# Eulerova funkcija, Eulerov teorem

## Kongruencije

Najprije se podsjetimo pojma kongruencije: ako cijeli broj $m \neq 0$ dijeli $a - b$, onda kažemo da je $a$ kongruentan s $b$ i pišemo $a \equiv b \pmod{m}$.

Vrlo je lagano dokazati sljedeća svojstva kongruencije (pretpostavit ćemo da su svi brojevi koji se navode prirodni):

(1) ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$, onda je $a+c \equiv b+d \pmod{m}$, $a-c \equiv b-d \pmod{m}$ i $ac \equiv bd \pmod{m}$,

(2) ako je $a \equiv b \pmod{m}$ i $d|m$ onda je $a \equiv b \pmod{d}$,

(3) ako je $a \equiv b \pmod{m}$, onda je $ac \equiv bc \pmod{mc}$ za svaki $c$,

(4) $ac \equiv bc \pmod{m}$ ako i samo ako je $a \equiv b \pmod{\frac{m}{NZD(c,m)}}$

## Eulerova funkcija

Funkcija koja broju $n$ pridružuje broj $\phi(n)$ koji predstavlja broj elemenata skupa $\{1, 2, ..., n\}$ koji su relativno prosti s $n$ naziva se *Eulerova funkcija.*

Za vježbu izračunajte $\phi(25)$, $\phi(29)$, $\phi(60)$, $\phi(125)$.

Lako je odmah uočiti kako da, ako je $p$ prost, onda je $\phi(p) = p - 1$ i općenitije $\phi(p^n) = p^n - p^{n-1}$.

Nije teško doći ni do općenite formule za $\phi(n)$. Naime, ako su $p_1$, $p_2$,...$p_k$ svi različiti prosti faktori od $n$, onda, korištenjem formule uključivanja i isključivanja, zaključujemo da je

$$\phi(n) = n - n \sum_{1 \leqslant i \leqslant k} \frac{1}{p_i} + n \sum_{1 \leqslant i < j \leqslant k} \frac{1}{p_i p_j} - ... + (-1)^k \frac{n}{p_1 ... p_k}$$

tj.

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_k}\right).$$

Sada, iz $60 = 2^2 \cdot 3 \cdot 5$, zaključujemo da je $\phi(60) = 60\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right) = 60 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{4}{5} = 16$.

Zadatak - za vježbu dokažite da je $\sum_{k|n} \phi(k) = n$.

## Eulerov teorem

*Teorem (Euler).* Ako su cijeli broj $a$ i prirodni broj $n$ relativno prosti, onda vrijedi $a^{\phi(n)} \equiv 1 \pmod{n}$.

Dokaz. Neka je $r = \phi(n)$. Označimo s $k_1$,...,$k_r$ brojeve manje od $n$ i relativno proste s $n$. S obzirom da su $a$ i $n$ relativno prosti, tada su i brojevi $ak_1$,...,$ak_r$ relativno prosti s $n$. Ujedno, njihovi ostatci pri dijeljenju s $n$ su međusobno različiti. Naime, pretpostavimo li da $ak_i$ i $ak_j$ za $k_i \neq k_j$ daju isti ostatak pri dijeljenju s $n$, slijedilo bi da je $a(k_i - k_j)$ djeljivo s $n$, što nije moguće, jer je $a$ relativno prost s $n$, dok je $k_i - k_j$ manje od $n$. Zato, imamo

$ak_i \equiv a_i \pmod{n}$, za svaki $i = 1, ..., r$,

pri čemu su $a_1$, $a_2$,...,$a_r$ isti kao i brojevi $k_1$, $k_2$,...,$k_r$, ali ne nužno u istom redoslijedu.

Množenjem ovih kongruencija dobivamo $a^r \equiv 1 \pmod{n}$.

Specijalan slučaj ovog teorema za prost broj $n$, poznat je pod nazivom *"mali" Fermatov teorem*:

Ako je $p$ prost broj te ako je $a$ cijeli broj koji nije djeljiv s $p$, tada je $a^{p-1} \equiv 1 \pmod{p}$.

Primijenimo sada Eulerov (ili specijalno Fermatov) teorem za rješavanje raznih zadataka:

1. Dokažite da je, za sve prirodne brojeve $m$ i $n$, $m^{61}n - mn^{61}$ djeljivo s 2015.

   *Rješenje.* S obzirom da je $2015 = 5 \cdot 13 \cdot 31$, treba dokazati da je $m^{61}n - mn^{61}$ djeljivo s 5, 13 i 31.

   Dokažimo da je $m^{61}n - mn^{61} = mn(m^{60} - n^{60})$ djeljivo s 31.

   Ako je neki od brojeva $m$ i $n$ djeljiv s 31, onda smo gotovi, a ako nije, po malom Fermatovom teoremu slijedi da je $m^{30} \equiv 1 \pmod{31}$ i $n^{30} \equiv 1 \pmod{31}$, a onda i $m^{60} \equiv 1 \pmod{31}$ i $n^{60} \equiv 1 \pmod{31}$, pa je $m^{60} - n^{60}$ djeljivo s 31.

   Na istovjetan način dokazujemo djeljivost s 13 i 5.

2. Odredite zadnje dvije znamenke broja $3^{1000}$.

   *Rješenje.* Budući da je $\phi(25) = 20$, imamo $3^{20} \equiv 1 \pmod{25}$. A onda je i $3^{1000} \equiv 1 \pmod{25}$. Također je $3^2 \equiv 1 \pmod{4}$, a onda je i $3^{1000} \equiv 1 \pmod{4}$.

   Iz toga zaključujemo da je $3^{1000} \equiv 1 \pmod{100}$, pa su zadnje dvije znamenke broja $3^{1000}$ znamenke 01.

3. Dokažite: ako prost broj $p$ dijeli $a^p - 1$, za neki prirodni broj $a$, tada $p^2$ također dijeli $a^p - 1$.

   *Rješenje.* Ovaj zadatak, u kojem se primjenjuje mali Fermatov teorem, je zgodan za samostalnu vježbu, jer nije težak, a rješenje se može naći na webu; radi se o a) dijelu jednog zadatka s IMO Shortlista 1993.

4. Neka je $p$ prost broj oblika $3k+2$ koji dijeli $a^2 + ab + b^2$ za neke prirodne brojeve $a$ i $b$.

   Dokaži da su $a$ i $b$ djeljivi s $p$.

   *Rješenje.* Neka je $p = 3k + 2$ za neki nenegativni cijeli broj $k$.

   S obzirom da je $a^3 - b^3 = (a - b)(a^2 + ab + b^2)$, slijedi $a^3 \equiv b^3 \pmod{p}$, pa onda i $a^{3k} \equiv b^{3k} \pmod{p}$.

Pretpostavimo sada da $p$ ne dijeli $a$. Tada ne dijeli ni $b$, pa, po malom Fermatovom teoremu, imamo $a^{p-1} = a^{3k+1} \equiv 1 \pmod{p}$ i $b^{p-1} = b^{3k+1} \equiv 1 \pmod{p}$.

Iz $a^{3k} \equiv b^{3k} \pmod{p}$ i $a^{3k+1} \equiv b^{3k+1} \pmod{p}$ i $NZD(a,p) = 1$, slijedi da je $a \equiv b \pmod{p}$. Sada, iz uvjeta $a^2 + ab + b^2 \equiv 0 \pmod{p}$, slijedi $3a^2 \equiv 0 \pmod{p}$,a, s obzirom da je $p \neq 3$, slijedi $p|a$, što je kontradikcija.

5. Dokaži da, za svaki prost broj $p$, postoji $n \in \mathbf{N}$ tako da je $2^n + 3^n + 6^n - 1$ djeljivo s $p$.

   *Odgovor.* Lako je pokazati da za $p > 3$ možemo uzeti $n = p - 2$ i tvrdnja je zadovoljena (dokažite sami!). Za $p = 2$ svaki prirodni $n$ zadovoljava, a za $p = 3$ zadovoljava $n = 2$.

   Sada iskažimo jednu (dosta poznatu) tvrdnju koju je lagano dokazati pomoću malog Fermatovog teorema: za prirodan broj $n$, broj $n^2 + 1$ nema faktor oblika $4k + 3$ za prirodan $k$ (tj. nije djeljiv brojem $4k + 3$.)

   Naime, pretpostavimo li suprotno, postoji prost faktor $p = 4k + 3$ koji dijeli $n^2 + 1$. Tada je $n^{4k+2} = (n^2)^{2k+1} \equiv -1 \pmod{4k + 3}$, što je u kontradikciji s malim Fermatovim teoremom.

   Navedenu tvrdnju treba iskoristiti za rješavanje sljedeća tri zadatka (jedan ćemo riješiti, a dva ostaviti čitatelju za samostalnu vježbu).

6. Dokažite da $4mn - m - n$ nije potpuni kvadrat ni za koje prirodne brojeve $m$ i $n$.

   *Rješenje.* Pretpostavimo $4mn - m - n = k^2$, tj. $16mn - 4m - 4n = 4k^2$, odnosno $(4m - 1)(4n - 1) = 4k^2 + 1$, što nije moguće, prema gornjoj tvrdnji.

7. Dokažite da ne postoje cijeli brojevi $x$ i $y$ koji zadovoljavaju jednadžbu $x^2 = y^3 + 7$.

8. Dokažite da ne postoje cijeli brojevi $a$ i $b$ takvi da su oba broja $a + b$ i $ab - 1$ potpuni kvadrati.

   Nastavljamo sa zadatcima u kojima je potrebno primijeniti Eulerov teorem.

9. Neka je $p$ prost broj i neka je $m$ prirodan broj. Dokažite da postoji prirodni broj $n$ takav da broj $p^n$ u decimalnom prikazu ima $m$ uzastopnih znamenki 0.

   *Rješenje.* Najprije dokažimo tvrdnju za $p \neq 2, 5$.

   Za dani $m$, stavimo $n = \phi(10^{m+1})$. Tada, s obzirom da su $p$ i $10^{m+1}$ relativno prosti, iz Eulerovog teorema dobivamo

   $p^n \equiv 1 \pmod{10^{m+1}}$,

   pa $p^n$ ima $m$ uzastopnih znamenki 0.

   Sada promotrimo slučaj $p = 2$.

   Za sve prirodne brojeve $s$, brojevi 2 i $5^s$ su relativno prosti, pa je $2^{\phi(5^s)} \equiv 1 \pmod{5^s}$, a onda i

   $2^{\phi(5^s)+s} \equiv 2^s \pmod{10^s}$.

   Sada odaberimo $s$ tako da bude $5^s > 10^m$. Tada je $10^{s-m} > 2^s$, pa $2^{\phi(5^s)+s}$ ima $m$ uzastopnih znamenki 0.

   Slijedi zadatak za samostalnu vježbu:

10. Formirajmo niz koji se sastoji od tri zadnje znamenke potencije broja 2. Dokažite da se, počev od nekog člana, članovi niza ponavljaju periodički; odredite taj član i najmanji period.

    Primjedba. Zadatak se može poopćiti formiranjem niza zadnjih $m$ znamenki potencija broja 2.

11. Dokažite da iz bilo kojeg beskonačnog aritmetičkog niza, čiji su članovi prirodni brojevi, može biti izabran beskonačan geometrijski niz.

    *Rješenje.* Bez smanjenja općenitosti možemo pretpostaviti da su prvi član aritmetičkog niza $a$ i razlika $d$ relativno prosti (ako nisu, podijelimo sve članove niza s $NZD(a,d)$, odaberemo iz njega geometrijski niz i pomnožimo sve članove niza s $NZD(a,d)$).

    Po Eulerovom teoremu, za relativno proste $a$ i $d$, postoji $r \in \mathbf{N}$ $(r = \phi(d))$ tako da je $a^r - 1 = kd$ za neki $k \in \mathbf{N}$. Odatle imamo $a^{r+1} = a + kad$, pa $a^{r+1}$ pripada zadanom aritmetičkom nizu. Osim toga, s obzirom da je broj $a^{nr} - 1$, $n \in \mathbf{N}$, djeljiv s $a^r - 1$, on je djeljiv i s $d$, te je $a^{nr+1} = a + k(n)d$ za neki $k(n) \in \mathbf{N}$ i pripada zadanom aritmetičkom nizu. Dakle, brojevi $a^{nr+1}$, $n \in \mathbf{N_0}$ pripadaju zadanom aritmetičkom nizu i formiraju beskonačni geometrijski niz.

12. Dokažite da postoji beskonačan niz brojeva oblika $2^n - 3$, $n \in \mathbf{N}$, za koji vrjedi da su svaka dva među njima relativno prosta.

    *Rješenje.* Pretpostavimo da su $k_1$,...,$k_s$ prirodni brojevi takvi da su svaka dva broja oblika $2^{k_i} - 3$, $i = 1, ..., s$ međusono relativno prosta. Stavimo $n = \prod_{i=1}^{s}(2^{k_i} - 3)$. Po Eulerovom teoremu je $2^{\phi(n)} - 1$ djeljiv s $n$, pa je djeljiv i sa svakim od brojeva $2^{k_i} - 3$, $i = 1, ..., s$.

    Sada lagano slijedi da je $2^{\phi(n)} - 3$ relativno prost sa svakim od brojeva $2^{k_i} - 3$, $i = 1, ..., s$.

    Naime, neka je $q_i$ zajednički faktor brojeva $2^{\phi(n)} - 3$ i $2^{k_i} - 3$. S obzirom da je $2^{\phi(n)} - 1$ djeljiv s $2^{k_i} - 3$, slijedi da $q_i$ dijeli neparan broj $2^{\phi(n)} - 1$, kao i $(2^{\phi(n)} - 1) - (2^{\phi(n)} - 3) = 2$, pa je $q_i = 1$.

    Ostavljamo još nekoliko zadataka za samostalni rad:

13. Dokažite da za svaki prirodan broj $n \neq 2, 6$ vrijedi $\phi(n) \geqslant \sqrt{n}$.

14. Dokažite sljedeće tvrdnje:

    a) ne postoji prirodan broj $n > 1$ takav da $n | 2^n - 1$,

    b) ne postoje prirodni brojevi $n_1$, $n_2 > 1$ takvi da $n_1 | 2^{n_2} - 1$ i $n_2 | 2^{n_1} - 1$.

15. Neka je $n$ prirodan broj. Dokažite da $n^2 - 1$ dijeli $2^{n!} - 1$.

16. Neka je, za neki prirodan broj $n$, broj $3^n - 2^n$ potencija prostog broja.

    Dokažite da je $n$ prost broj.

17. Neka je $a > 1$ prirodan broj. Dokažite da skup

$$\{a^2 + a - 1, a^3 + a^2 - 1, a^4 + a^3 - 1, ...\}$$

    sadrži beskonačan podskup čija su svaka dva elementa relativno prosta.

18. Neka je $m$ prirodan broj.

    Dokaži: broj $2^{m+1}+1$ dijeli $3^{2^m}+1$ ako i samo ako je $2^{m+1}+1$ prost.

    Zainteresirani učenici mogu poslati rješenja zadataka ili upit u vezi s njima e-mail porukom na adresu: ilko.brnetic@fer.hr

    Napomena. Za pripremu predavanja koristio sam razne izvore. Za sustavno učenje osnova teorije brojeva od literature na hrvatskom jeziku svakako preporučam skripta Dujella: Uvod u teoriju brojeva (web.math.pmf.unizg.hr/ duje/utb/utblink.pdf)