MFT i Eulerov teorem

Katja Varjačić

6.11.2022.

1 Uvod

U ovom predavanju proći ćemo jedan od osnovnih teorema u teoriji brojeva; Mali Fermatov teorem te njegovo poopćenje Eulerov teorem.

Teorem 1.1 (Mali fermatov teorem)
Neka je a cijeli broj i p prost broj koji ne dijeli a. Tada vrijedi:

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

Kako su a i p relativno prosti vrijedi:

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

Također, ukoliko $p \mid a$, onda imamo $a^p \equiv a \equiv 0 \pmod{p}$. Zato tvrdnju malog Fermatovog teorema možemo i ovako izreći:
Za svaki prost broj p i svaki prirodan broj a vrijedi:

$$a^p \equiv a \pmod{p}$$

Dokaz MFT-a možete pogledati ovdje.

Primjer 1.1. Ako su p i q različiti prosti brojevi, dokažite da je broj $p^{q-1} + q^{p-1} - 1$ djeljiv sa pq.

Rješenje: Po malom Fermatovom teoremu imamo $p \mid q^{p-1} - 1$, $q \mid p^{q-1} - 1$, a odavde slijedi $p \mid p^{q-1} + q^{p-1} - 1$, $p \mid p^{q-1} + q^{p-1} - 1$. Budući da su p i q relativno prosti, slijedi tvrdnja zadatka.

Promotrimo sada još jedan primjer u kojem se koristi Mali Fermatov teorem:

Primjer 1.2. Ako prost broj p dijeli $a^p - 1$ za neki $a \in \mathbb{N}$, tada p^2 također dijeli $a^p - 1$. Dokažite.

Rješenje: Prema malom Fermatovom teoremu imamo $a^p \equiv a \pmod{p}$, a prema uvjetu zadatka $a^p \equiv 1 \pmod{p}$. Dakle, $a \equiv 1 \pmod{p}$, tj. $p \mid a - 1$. Nadalje,

$$a^{p-1} + a^{p-2} + \cdots + a + 1 \equiv 1 + 1 + \cdots + 1 + 1 \equiv p \equiv 0 \pmod{p},$$

pa vidimo da vrijedi i $p \mid a^{p-1} + a^{p-2} + \cdots + a + 1$. Zato

$$p^2 \mid (p-1)(a^{p-1} + a^{p-2} + \cdots + a + 1) = a^p - 1$$

Označimo s $\varphi(n)$ broj prirodnih brojeva manjih ili jednakih n koji su relativno prosti s n, za svaki prirodan broj n. Time smo definirali funkciju $\varphi : \mathbb{N} \to \mathbb{N}$ poznatu pod imenom **Eulerova funkcija**.

Za nju postoji i eksplicitna formula. Za $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, gdje su p_i prosti, a α_i prirodni brojevi, imamo:

$$\begin{aligned}\varphi(m) &= m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_r}\right) \\ &= p_1^{\alpha_1-1} p_2^{\alpha_2-1}\cdots p_r^{\alpha_r-1}(p_1-1)(p_2-1)\cdots(p_r-1)\end{aligned}$$

Ona ima svojstvo **multiplikativnosti**, odnosno za bilo koje relativno proste brojeve m i n vrijedi

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$$

Konačno, možemo iskazati **Eulerov teorem** :

Teorem 1.2 (Eulerov teorem)
Ako su a i m relativno prosti brojevi, onda vrijedi

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

Primjer 1.3. Odredimo zadnju znamenku broja 43^{44}.

Rješenje: Budući da je od brojeva manjih od njega, 10 relativno prost s brojevima $1, 3, 7$ i 9, zato je $\varphi(10) = 4$. Kako je 43 relativno prost s 10, vrijedi $43^{44} \equiv (43^{11})^4 \equiv 1 \pmod{10}$, prema Eulerovom teoremu.

Primjer 1.4. Odredimo posljednje dvije znamenke broja 3^{400}.

Rješenje: U ovom primjeru koristit ćemo svojstvo multiplikativnosti Eulerove funkcije te njezinu eksplicitnu formulu. Vrijedi sljedeće:

$$\varphi(100) = \varphi(4)\varphi(25) = 4(1-\frac{1}{2}) \cdot 25(1-\frac{1}{5}) = 40,$$

pa je $3^{40} \equiv 1 \pmod{100}$. Zato je

$$3^{400} \equiv (3^{40})^{10} \equiv 1 \pmod{100}.$$

Primjer 1.5. Pokažite ako je n neparni cijeli broj, onda n dijeli $2^{(n-1)!} - 1$.

Rješenje: Tvrdnja je očita za $n = 1$, pa pretpostavimo $n > 1$. Po Eulerovom teoremu $2^{\varphi(n)} \equiv 1 \pmod{n}$. Kako je $\varphi(n) \leq n - 1$ imamo $(n-1)! = \varphi(n) \cdot k$, za neki cijeli broj k. Dakle,

$$2^{(n-1)!} \equiv 2^{\varphi(n)\cdot k} \equiv \left(2^{\varphi(n)}\right)^k \equiv 1^k \equiv 1 \pmod{n}.$$

Više primjera o Malom Fermatovom i Eulerovom teoremu možete pogledati na: MNM Online predavanje: MFT i Euler.

2 Osnovni lanac

1. **Zadatak** Odredite koliko je $2^{98} \pmod{33}$.

   Rješenje: Računamo $\varphi(33) = \varphi(3) \cdot \varphi(11) = 2 \cdot 10 = 20$. Sada slijedi:

   $$2^{98} \equiv (2^{20})^4 \cdot (2^5)^3 \cdot 2^3 \equiv 1 \cdot (-1)^3 \cdot 8 \equiv -8 \equiv 25 \pmod{33}$$

2. **Zadatak** Za koliko prirodnih brojeva i takvih da $1 \leq i \leq 1000$, postoji prirodan broj j takav da $1 \leq j \leq 1000$ te da je i djelitelj od $2^j - 1$?

   Rješenje: Za parni i očito ne može vrijediti $i | 2^j - 1$. Za neparni i stavimo $j = \varphi(i)$, pa imamo $2^{\varphi(i)} - 1 \equiv 0 \pmod{i}$. Kako je $\varphi(i) < 1000$ slijedi da za svaki neparni i uvijek postoji traženi j pa je odgovor $\frac{1000}{2} = 500$.

3. **Zadatak** Za koje sve proste brojeve p je $29^p + 1$ višekratnik od p?

   Rješenje: Prema Malom Fermatovom teoremu vrijedi

$$29^p \equiv 29 \pmod p$$

   Sada imamo

$$29^p + 1 \equiv 29 + 1 \equiv 30 \equiv 0 \pmod p$$

   Odnosno

$$p|30$$

$$\implies p = \{2, 3, 5\}$$

4. **Zadatak** Ako je $a^p \equiv b^p \pmod p$ dokaži da je tada $a^p \equiv b^p \pmod{p^2}$.

   Rješenje: Iz Malog Fermatovog teorema imamo $a^p \equiv a \pmod p$ i $b^p \equiv b \pmod p$, odnosno znamo da vrijedi

$$a \equiv b \pmod p.$$

   Želimo pokazati $p^2 \mid a^p - b^p$. Dani izraz možemo faktorizirati kao

$$a^p - b^p = (a - b)(a^{p-1} + a^{p-2}b + \cdots ab^{p-2} + b^{p-1}).$$

   Iz pretpostavke zadatka dobili smo da p dijeli lijevu zagradu pa nam je dovoljno pokazati da p dijeli i desnu zagradu. To nam slijedi iz Malog Fermatovog teorema i uvjeta $a \equiv b \pmod p$.

$$\begin{aligned} a^{p-1} + a^{p-2}b + \cdots ab^{p-2} + b^{p-1} &\equiv a^{p-1} + a^{p-1} + \cdots + a^{p-1} + a^{p-1} \pmod p \\ &\equiv 1 + 1 + \cdots + 1 + 1 \pmod p \\ &\equiv p \equiv 0 \pmod p. \end{aligned}$$

5. **Zadatak** Odredite sve proste brojeve p za koje vrijedi da su djelitelj broja $2^p + 1$.

   Rješenje: Iz Malog Fermatovog teorema slijedi

$$2^p + 1 \equiv 2 + 1 \equiv 3 \equiv 0 \pmod p$$

   Pa je onda jedino rješenje $p = 3$.

3 Ozbiljniji lanac

1. **Zadatak** Dokaži da za svaki parni prirodni broj n vrijedi $n^2 - 1 \mid 2^{n!} - 1$.

   Rješenje: Kako $2 \mid n$, imamo da $2 \nmid n - 1$ i $2 \nmid n + 1$. Kako je $n^2 - 1 = (n + 1)(n - 1)$, pokazat ćemo da $n - 1 \mid 2^{n!} - 1$ i $n + 1 \mid 2^{n!} - 1$.

   Vrijedi $\varphi(n + 1) \leq n$ pa zato $\varphi(n + 1) \mid n!$. Po Eulerovom teoremu, $2^{\varphi(n+1)} \equiv 1 \pmod{n + 1}$. Dakle, $2^{n!} \equiv 2^{k\varphi(n+1)} \equiv (2^{\varphi(n+1)})^k \equiv 1 \pmod{n + 1}$, tj. $n + 1 \mid 2^{n!} - 1$.

   Vrijedi $\varphi(n - 1) \leq n$ pa $\varphi(n - 1) \mid n!$, zatim analogno kao i za $n + 1$ zaključujemo $n - 1 \mid 2^{n!} - 1$.

   Time je tvrdnja dokazana.

2. **Zadatak** Neka je $a_n = 6^n + 8^n$. Odredite ostatak pri dijeljenju broja a_{83} sa 49.

   Rješenje: Kako je $\varphi(49) = 42$, i $\mathrm{M}(6, 49) = \mathrm{M}(8, 49) = 1$, iz Eulerovog teorema slijedi: $6^{84} \equiv 1 \pmod{49}$ i $8^{84} \equiv 1 \pmod{49}$. Nadalje računamo:

$$6^{83} + 8^{83} \equiv 6^{84} \cdot 6^{-1} + 8^{84} \cdot 8^{-1} \equiv 6^{-1} + 8^{-1} \pmod{49}$$

   Zatim izlučimo 6^{-1} i 8^{-1} i dobimo:

$$6^{-1} + 8^{-1} \equiv (6 + 8) \cdot 6^{-1}8^{-1} \equiv (14) \cdot 48^{-1} \equiv (14) \cdot (-1) \equiv 35 \pmod{49}$$

3. **Zadatak** Pokaži da $19 \mid 2^{2^{6k+2}} + 3$ za $k = 0, 1, 2, \ldots$.

   Rješenje: Iz Malog Fermatovog teorema vrijedi $2^{18} \equiv 1 \pmod{19}$. Sada promatramo koji ostatak 2^{6k+2} daje pri dijeljenju sa 18. Naime vrijedi $2^6 \equiv 64 \equiv 1 \pmod 9$ pa stoga i $2^{6k} \equiv 1 \pmod 9$. Zatim $2^{6k+2} \equiv 2^{6k} \cdot 2^2 \equiv 4 \pmod 9$, a kako su obje strane parne isto vrijedi i za ostatak pri dijeljenju sa 18, tj, $2^{6k+2} \equiv 4 \pmod{18}$. Znači možemo pisati $2^{6k+2} = 18m + 4$, $m \in \mathbb{N}_0$. Dakle sada imamo sljedeće:

$$2^{2^{6k+2}} + 3 \equiv 2^{18m+4} + 3 \equiv 2^{18m} \cdot 2^4 + 3 \equiv 1 \cdot 16 + 3 \equiv 0 \pmod{19}.$$

4. **Zadatak** Jedna od slutnji velikog matematičara Eulera je opovrgnuta 1960.-ih godina kada su 3 američka matematičara pokazala da postoji prirodan broj n koji zadovoljava jednadžbu

$$133^5 + 110^5 + 84^5 + 27^5 = n^5.$$

   Odredite koji je to n i tako i sami opovrgnite slutnju jednog od najvećih matematičara u povijesti!

   Rješenje: Uočimo da je n djeljiv s 2 jer je lijeva strana zbroj 2 neparna i 2 parna broja. Iz Malog Fermatovog teorema slijedi $n^5 \equiv n \pmod 5$. Pa dobivamo:

$$n \equiv 3 + 0 + 4 + 2 \equiv 4 \pmod 5.$$

   Zatim promatrajući jednakost modulo 3 dobivamo:

$$1^5 + (-1)^5 + 0 + 0 \equiv 1 - 1 \equiv 0 \equiv n^5 \pmod 3$$

   Sada imamo:

$$n \equiv 0 \pmod 3$$
$$n \equiv 4 \pmod 5$$
$$n \equiv 0 \pmod 2$$

   Odnosno n je djeljiv s 6 i daje ostatak 4 pri dijeljenju s 5, odakle možemo zaključiti da je:

$$n \equiv 24 \pmod{30}$$

   Poigrajmo se malo i s nejednakostima:

$$133^5 < 133^5 + 110^5 + 84^5 + 27^5 = n^5$$
$$\implies n > 133 \quad (*)$$
$$n^5 = 133^5 + 110^5 + 84^5 + 27^5 < 133^5 + 110^5 + 111^5 < 3 \cdot 133^5$$
$$\left(\frac{n}{133}\right)^5 < 3 \quad (**)$$

   Sada trebamo pronaći gornju granicu za n iz $(**)$. Pogledajmo što se dogodi kada je $n = 168$.

$$\left(\frac{168}{133}\right)^5 = (1 + \frac{5}{19})^5 =$$
$$= 1 + 5 \cdot \frac{5}{19} + 10 \cdot \frac{5^2}{19^2} + 10 \cdot \frac{5^3}{19^3} + 5 \cdot \frac{5^4}{19^4} + \frac{5^5}{19^5} > 1 + 5 \cdot \frac{5}{19} + 10 \cdot \frac{5^2}{19^2} = 1 + \frac{725}{361} > 1 + 2 = 3$$
$$\implies n < 168.$$

   Jedini broj koji daje ostatak 24 pri dijeljenju s 30 u intervalu od 133 do 168 je 144 $\implies n = 144$.

4 Najteži lanac

1. **Zadatak** Neka je $n \geq 3$ prirodan broj. Dokažite da je $n^{n^{n^n}} - n^{n^n}$ djeljivo s 1989.

   Rješenje: Imamo da je $1989 = 3^2 \cdot 13 \cdot 17$. Dokazat ćemo prvo djeljivost s $3^2 = 9$. Ako $3 \mid n$, tvrdnja slijedi odmah. Pretpostavimo da $3 \nmid n$. Treba pokazati da

   $$9 \mid n^{n^{n^n}} - n^{n^n} = n^{n^n}(n^{n^{n^n}-n^n} - 1) \iff n^{n^{n^n}-n^n} \equiv 1 \pmod 9$$

   Možemo primijeniti Eulerov teorem. Imamo da je $\varphi(9) = 6$ pa je dovoljno dokazati

   $$n^{n^n} - n^n \equiv 0 \pmod 6$$

   $$\iff n^n(n^{n^n-n} - 1) \equiv 0 \pmod 6)$$

   Očito vrijedi da $2 \mid n^{n^n} - n^n$. Dokažimo sada

   $$n^{n^n-n} \equiv 1 \pmod 3.$$

   To slijedi iz $\varphi(3) = 2$ i $2 \mid n^n - n$, $\forall n \in \mathbb{N}$. Time smo dokazali djeljivost s 9.

   Sada ćemo dokazati djeljivost izraza s 13. Ako $13 \mid n$, tvrdnja je očita. Pretpostavimo da $13 \nmid n$. Treba pokazati da je

   $$n^{n^{n^n}-n^n} \equiv 1 \pmod{13}$$

   Prema Eulerovom teoremu dovoljno je pokazati da je

   $$n^{n^n} - n^n \equiv 0 \pmod{12}$$

   Već smo pokazali djeljivost s 3 pa je dovoljno pokazati

   $$n^n(n^{n^n-n} - 1) \equiv 0 \pmod 4$$

   Ako $2 \mid n$, tvrdnja je očita. Pretpostavimo da $2 \nmid n$. Potrebno je dokazati da je

   $$n^{n^n-n} \equiv 1 \pmod 4,$$

   a to sigurno vrijedi jer je $\varphi(4) = 2$, a $2 \mid n^n - n$; $\forall n \in \mathbb{N}$. Time smo dokazali djeljivost s 13.

   Preostaje dokazati djeljivost sa 17. Ako $17 \mid n$, tvrdnja je očita. Pretpostavimo da $17 \nmid n$. Treba pokazati da je

   $$n^{n^{n^n}-n^n} \equiv 1 \pmod{17}$$

   Prema Eulerovom teoremu dovoljno je pokazati da je

   $$n^{n^n} - n^n \equiv 0 \pmod{16}.$$

   Ako $2 \mid n$, tvrdnja je očita. Pretpostavimo da $2 \nmid n$. Treba pokazati da je

   $$n^{n^n-n} \equiv 1 \pmod{16}$$

   za sve neparne n.

   Kako je $\varphi(16) = 8$, po Eulerovom teoremu dovoljno je pokazati da vrijedi

   $$n^n \equiv n \pmod 8.$$

   Kako je n neparan, vrijedi $n^2 \equiv 1 \pmod 8$. Stoga slijedi

   $$n^{n-1} \equiv 1 \pmod 8 \implies n^n \equiv n \pmod 8$$

   Time smo dokazali djeljivost sa 17, a i tvrdnju zadatka.

2. **Zadatak** Neka je a_n niz zadan sa

$$a_n = 2^n + 3^n + 6^n - 1,$$

za sve prirodne brojeve n. Odredi sve prirodne brojeve koji su relativno prosti sa svakim članom zadanog niza.

Rješenje: Ako $n = p - 2$ gdje je p neki prost broj veći od 3, dobijemo

$$a_{p-2} \equiv 2^{p-2} + 3^{p-2} + 6^{p-2} - 1 \equiv \frac{1}{2} + \frac{1}{3} + \frac{1}{6} - 1 \equiv 1 - 1 \equiv 0 \pmod{p},$$

koristeći MFT koji je tu primjenjiv jer $p > 3$ ne dijeli $2, 3, 6$.

Dakle imamo $p \mid a_{p-2}$ te uvrštavanjem imamo i $2 \mid a_1 = 10$ i $3 \mid a_2 = 48$, tj. za svaki prost broj postoji član niza (a_n) koji je djeljiv tim prostim brojem. Iz toga slijedi da je jedini broj koji je relativno prost sa svim članovima niza broj 1.