KONGRUENCIJE

Za cele brojeve *a* i *b* kaže se da su kongruentni po modulu *m* ako *a* i *b* pri deljenju sa *m* daju iste ostatke. Zapisujemo:

$$a \equiv b \pmod{m} \text{ ili } a \equiv_m b$$

Na primer:

$17 \equiv 12 \pmod{5}$ jer pri deljenju sa 5 i 17 i 12 daju ostatak 2

$18 \not\equiv 12 \pmod{5}$ jer pri deljenju sa 5, 18 daje ostatak 3 a 12 daje ostatak 2

Neki profesori vole kongruencije da opišu ovako:

$$a \equiv b \pmod{m} \Leftrightarrow a - b \text{ je deljivo sa m (može i zapis } m / a - b)$$

Za naš primer bi bilo :

$17 \equiv 12 \pmod{5} \Leftrightarrow 5 / 17 - 12 = 5$

Navešćemo (bez dokaza) nekoliko osobina koje će nam pomoći u izradi zadataka:

1. $a \equiv_m a$
2. $a \equiv_m b \Rightarrow b \equiv_m a$
3. $a \equiv_m b \wedge b \equiv_m c \Rightarrow a \equiv_m c$
4. $a \equiv_m b \wedge c \equiv_m d \Rightarrow a + c \equiv_m b + d$
5. $a \equiv_m b \wedge c \equiv_m d \Rightarrow ac \equiv_m bd$
6. $a \equiv_m b \Rightarrow a^n \equiv_m b^n \quad (n \in N)$
7. Ako je $a \equiv_m b$ i d deli $m \Rightarrow a \equiv_d b$

Može nam koristiti i mala Fermaova teorema:

Ako je p prost broj i p ne deli a , onda je

$$a^{p-1} \equiv_p 1$$

Dalje ćemo uraditi nekoliko primera....

Primer 1.

Nađi ostatak pri deljenju

a) 2^{100} sa 7
b) 317^{259} sa 15

Rešenje:

a) Česta ideja je da koristimo pravila za stepenovanje $a^m \cdot a^n = a^{m+n}$ i $(a^m)^n = a^{mn}$

$$2^3 = 8 \equiv_7 1$$

$$2^{100} = 2^{99} \cdot 2 = \left(2^3\right)^{33} \cdot 2 \equiv_7 1^{33} \cdot 2 \equiv_7 2$$

b) Kad podelimo 317 sa 15 dobijamo 21 i ostatak 2, pa zaključujemo

$$317^{259} \equiv_{15} 2^{259}$$

Kako je $16 = 2^4 \equiv_{15} 1$ to nam daje ideju da 259 zapišemo kao $256 + 3$

$$2^{259} \equiv_{15} 2^{256+3} \equiv_{15} 2^{256} \cdot 2^3 \equiv_{15} \left(2^4\right)^{64} \cdot 2^3 \equiv_{15} 1 \cdot 2^3 \equiv_{15} 8$$

Primer 2.

Kojom cifrom se završava broj 7^{2024} ?

Rešenje:

Poslednja cifra nekog broja je ostatak pri deljenju sa 10.

Znači treba da ispitamo čemu je ovaj broj kongruentan po modulu 10.

$$49 = 7^2 \equiv_{10} 9 \equiv_{10} -1$$

$$7^{2024} = \left(7^2\right)^{1024} \equiv_{10} (-1)^{1024} = 1$$

Broj 7^{2024} se završava sa 1.

Primer 3.

Dokazati da je broj $2222^{5555} + 5555^{2222}$ deljiv sa 7.

Rešenje:

Radimo za svaki sabirak posebno , pa saberemo te dve kongruencije.(Osobina 4.)

2222:7 = 317 i ostatak 3

$2222^{5555} \equiv_7 3^{5555}$

Kako je $3^5 = 243,$ a 243:7=34 i ostatak 5 imamo $3^{5555} \equiv_7 \left(3^5\right)^{1111} \equiv_7 5^{1111}$

Kako je $5 \equiv_7 -2$ to je $5^{1111} \equiv_7 (-2)^{1111}$

Kako je $8=2^3 \equiv_7 1$ radimo $(-2)^{1111} = -2 \cdot 2^{1110} = -2 \cdot \left(2^3\right)^{370} \equiv_7 -2 \cdot 1 = -2$

5555 : 7 = 793 i ostatak 4

$5555^{2222} \equiv_7 4^{2222} = \left(2^2\right)^{2222} = 2^{4444}$

Kako je $8=2^3 \equiv_7 1$ radimo $2^{4444} = 2^{4443+1} = 2^{4443} \cdot 2^1 = \left(2^3\right)^{1481} \cdot 2 \equiv_7 1 \cdot 2 = 2$

$$2222^{5555} + 5555^{2222} \equiv_7 -2 + 2 = 0$$

Primer 4.

Dokazati da je broj $5^{5n+1} + 4^{5n+2} + 3^{5n}$ deljiv sa 11.

Rešenje:

Do sada smo ovakve primere rešavali matematičkom indukcijom, sad možemo i preko kongruencija.

Svaki sabirak radimo posebno , pa to saberemo. Osobina 4. nam to dozvoljava.

$5^{5n+1} = 5^{5n} \cdot 5^1 = \left(5^5\right)^n \cdot 5 = 3125^n \cdot 5$

Kako je 3125 : 11 =284 i ostatak 1 to je $3125^n \equiv_{11} 1$ pa je $3125^n \cdot 5 \equiv_{11} 5$

$4^{5n+2} = 4^{5n} \cdot 4^2 = \left(4^5\right)^n \cdot 4^2 = 1024^n \cdot 16$

Kako je 1024 : 11 =93 i ostatak 1 to je$1024^n \equiv_{11} 1$ pa je $1024^n \cdot 16 \equiv_{11} 16$

$3^{5n} = \left(3^5\right)^n = 243^n$

$243 : 11 = 22$ i ostatak $1 \Rightarrow 243^n \equiv_{11} 1$

Sad sve zajedno:

$5^{5n+1} + 4^{5n+2} + 3^{5n} \equiv_{11} 5 + 16 + 1 = 22 \equiv_{11} 0$

Znači da je broj deljiv sa 11.

Primer 5.

Odrediti ostatak pri deljenju broja 2^{p^2} sa 13, ako je p prost broj i p > 3.

Rešenje:

U prethodnom fajlu o prostim brojevima smo videli primer da sve proste brojeve veće od 3 možemo opisati sa 6k+1 i 6k+5 .

Taj zaključak ćemo upotrebiti u ovom primeru.

Razmišljamo šta se dešava sa p^2 ?

$$(6k+1)^2 = 36k^2+12k+1 = 12(3k^2+k)+1$$
$$(6k+5)^2 = 36k^2+60k+25 = 36k^2+60k+24+1 = 12(3k^2+5k+2)+1$$

Ovo nam govori da je

$$p^2 \equiv_{12} 1$$

Neka je onda $p^2 = 12k+1$

$$2^{12k+1} \equiv_{13} ?$$
$$2^{12k+1} = 2^{12k}\cdot 2 = \left(2^{12}\right)^k \cdot 2$$
$$2^{12} = \left(2^6\right)^2 = 64^2 \text{ a kako je } 64 \equiv_{13} -1 \text{ (jer 13*5=65) imamo } 2^{12} \equiv_{13} (-1)^2 = 1$$
$$2^{12k+1} \equiv_{13} 1^k \cdot 2 = 2$$

Ostatak je 2.