PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **15** (1987/1988)
Številka 4
Strani 194–196

Dušan Pagon:

# KONGRUENCE IN EULERJEV IZREK

Ključne besede: algebra, matematika.

Elektronska verzija: http://www.presek.si/15/902-Pagon.pdf

## KONGRUENCE IN EULERJEV IZREK

Pogovarjali se bomo o lastnostih celih števil. S pojmom *kongruenca* smo se seznanili v "ogrevanju", v pričujočem sestavku pa bomo najprej na kratko orisali osnovne pojme, nato pa nanizali nekaj rezultatov.

Beseda kongruenca izvira iz latinske besede *congruens,* ki označuje ustreznost oziroma sovpadanje. Nas bodo zanimali ostanki pri deljenju celih števil z določenim naravnim številom $m$, ki ga bomo imenovali *modul* (lat. *modulus* — mera).

Za dve celi števili $a$ in $b$ bomo rekli, da sta *kongruentni po modulu m,* če pri deljenju s številom $m$ dasta enak ostanek $r$. Zapis $a \equiv b \pmod m$ torej pomeni, da je

$$a = k_1 m + r \quad \text{in} \quad b = k_2 m + r \tag{1}$$

kjer je $r$ ostanek pri deljenju z $m$ (torej $0 \leqslant r < m$).

Hitro se lahko prepričamo, da je zgornja definicija kongruence ekvivalentna naslednji.

*IZREK 1. $a \equiv b \pmod m$ takrat in samo takrat, ko je razlika števila a in b deljiva s številom m.*

*Dokaz.* Res, če med seboj odštejemo enakosti (1), dobimo $a - b = (k_1 - k_2)m$ obratno pa iz $a - b = km$ in $a = k_1 m + r$ sledi $b = (k_1 - k)\, m + r$, torej sta ostanka deljenja števil $a$ in $b$ z $m$ enaka. □

Kongruence imajo veliko podobnih lastnosti kot navadne enakosti. Oglejmo si jih nekaj.

*IZREK 2. Če je $a_1 \equiv b_1 \pmod m$ in $a_2 \equiv b_2 \pmod m$, potem je tudi $a_1 + a_2 \equiv b_1 + b_2 \pmod m$ in $a_1 a_2 \equiv b_1 b_2 \pmod m$.*

*Dokaz.* Razliki $a_1 - b_1$ in $a_2 - b_2$ sta deljivi z $m$, zato je deljiva z $m$ tudi njuna vsota, ki jo lahko zapišemo v obliki $(a_1 + a_2) - (b_1 + b_2)$, kar dokazuje prvi del izreka. Naj bo $a_1 = b_1 + k_1 m$ in $a_2 = b_2 + k_2 m$. Potem je tudi $a_1 a_2 = b_1 b_2 + {} + (b_1 k_2 + k_1 b_2 + k_1 k_2 m)\, m$, od koder sledi drugi del našega izreka. □

*IZREK 3. Relacija $a \equiv b \pmod m$ velja takrat in samo takrat, ko je $ca \equiv cb \pmod{cm}$ za poljubno naravno število c. Iz kongruence $a \equiv b \pmod m$ sledi kongruenca $a \equiv b \pmod{m_1}$, kjer je $m_1$ poljuben delitelj števila m.*

*Dokaz.* Prva trditev očitno sledi iz ekvivalentnosti naslednjih enakosti: $a - b = km$ in $ca - cb = kcm$. Za dokaz druge trditve naj bo $a - b = km$ in

$m = m_1 m_2$. Potem je tudi $a - b = (km_2)m_1$, kar smo želeli dokazati. □

*IZREK 4. Naj bo* $ca \equiv cb \pmod m$ *in največji skupni delitelj števil* $c$ *in* $m$ *(označujemo ga z* $D(c, m)$*) enak 1. Potem je tudi* $a \equiv b \pmod m$.

*Dokaz.* Vemo, da je $c(a - b) = km$ in da števili $c$ in $m$ nimata skupnih deliteljev razen števila 1. Torej mora biti $k = ck_1$, $k_1 \in \mathbb{N}$, od koder vidimo, da je $a - b = k_1 m$ oziroma $a \equiv b \pmod m$. □

Razdelimo množico vseh celih števil na paroma disjunktne podmnožice, ki jim bomo rekli *razredi števil po modulu m,* tako da v isti razred uvrstimo vsa cela števila, ki dajo pri deljenju z $m$ enak ostanek. Vsako množico iz $m$ števil, od katerih nobeni dve nista iz istega razreda po modulu $m$, bomo imenovali *kompletna množica predstavnikov po modulu m. Reducirana množica predstavnikov po modulu m* pa bomo rekli podmnožici kompletne množice, sestavljeni iz vseh tistih števil, ki so tuja številu $m$. Označimo reducirano množico, dobljeno iz kompletne množice $\{1, 2, 3, \ldots, m\}$ z $R_m$, število elementov v njej pa s $\varphi(m)$.

*Primer 1.* $R_6 = \{1, 5\}$, $\varphi(6) = 2$ in
$R_7 = \{1, 2, 3, 4, 5, 6\}$, $\varphi(7) = 6$

Na ta način smo opredelili funkcijo $\varphi: n \mapsto \varphi(n)$ za vsa naravna števila $n$. Imenujemo jo Eulerjeva funkcija. Očitno je za vsako praštevilo $p$ vrednost $\varphi(p)$ enaka $p - 1$.

Reducirane množice imajo naslednjo pomembno lastnost.

*IZREK 5. Če sta števili* $a$ *in* $m$ *tuji, potem je množica* $\{ax: x \in R_m\}$ *reducirana množica predstavnikov po modulu m.*

*Dokaz.* Iz $D(a, m) = 1$ in $D(x, m) = 1$ sledi enakost $D(ax, m) = 1$, torej se moramo prepričati le, da vsa števila $ax$, $x \in R_m$, pripadajo različnim razredom po modulu $m$. To pa dobimo s pomočjo izreka 4. Iz $ax_1 \equiv ax_2 \pmod m$ bi namreč dobili $x_1 \equiv x_2 \pmod m$, to pa nasprotuje dejstvu, da so vrednosti spremenljivke $x$ v reducirani množici $R_m$ predstavnikov po modulu $m$. □

Naslednja trditev je znana pod imenom Eulerjev izrek.

*IZREK 6. Naj bo* $m > 1$ *in* $D(a, m) = 1$. *Potem je* $a^{\varphi(m)} \equiv 1 \pmod m$.

*Dokaz.* Označimo s $c$ vrednost $\varphi(m)$ in z $r_1, r_2, \ldots, r_c$ elemente množice $R_m$. Naj bo za vsako celo število $i$ $(1 \leqslant i \leqslant c)$ $q_i$ najmanjši pozitivni predstavnik razreda, ki mu pripada število $ar_i$. Potem zaradi druge lastnosti kongruence,