ДОДАТНА НАСТАВА МАТЕМАТИКЕ ЗА УЧЕНИКЕ ОСНОВНЕ ШКОЛЕ
8. РАЗРЕД

КОНГУЕНЦИЈЕ И ПРИМЕНЕ (1)

У седмом разреду користили смо метод последње цифре, тј. систем остатака при дељењу целог броја са 10. Сада желимо да та знања проширимо посматрањем система остатак при дељењу са било којим природним бројем различитим од 1. За то нам је неопходно да дефинишемо једну нову релацију коју ћемо звати конгруенција по модулу. Конгруенција по модулу је релација која је преко остатка повезана са већ посматраном једнакошћу $a = bq + r$, дакле са релацијом дељивости, али која има много сличних особина са релацијом једнакости.

За целе бројеве a и b каже се да су конгруентни по модулу m ($m \in Z$ и $m \neq 0$), ако a и b при дељењу са m дају једнаке остатке. Симболички се то записује $a \equiv b \pmod{m}$. Ако a и b при дељењу са m имају различите остатке, онда се каже a није конгруентно b по модулу m и записује $a \not\equiv b \pmod{m}$.[1]

Тако је на пример $37 \equiv 12 \pmod{5}$, јер и 37 и 12 при дељењу са 5 имају остатак 2. Слично је и $2011 \equiv 1 \pmod{67}$, јер 2011 и 1 при дељењу са 67 дају остатак 1. Тачно је и да $56 \not\equiv 82 \pmod{3}$, јер 56 при дељењу са 3 даје остатак 2, а 82 при дељењу са 3 даје остатак 1.

Примери који следе ће најбоље илустровати основне особине релације конгруенције по модулу, али и многобојне могућности примена релације конгруенције по модулу.

ПРИМЕР 1.

Ако је $a \equiv b \pmod{m}$ онда и само онда је $a - b$ дељиво са m. Докажи.

РЕШЕЊЕ: Ако је $a \equiv b \pmod{m}$, онда на основу дате дефиниције a и b при дељењу са m имају једнаке остатке, тј. $a = км + r$ и $b = lm + r$. Тада је $a - b = км + r - (lm + r) = m(к - l)$. Дакле $a - b$ је дељиво са m.

Обрнуто, нека је $a = pm + r_1$ и $b = qm + r_2$ $(0 \leq r_1, r_2 < m)$ и нека је $a - b$ дељиво са m, тј. нека је $a - b = км$. Тада се одузимањем једнакости добија $a - b = pm + r_1 - (qm + r_2) = m(p - q) + r_1 - r_2 = км$. Како је десна страна једнакости дељива са m, то мора бити и лева па $r_1 - r_2$ дељиво са m. Тада је због обавезног услова $(0 \leq r_1, r_2 < m)$ $r_1 - r_2 = 0$. То значи да су r_1 и r_2 једнаки, па a и b при дељењу са m имају једнаке остатке, а то значи да је $a \equiv b \pmod{m}$.

ПРИМЕР 2.

Конгруенција по модулу је релација еквиваленције.[2]

---

[1] Овакав начин записивања увео је Гаус у својој књизи "Disquisitiones arithmeticae", која је објављена 1801. године, када је Гаусу било свега 24 године.

[2] За релацију се каже да је релација еквиваленцује ако је рефлексивна, симетрична и транзитивна.

Решење: Конгруенција по модулу је рефлексивна релација јер је $a - a = 0$, а 0 је увек дељива са m. Ако је $a \equiv b \pmod m$, онда $a - b = кm$. Међутим, тада је $b - a = -кm$, односно $b - a$ је дељиво са m. Значи да је и $b \equiv a \pmod m$, па је релација и симетрична. Ако је $a \equiv b \pmod m$ и $b \equiv c \pmod m$, онда на основу претходног задатка следи да је $a - b = кm$ и $b - c = lm$. Тада је $a - c = кm - lm = m(к - l)$, тј. $a - c$ је дељиво са m, што значи да је $a \equiv c \pmod m$, па је конгруенција по модулу и транзитивна релација, дакле и релација еквиваленције.

ПРИМЕР 3.

Релација конгруенције по модулу је сагласна са операцијама сабирања, одузимања, множења и степеновања (природним бројем). Докажи.

РЕШЕЊЕ: Ако је $a \equiv b \pmod m$ и $c \equiv d \pmod m$, онда је $a - b = кm$ и $c - d = lm$. Сабирањем једнакости се добија $a - b + c - d = кm + lm$ тј. $a + c - (b + d) = m(к + l)$, а то значи да је $a + c \equiv b + d \pmod m$. На сличан начин се доказује сагласност са одузимањем, множењем и степеновањем, тј. чињенице:

- Ако је $a \equiv b \pmod m$ и $c \equiv d \pmod m$, онда је $a - c \equiv b - d \pmod m$
- Ако је $a \equiv b \pmod m$ и $c \equiv d \pmod m$, онда је $a\,c \equiv b\,d \pmod m$
- Ако је $a \equiv b \pmod m$ и $n \in \mathrm{N}$, онда је $a^n \equiv b^n \pmod m$.

Без доказа наводимо и следеће особине релације конгруенције по модулу:

- Ако су x и y цели бројеви и ако је је $a \equiv b \pmod m$ и $c \equiv d \pmod m$, онда је и $ax + cy \equiv bx + dy \pmod m$ (особина линеарности)
- Ако је $a \equiv b \pmod m$, онда постоји цео број q такав да је $a = mq + b$..
- Ако је $a \equiv b \pmod m$ и $c \equiv d \pmod m$, онда је и $ac \equiv bd \pmod m$ (особина мултипликативности)
- Ако је $a \equiv b \pmod m$ и P(x) полином са целим коефицијентима, онда је $\mathrm{P}(a) \equiv \mathrm{P}(b) \pmod m$.
- Ако је $a \equiv b \pmod m$ и $d \mid m$, онда је $a \equiv b \pmod d$.

Вероватно најчешће коришћена особина конгуенције са модулом је њена сагласност са степеновањем и лакоћа са којом се ова особина релације примењује уколико је $a^n \equiv 1 \pmod m$ или $a^n \equiv -1 \pmod m$.

ПРИМЕР 4.

Колики је остатак при дељењу броја 2^{2011} са 13 ?

РЕШЕЊЕ: Како је $2^6 = 64 \equiv -1 \pmod{13}$, закључујемо да је $2^{2010} = (2^6)^{335} \equiv (-1)^{335} \equiv -1 \pmod{13}$. Даље је $2^{2011} = 2 \cdot 2^{2010} \equiv 2 \cdot (-1) = -2 \equiv 11 \pmod{13}$. Дакле, број 2^{2011} при дељењу са 13 даје остатак 11.

ЗАДАЦИ

1. Докажи да је број $10! + 1$ дељив са 11.
2. Да ли је број $2^{33} + 1$ прост или сложен?
3. Докажи да је број $3^{2007} + 1$ дељив са 13 .
4. Докажи да је $317^{259} - 8$ дељиво са 15.
5. Којом цифром се завршава број 7^{2020} ?
6. Докажи да је број $2222^{5555} + 5555^{2222}$ дељив са 3, 7 и 231.
7. Докажи да је број $3^{105} + 4^{105}$ дељив са 7 и 13, а није дељив са 11.
8. Одредити последње две цифре броја 99^{12345}.
9. Које су последње две цифре броја 2^{100}?
10. Која је последња цифра броја $(9^9)^9$, а која броја 9^{9^9} ?
11. Које су последње две цифре броја $\left(\left(7^9\right)^9\right)^9$?