedinstvenu faktorizaciju na proste brojeve, Ojlerova funkcija je određena vrednostima u stepenima prostim brojevima.

Ako je p prost broj, imamo da je $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$ (Jedini brojevi koji nisu uzajamno prosti sa p^α su stepeni p, kojih ima upravo $p^{\alpha-1}$ između 1 i p. Posebno, za prost broj p važi $\varphi(p) = p - 1$). Prema tome, ako je $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$, tada je

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_k}\right) = \frac{n}{p_1 \ldots p_k}(p_1 - 1)\ldots(p_k - 1).$$

Primer 1.2. $\varphi(120) = \varphi(2^3 \cdot 3 \cdot 5) = 120(1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{5}) = 32.$

Teorema 1.3 (Ojlerova teorema)**.** *Ako za prirodne brojeve a i m važi $(a, m) = 1$, tada je $a^{\varphi(m)} \equiv 1 \pmod m$.*

Teorema 1.4 (Mala Fermaova teorema)**.** *Ako za prirodan broj a i prost broj p važi $p \nmid a$, tada je $a^{p-1} \equiv 1 \pmod p$.*

Ova funkcija ima i sledeća svojstva:

Tvrđenje 1.5. *Za prirodne brojeve m i n, ako sa d obeležimo njihov najveći zajednički delilac, tada je $\varphi(mn) = \varphi(m)\varphi(n)\frac{d}{\varphi(d)}$.*

Tvrđenje 1.6. *Za bilo koji prirodan broj n važi*

$$\sum_{d|n} \varphi(d) = n.$$

1. Odrediti sve prirodne brojeve n za koje je (a) $\varphi(n) = 10$; (b) $\varphi(n) = 8$; (c) $\varphi(n) = 14$.
(a) Neka je $n = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$. Tada je $\frac{n}{p_1 \ldots p_k}(p_1 - 1)\ldots(p_k - 1) = 10$. Vidimo da je $\frac{n}{p_1 \ldots p_k}$ prirodan broj koji deli 10. Nijedan faktor u $\varphi(n)$ oblika $(p_i - 1)$ ne može biti 5, jer 6 nije prost broj.

Ako je $\frac{n}{p_1 \dots p_k} = 1$, tada je jedno $p_i - 1 = 11$, tj. jedan prost faktor je 11. Ako ima još faktora, oni su 1. Dakle, n je ili 11 ili 22 u ovom slučaju.

Ako je $\frac{n}{p_1 \dots p_k} = 5$, tada $5 \mid n$, što znači da je jedan od prostih faktora 5, pa je jedno od $p_i - 1 = 4$. Odavde bi bilo $\varphi(n) \geqslant 20$.

Ako bi bilo $\frac{n}{p_1 \dots p_k} = 10$, ostali faktori bi bili 1, zbog čega bi n moglo biti ili 1 ili 2, a $varphi(n)$ tražimo da bude 10. Dakle jedini n koji zadovoljavaju $\varphi(n) = 10$ su 11 i 22.

2. Da li 10 deli $43^{43} - 17^{17}$?

$$43^{43} - 17^{17} \equiv 3^{43} - 7^{10} \pmod{10},\ \varphi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5}) = 4.$$

Pošto su 3 i 7 uzajamno prosti sa 10, to je po Ojlerovoj teoremi $3^4 \equiv 1 \pmod{10}$ i $7^4 \equiv 1 \pmod{10}$. Odavde je $3^{43} = 3^{10 \cdot 4 + 3} \equiv 3^3 = 27 \equiv 7 \pmod{10}$, a $7^{17} = 7^{4 \cdot 4 + 1} \equiv 7 \pmod{10}$. Dakle, $10 \mid 43^{43} - 17^{17}$.

3. Ako je p prost broj veći od 3, da li $6p$ deli $ab^p - a^p b$, za bilo koje prirodne brojeve a i b?

Po Maloj Fermaovoj teoremi, p deli $ab^p - a^p b$. Pošto je $p > 3$, to su p i 6 uzajamno prosti, pa treba pokazati da 2 i 3 dele $ab^p - a^p b$, što je laka provera.

4. a) Da li 42 deli $n^7 - n$, za bilo koji prirodan broj n?

4. b) Da li 2730 deli $n^{13} - n$, za bilo koji prirodan broj n?

5. Neka su p i q različiti prosti brojevi. Da li važi $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$?

6. Naći ako postoji prost broj p takav da je $5^{p^2} + 1 = (5^p)^p + 1$ deljivo sa p^2.

7. a) Odrediti ostatak pri deljenju 2^{30} sa 13.

7. b) Odrediti poslednju cifru 7^{7^7}.

7. c) Odrediti poslednju cifru 9^{9^9}.

Teorema 1.7 (Vilsonova teorema)**.** *Ako je p prost broj, tada je $(p-1)! \equiv -1$ (mod p), gde je $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (n-1) \cdot n$.*

8. Neka su p i q prosti brojevi, $p > q > 2$. Da li p i q dele $q^{(p+10)!} - (p-2)!$

Po Maloj Fermaovoj teoremi, $q^{p-1} \equiv 1 \pmod{p}$. Pošto $p-1$ deli $(p+10)!$, to je $q^{(p+1)!} \equiv 1 \pmod{p}$. Po Vilsonovoj teoremi $(p-1)! \equiv p-1 \pmod{p}$, pa je $(p-2)! \equiv 1 \pmod{p}$.

Sa druge strane, q svakako deli stepen samog sebe, i pošto su p i q neparni prosti, razlika između njih je barem 2, pa je $q! \leqslant (p-2)!$, odakle q deli $(p-2)!$. Dakle, izraz je deljiv i sa p, i sa q.

9. Ispitati da li za sve proste brojeve p, i za sve cele brojeve a koji nisu deljivi sa p važi da je $a^p + (p-1)!a$ deljivo sa p.