Kongruence

Kongruence je uvedel eden največjih matematikov *Carl Friedrich Gauss* koncem 18.st.

Za kaj gre? Gre za to, da se z relacijo deljivosti v množici celih števil deljenci velikokrat obnašajo podobno kot ostanki teh števil pri deljenju z deliteljem.

Ker je množica ostankov omejena množica, se problemi z deljivostjo na ta način poenostavijo. Namesto da bi računali z deljenci, računamo z ostanki...

Opazimo lahko, da imajo cela števila pri deljenju z naravnim številom m končno mnogo ostankov: ti so lahko $0, 1, \ldots, m-1$.

Tako pri deljenju s 5 dobimo ostanke iz množice {0,1,2,3,4}:

$-1 = (-1)\cdot 5 + \mathbf{4}$	$0 = 0\cdot 5 + \mathbf{0}$	$6 = 1\cdot 5 + \mathbf{1}$
$-2 = (-1)\cdot 5 + \mathbf{3}$	$1 = 0\cdot 5 + \mathbf{1}$	$7 = 1\cdot 5 + \mathbf{2}$
$-3 = (-1)\cdot 5 + \mathbf{2}$	$2 = 0\cdot 5 + \mathbf{2}$	$8 = 1\cdot 5 + \mathbf{3}$
$-4 = (-1)\cdot 5 + \mathbf{1}$	$3 = 0\cdot 5 + \mathbf{3}$	$9 = 1\cdot 5 + \mathbf{4}$
$-5 = (-1)\cdot 5 + \mathbf{0}$	$4 = 0\cdot 5 + \mathbf{4}$	$10 = 2\cdot 5 + \mathbf{0}$
$-6 = (-2)\cdot 5 + \mathbf{4}$	$5 = 1\cdot 5 + \mathbf{0}$	$11 = 2\cdot 5 + \mathbf{1}$
$\ldots$	$\ldots$	$\ldots$

Opazimo lahko, da imata naprimer števili 11 in 6 nekaj skupnega - to je ostanek 1 pri deljenju s 5. Pravimo,da je 11 *kongruentno* 6 *po modulu* 5.

Zapišimo še formalno definicijo.

Definicija 1 *Naj bo $m \in \mathbb{N}$, in $a, b \in \mathbb{Z}$. Pravimo, da je a kongruenten b po modulu m ter to zapišemo*

$$a \equiv b (\mathrm{mod}\ m),$$

če imata števili a in b enak ostanek pri deljenju z m.

Primeri: $55 \equiv 61 \pmod 3$, $6 \equiv -4 \pmod 5$, $123123 \equiv 0 \pmod{11}$.

Razlika števil, ki sta konruentni po nekem modulu, je deljiva z modulom. Tako velja

$$3|55-61, \quad 5|6-(-4), \quad 11|123123-0.$$

Na teh nekaj zgledih oblikujemo trditev 1.

Trditev 1 *$a \equiv b\ (\mathrm{mod}\ m)$ natanko tedaj, ko velja $m|(a-b)$.*

Dokaz: Naj bosta $a = k_1m + r_1$ in $b = k_2m + r_2$, kjer je $0 \leq r_1, r_2 < m$. Sledi

$$a - b = (k_1m + r_1) - (k_2m + r_2) = m(k_1 - k_2) + (r_1 - r_2).$$

Sledi, da m deli $a-b$ natanko tedaj, ko $m|(r_1-r_2)$. Opazimo, da je $m > r_1-r_2$. Potem je edina možnost, da $m|(r_1 - r_2)$ ta, da je $r_1 - r_2 = 0$ oziroma $r_1 = r_2$. □

Posledica 1 *$a \equiv 0 \pmod{m}$ natanko tedaj, ko velja $m|a$.*

Trditev 2 *Relacija $\equiv$ je ekvivalenčna relacija.*

- *refleksivnost:* za vsako celo število a velja $a \equiv a \pmod{m}$.
- *simetričnost:* če je $a \equiv b \pmod{m}$, je $b \equiv a \pmod{m}$ za poljubni celi števili a in b.
- *tranzitivnost:* če velja $a \equiv b \pmod{m}$ ter $b \equiv c \pmod{m}$, sledi $a \equiv c \pmod{m}$ za poljubni celi števili a, b, c.

Dokaz: Prepuščeno dijaku.

Kongruence imajo podobne lastnosti kot enačbe. Navedimo le nakatere.

Trditev 3 *Naj bo $a \equiv b \pmod{m}$. Potem za vsako celo število $c \in \mathbb{Z}$ velja*

$$a + c \equiv b + c \pmod{m}.$$

Dokaz: Ker $a \equiv b \pmod{m}$ sledi, da m deli

$$a - b = (a + c) - (b + c).$$

Torej je $a + c \equiv b + c \pmod{m}$. □

Trditev 4 *Naj bo $a \equiv b \pmod{m}$. Potem za vsako celo število $c \in \mathbb{Z}$ velja*

$$a \cdot c \equiv b \cdot c \pmod{m}.$$

Dokaz: Podobno kot dokaz trditve 3. Prepuščeno dijaku. □

Trditev 5 *Naj bo $a \equiv b \pmod{m}$ in $c \equiv d \pmod{m}$. Potem velja*

1. $a + c \equiv b + d \pmod{m}$,
2. $a \cdot c \equiv b \cdot d \pmod{m}$.

Dokaz:

(1) Ker je $a \equiv b$ (mod m), prištejemo c levi in desni strani. Po trditvi 3 je

$$a + c \equiv b + c \text{ (mod m)}.$$

Ker je $c \equiv d$ (mod m), prištejemo b levi in desni strani. Po trditvi 3 je

$$b + d \equiv c + b \pmod{m}.$$

Zaradi trditve 2 (tranzitivnost) sledi $a + c \equiv b + d \pmod{m}$. □

(2) Dokaz je podoben (1). Podrobnosti so prepuščene bralcu. □

Trditev 6 *Če je $a \equiv b \pmod{m}$, potem sledi $a^k \equiv b^k \pmod{m}$ za neki $k \in \mathbb{N}$.*

Dokaz: Večkratna uporaba trditve 5, točka (2). Podrobnosti prepuščene dijaku. □

Primer: Kakšen ostanek ima število 3^{100} pri deljenju z 8?

Ker je $3^2 \equiv 1 \pmod{8}$, je $3^{100} \equiv 1^{50} \equiv 1 \pmod{8}$, kar pomeni, da ima število 3^{100} ostanek 1 pri deljenju z 8.

Primer: Vsak delitelj $a - b$ je delitelj $a^k - b^k$, kjer je $k \in \mathbb{N}$.

Pokažimo, da to res velja: Naj bo m delitelj razlike $a - b$ oz. $a \equiv b \pmod{m}$. Po zadnji trditvi sledi $a^k \equiv b^k \pmod{m}$, kar pomeni, da je $a^k \equiv b^k \pmod{m}$. Razlika $a^k - b^k$ je kongruentna z 0, torej je m delitelj $a^k - b^k$.

Trditev 7 *Naj bo $d \in \mathbb{N}$, $a \equiv b \pmod{m}$ natanko tedaj, ko je*

$$ad \equiv bd \pmod{md}.$$

Dokaz: Po predpostavki $m|(a-b)$. Velja: m je večkratnik $a-b$ natanko tedaj, ko je md večkratnik $d(a - b) = da - db$. Torej je $da - db$ deljivo z md oziroma

$$ad \equiv bd \pmod{md}.$$

□

Trditev 8 *Naj bo celo število $c \in \mathbb{Z}$ in naj velja $a + c \equiv b + c \pmod{m}$. Potem je $a \equiv b \pmod{m}$.*

Dokaz: Odšteti c pomeni prišteti $-c$. Uporabimo to in še trditev 3. Podrobnosti prepuščene dijaku. □

$\rightsquigarrow$ Kongruence se torej v marsičem obnašajo kot enačbe:

- Levi in desni strani lahko *prištejemo* ali *odštejemo* neko celo število.
- Levo in desno stran lahko *pomnožimo* z nekim celim številom.
- Težave pa nastanejo, če želimo desno in levo stran *deliti* z nekim celim številom.

  Primer: Naj bo $4 \equiv 2 \pmod{2}$, toda $2 \equiv 1 \pmod{2}$ ne velja.

Lahko pa dokažemo podobno trditev.

Trditev 9 *Naj bosta a in m tuji si števili. Potem obstaja celo število $k \in \mathbb{Z}$, da velja*

$$ak \equiv 1 \pmod{m}.$$

Dokaz: Za dve tuji si števili a in m obstajata celi števili e in k, da velja

$$ak + em = 1.$$

Splošneje zadnjo vrstico zapišemo tudi takole:

> Za poljubni celi števili a in m obstajata celi števili e in k, da velja
>
> $$ak + em = d,$$
>
> kjer je $d = D(a, m)$.

Odtod sledi $ak \equiv 1 \pmod{m}$.

S pomočjo zadnje trditve lahko zapišemo:

Trditev 10 *Naj bo $ab \equiv ac \pmod{m}$ ter naj bo $D(a, m) = 1$. Potem velja*

$$b \equiv c \pmod{m}.$$

Oziroma: kongruenco lahko delimo s skupnim faktorjem, če je le-ta tuj z modulom.

Dokaz: Po trditvi 4 lahko obe strani kongruence

$$ab \equiv ac \pmod{m}$$

pomnožimo s k. Sledi $(ka)b \equiv (ka)c \pmod{m}$. Ker je $ka \equiv 1$ (mod m), velja $(ka)b \equiv b \pmod{m}$, $(ka)c \equiv c \pmod{m}$. Sledi

$$b \equiv c \pmod{m},$$

kar smo želeli pokazati. □

Trditev 11 *Naj bo $D(a, m) = 1$. Potem obstaja natanko eno število k, $0 < k < m$, za katerega velja*

$$ak \equiv 1(\text{mod m}).$$

Dokaz: Recimo, da obstajata dve števili k_1 in k_2, $0 < k_1, k_2 < m$, za kateri velja

$$ak_1 \equiv 1(\text{mod m}) \text{ in } ak_2 \equiv 1(\text{mod m}).$$

Sledi, da je

$$ak_1 \equiv ak_2(\text{mod m}).$$

Ker je $D(a, m) = 1$, lahko delimo z a:

$$d_1 \equiv k_2(\text{mod m}).$$

Sledi $m|(k_1 - k_2)$. Ker velja $0 < k_1, k_2 < m$, je $|k_1 - k_2| < m$. Torej je $k_1 - k_2 = 0$ oziroma $k_1 = k_2$. □

Trditev 12 *Naj bo $a \equiv b$ (mod m) in naj bo d naravno število, $d|m$. Tedaj velja*

$$a \equiv b \pmod{d}.$$

Dokaz: Če je $a \equiv b \pmod{m}$, velja $m|a - b$. Ker je d delitelj m, sledi $d|a - b$. □

Trditev 13 *Naj bo $v(m_1, m_2, \ldots, m_n)$ najmanjši skupni večkratnik naravnih števil $m_1, m_2, \ldots, m_n$.*

$$\begin{aligned} x &\equiv y \pmod{m_1} \\ x &\equiv y \pmod{m_2} \\ &\vdots \\ x &\equiv y \pmod{m_n} \end{aligned}$$

velja natanko tedaj, ko

$$x \equiv y \pmod{v(m_1, m_2, \ldots, m_n)}.$$

Dokaz: Predpostavimo, da velja $x \equiv y \pmod{m_i}$ za $i = 1, 2, \ldots, n$. Odtod sledi, da je $x - y$ večkratnik števil $m_1, m_2, \ldots, m_n$, zato je

$$v(m_1, m_2, \ldots, m_n) | (x - y)$$

oziroma $x \equiv y(\mod v(m_1, m_2, \ldots, m_n)$.

Obratno: če je $x \equiv y \pmod{v(m_1, m_2, \ldots, m_n)}$, potem po trditvi 12 velja

$$x \equiv y \pmod{m_i},$$

saj $m_i | v(m_1, m_2, \ldots, m_n)$. □

Primer: Zapiši kongruenco, ki je ekvivalentna paru kongruenc $x \equiv 1 \pmod 4$ in $x \equiv 2 \pmod 3$.

Prvo in drugo kongruenco pomnožimo tako, da dobimo skupno skupni modul (po trditvi 7):

$$\begin{aligned} 3x &\equiv 3 \pmod{12} \quad \text{(prva pomnožena s 3)} \\ 4x &\equiv 8 \pmod{12} \quad \text{(prva pomnožena s 4, nakar seštejemo...)} \\ 7x &\equiv 11 \pmod{12} / \cdot 5 \text{ (po trditvi 13 je ta kongruenca ekvivalentna izhodiščnima)} \\ 35x &\equiv 55 \pmod{12} \\ -x &\equiv 7 \pmod{12} \\ x &\equiv 5 \pmod{12} \end{aligned}$$

Za konec pa zastavimo problem, ki pravi:

> Če bonbone razdelimo med 4 prijatelje, nam ostanejo 3 bonboni, če jih razdelimo med 5 prijateljev, nam ostaneta 2, če pa jih razdelimo med 7 prijateljev, nam jih ostane 6. Koliko bonbonov lahko imamo?

Hitro ugotovimo, da velja več kongruenc

$$x \equiv 3 \pmod 4$$
$$x \equiv 2 \pmod 5$$
$$x \equiv 6 \pmod 7$$

Določiti je potrebno x, ki ustreza vsem kongruencam hkrati. Ker je desna stran kongruenc različna, situacija ne ustreza trditvi 13.

Velja naslednji splošnejši izrek:

Trditev 14 (Kitajski izrek o ostankih, Sun Tsu, 350 n.št.) *Sistem kongruenc*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

kjer so $m_1, m_2, \ldots, m_n$ naravna paroma tuja si števila, ima neskončno rešitev in ta se razlikujejo za večkratnik $m = m_1 \cdot m_2 \cdots m_n$.

Dokaz: izpustimo. Poglejmo raje recept, kako tak sistem kongruenc rešiti.

1. izračunamo $m = m_1 \cdot m_2 \cdots m_n$
2. določimo $M_1 = \frac{m}{m_1}, M_2 = \frac{m}{m_2}, M_3 = \frac{m}{m_3}, \ldots, M_n = \frac{m}{m_n}$
3. poiščemo $x_1, x_2, \ldots x_n$ kot rešitve kongruenc

$$\begin{aligned} M_1 x_1 &\equiv 1 \pmod{m_1} \\ M_2 x_2 &\equiv 1 \pmod{m_2} \\ &\vdots \\ M_n x_n &\equiv 1 \pmod{m_n} \end{aligned}$$

4. izračunamo $e_1, e_2, \ldots, e_n$:

$$e_1 = x_1 m_1, e_2 = x_2 m_2, \ldots e_n = x_n m_n$$

5. splošna rešitev x je oblike

$$x \equiv e_1 a_1 + e_2 a_2 + \ldots + e_n a_n \pmod{m}$$

Reši zdaj nalogo o bonbonih, rešitev je $x \equiv 27 \pmod{140}$.

Naloge.

1. Dokaži *trditev 2.*
2. Dokaži *trditev 4.*
3. Dokaži *trditev 5, točka* 2.
4. Dokaži *trditev 6.*
5. Dokaži *trditev 8.*
6. Zapiši vsa naravna števila n, manjša od 100, za katera velja
$$n \equiv 7 \pmod{17}.$$
7. Če je število n sodo, ustreza kongruenci $x \equiv 0 \pmod 2$. Razmisli:
   (a) Kateri kongruenci ustrezajo liha števila?
   (b) Kateri kongruenci ustrezajo števila oblike $6k + 1$?
8. Pokaži veljavnost trditve: Naj bodo $a, b, m, k \in \mathbb{Z}$ in $a + mk \equiv b \pmod m$. Potem velja $a \equiv b \pmod m$.
9. Naj bo n naravno število, ki ni deljivo s 3. Pokaži, da dobimo ostanek 1, če delimo n^2 s 3.
10. Zapiši kongruenco, ki je ekvivalentna kongruenci $15x \equiv 15y \pmod 3$.
11. Zapiši kongruenco, ki je ekvivalentna paru kongruenc $x \equiv 2 \pmod 9$ in $x \equiv 4 \pmod{10}$.
12. Zapiši kongruenco, ki je ekvivalentna paru kongruenc $5x \equiv 14 \pmod{17}$ in $3x \equiv 2 \pmod{13}$.
13. S kongruencami pokaži, da imajo kvadrati naravnih števil na zadnjem mestu števke $0, 1, 4, 5, 6$ ali 9.
14. Pokaži, da imajo četrte potence naravnih števil na zadnjem mestu števke $0, 1, 5$ ali 6.

15. Dokaži, da za

$$x^2 = 12345678909876543212345678901 2$$

x ni celo število.

16. Pokaži, da število oblike $3^n + 2 \cdot 7^n$ ni kvadrat nobenega naravnega števila.

Rešitev: Naredimo si tabelo za nekaj možnosti:

$n \pmod{10}$	$3^n \pmod{10}$	$2 \cdot 7^n \pmod{10}$	$3^n + 2 \cdot 7^n \pmod{10}$
0	1	$2 \cdot 1 \equiv 2$	3
1	3	$2 \cdot 7 \equiv 4$	7
2	9	$2 \cdot 9 \equiv 8$	7
3	7	$2 \cdot 3 \equiv 6$	3
4	1	$2 \cdot 1 \equiv 2$	3
5	3	$2 \cdot 7 \equiv 4$	7
6	9	$2 \cdot 9 \equiv 8$	7
7	7	$2 \cdot 3 \equiv 6$	3
8	1	$2 \cdot 1 \equiv 2$	3
9	3	$2 \cdot 7 \equiv 4$	7

Na podlagi nekaj primerov vidimo, da so števke vrednosti izraza na mestu enic le 3 ali 7, kar pomeni, da to ni kvadrat. Dokažimo to še splošno. Opazimo, da je

- $3^4 \equiv 1 \pmod{10}$ in $7^4 \equiv 1 \pmod{10}$, kar pomeni, da je $3^{4k} \equiv 1 \pmod{10}$ in $7^{4k} \equiv 1 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k} + 2 \cdot 7^{4k} \equiv 3 \pmod{10}.$$

- $3^{4k} \cdot 3 = 3^{4k+1} \equiv 3 \pmod{10}$ in $7^{4k} \cdot 7 = 7^{4k+1} \equiv 7 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k+1} + 2 \cdot 7^{4k+1} \equiv 17 \equiv 7 \pmod{10}.$$

- $3^{4k+1} \cdot 3 = 3^{4k+2} \equiv 9 \pmod{10}$ in $7^{4k+1} \cdot 7 = 7^{4k+2} \equiv 9 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k+2} + 2 \cdot 7^{4k+2} \equiv 27 \equiv 7 \pmod{10}.$$

- $3^{4k+2} \cdot 3 = 3^{4k+3} \equiv 7 \pmod{10}$ in $7^{4k+2} \cdot 7 = 7^{4k+3} \equiv 3 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k+3} + 2 \cdot 7^{4k+3} \equiv 13 \equiv 3 \pmod{10}.$$

  Dokazali smo, da je izraz za vsak n kongruenten bodisi 3 bodisi 7 po modulu 10, kar pa pomeni, da ne more biti kvadrat nobenega števila (glaj nalogo 13).

17. Poišči zadnjo števko v številu 3^{400}.

18. Poišči zadnjo števko v številu 2^{400}.

19. Poišči zadnji dve števki v številu 3^{400}.

20. Deli 7777^{8888} s 5. Kolikšen je ostanek?

21. Poišči vse take n, da bo izraz $81n + 53$ deljiv s 5.

22. Pokaži, da je izraz $10^{n+1} + 4 \cdot 10^n + 4$ deljiv z 9 za vsak naravni n.

23. Pokaži, da je izraz $5^{99} + 11^{99} + 17^{99}$ deljiv s 33 za vsak naravni n.

24. Pokaži, da je izraz $29^n + 16^{n+1} + 42^{n+2}$ deljiv s 13 za vsak naravni n.

25. Poišči vsa cela števila a, da velja

$$5|(3(n^2 + n) + 7).$$

26. Določi naravne vrednosti x, da bo $13|x^2 + 1$.

27. Pokaži, da izraz $\frac{m^3}{3} + \frac{m^2}{2} + \frac{m}{6}$ predstavlja celo število za vsako celo število m.

  Rešitev: Da bo število celo mora biti števec v ulomku $\frac{2m^3 + 3m^2 + m}{6}$ deljiv s 6.

  Pokazati moramo, da velja $2m^3 + 3m^2 + m \equiv 0 \pmod{6}$. Po trditvi 13 je kongruenca ekvivalentna

$$2m^3 + 3m^2 + m = m(2m + 1)(m + 1) \equiv 0 \pmod{2}$$

  in

$$2m^3 + 3m^2 + m = m(2m + 1)(m + 1) \equiv 0 \pmod{3}$$

  kar moramo tudi pokazati.

- Prva kongruenca je očitna, saj v primeru, da je m sod, trivialno velja, če je pa lih, pa je $2m+1$ sod, zato je produkt členov v obeh primerih sodo število.
- Če je v drugi kongruenci $m \equiv 0 \pmod 3$, je tudi produkt $\equiv 0 \pmod 3$.
  Če je $m \equiv 1 \pmod 3$, je faktor $2m+1 \equiv 0 \pmod 3$, zato je produkt $\equiv 0 \pmod 3$.
  Če je $m \equiv 2 \pmod 3$, je faktor $m+1 \equiv 0 \pmod 3$, zato je produkt $\equiv 0 \pmod 3$.
  Odtod sklepamo, da velja $2m^3+3m^2+m \equiv 0 \pmod 6$.

28. Pokaži, da je izraz $\frac{n^5}{5}+\frac{n^3}{3}+\frac{7n}{15}$ celo število za vsako celo število n.
29. Pokaži,da velja $3|n^3-n$ za vsak naravni n.
30. Pokaži,da velja $5|n^5-n$ za vsak naravni n.
31. Pokaži,da velja $7|n^7-n$ za vsak naravni n.
32. Katere najmanjše naravno število ima pri deljenju s 3 ostanek 2, pri deljenju s 5 ostanek 3, pri deljenju s 7 pa ostanek 2?

Odgovore na vprašanja in rešitve na zahtevo pošljem po *e*-pošti.

Rešitve nalog.

1. Dokaz *trditve 2:*

   - refleksivnost: za vsak a velja $m|(a-a)$, torej je $a \equiv a \pmod{m}$.
   - simetričnost: če je $a \equiv b \pmod{m}$, velja $m|(a-b)$ oziroma $m|(b-a)$. Torej je $b \equiv a \pmod{m}$.
   - tranzitivnost: Velja $a \equiv b \pmod{m}$ in $b \equiv c \pmod{m}$. Torej $m|(b-a)$ in $m|(c-b)$. Sledi $m|(c-b)+(b-a) = c-a$.

2. Dokaz *trditve 4:* Ker $a \equiv b \pmod{m}$ sledi, da m deli $a-b$. Deli tudi večkratnik te razlike $m|c(a-b) = ca - cb$. Torej je $a \cdot c \equiv b \cdot c \pmod{m}$.

3. Dokaz *trditve 5:* Ker je $a \equiv b \pmod{m}$, prištejemo c levi in desni strani. Po trditvi 4 je

   $$a \cdot c \equiv b \cdot c \pmod{m}.$$

   Ker je $c \equiv d \pmod{\text{m}}$, pomnožimo z b levo in desno stran. Po trditvi 4 je

   $$b \cdot d \equiv c \cdot b \pmod{m}.$$

   Zaradi trditve 2 (tranzitivnost) sledi $a \cdot c \equiv b \cdot d \pmod{m}$.

4. Dokaz *trditve 6 :* Velja $a \equiv b \pmod{m}$. Po trditvi 5 je $a \cdot a \equiv b \cdot b \pmod{m}$. To ponovimo še $k-2$ krat in pridemo do $a^k \equiv b^k \pmod{m}$.

5. Dokaz *trditve 8 :* Ker $a \equiv b \pmod{m}$ sledi, da m deli $a-b = (a-c)-(b-c)$. Torej je $a - c \equiv b - c \pmod{m}$.

6. $M = \{n \in \mathbb{N}, n < 100; n = 17k + 7\} = \{7, 21, 41, 58, 75, 92\}$.

7. (a) Liha števila so oblike $x \equiv 1 \pmod{2}$

   (b) $x \equiv 1 \pmod{6}$

8. Ločimo dva primera:

   - $x \equiv 1 \pmod{3}$. Tedaj je $x^2 \equiv 1^2 \equiv 1 \pmod{3}$.
   - $x \equiv 2 \pmod{3}$. Tedaj je $x^2 \equiv 2^2 = 4 \equiv 1 \pmod{3}$. V obeh primerih ima kvadrat ostanek 1 pri deljenju s 3.

9. Po trditvi 1 velja: $m|(a+mk-b)$, kar pomeni, da $m|a-b$ oziroma $a \equiv b \pmod{m}$.

10. Po trditvi 7 lahko modul in obe strani delimo s skupnim faktorjem. Dobimo kongruenco $3x \equiv 3y \pmod{2}$. Ker je faktor 3 tuj z modulom, lahko obe strani delimo s 3, dobimo $x \equiv y \pmod{2}$.

11. Uporabimo trditvi 7 in 4.

$$\begin{aligned} 10x &\equiv 20 \pmod{90} \quad \text{(prva pomnožena z 10)} \\ 9x &\equiv -36 \pmod{90} \quad \text{(prva pomnožena z 9)} \\ x &\equiv -16 \pmod{90} \quad /\text{odštejemo...} \\ x &\equiv 74 \pmod{90} \end{aligned}$$

12. Spravimo obe kongruenci v standardno obliko:

$$\begin{aligned} 5x &\equiv 14 \pmod{17} \quad /\cdot 7 \\ 35x &\equiv 98 \pmod{17} \\ x &\equiv 13 \pmod{17} \qquad (1) \end{aligned} \qquad \begin{aligned} 3x &\equiv 2 \pmod{13} \quad /\cdot 9 \\ 27x &\equiv 18 \pmod{13} \\ x &\equiv 5 \pmod{13} \qquad (2) \end{aligned}$$

$$\begin{aligned} & 13x \equiv 169 \pmod{221} \quad \text{((1), pomnožena s 13)} \\ & 17x \equiv 85 \pmod{221} \quad \text{((2), pomnožena s 17)} \\ \text{Odštejemo:} \quad & 4x \equiv -84 \pmod{221} \quad \text{(trditev 4)} \\ & x \equiv -21 \pmod{221} \\ & x \equiv 200 \pmod{221} \end{aligned}$$

13. Naj bo a števka na mestu enic. Določimo vsa možne rešitve kongruence $n^2 \equiv a \pmod{10}$. Glej drugi stolpec tabele.

14. Če kvadriramo kvadrate, je na mestu enic b, ki zadošča $n^4 \equiv b \pmod{10}$. Glej tretji stolpec tabele.

$n \pmod{10}$	$a \equiv n^2 \pmod{10}$	$b \equiv n^4 \pmod{10}$
0	0	0
1	1	1
2	4	6
3	9	1
4	6	6
5	5	5
6	6	6
7	9	1
8	4	6
9	1	1

15. Kvadrat celega števila ima na mestu enic le $1, 4, 5, 6$ ali 9, zato x ni celo število.

16. Naredimo si tabelo za nekaj možnosti:

$n \pmod{10}$	$3^n \pmod{10}$	$2 \cdot 7^n \pmod{10}$	$3^n + 2 \cdot 7^n \pmod{10}$
0	1	$2 \cdot 1 \equiv 2$	3
1	3	$2 \cdot 7 \equiv 4$	7
2	9	$2 \cdot 9 \equiv 8$	7
3	7	$2 \cdot 3 \equiv 6$	3
4	1	$2 \cdot 1 \equiv 2$	3
5	3	$2 \cdot 7 \equiv 4$	7
6	9	$2 \cdot 9 \equiv 8$	7
7	7	$2 \cdot 3 \equiv 6$	3
8	1	$2 \cdot 1 \equiv 2$	3
9	3	$2 \cdot 7 \equiv 4$	7

Na podlagi nekaj primerov vidimo, da so števke vrednosti izraza na mestu enic le 3 ali 7, kar pomeni, da to ni kvadrat. Dokažimo to še splošno. Opazimo, da je

- $3^4 \equiv 1 \pmod{10}$ in $7^4 \equiv 1 \pmod{10}$, kar pomeni, da je $3^{4k} \equiv 1 \pmod{10}$ in $7^{4k} \equiv 1 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k} + 2 \cdot 7^{4k} \equiv 3 \pmod{10}.$$

- $3^{4k} \cdot 3 = 3^{4k+1} \equiv 3 \pmod{10}$ in $7^{4k} \cdot 7 = 7^{4k+1} \equiv 7 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k+1} + 2 \cdot 7^{4k+1} \equiv 17 \equiv 7 \pmod{10}.$$

- $3^{4k+1} \cdot 3 = 3^{4k+2} \equiv 9 \pmod{10}$ in $7^{4k+1} \cdot 7 = 7^{4k+2} \equiv 9 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k+2} + 2 \cdot 7^{4k+2} \equiv 27 \equiv 7 \pmod{10}.$$

- $3^{4k+2} \cdot 3 = 3^{4k+3} \equiv 7 \pmod{10}$ in $7^{4k+2} \cdot 7 = 7^{4k+3} \equiv 3 \pmod{10}$ za nek $k \in \mathbb{N}$. Odtod sledi

$$3^{4k+3} + 2 \cdot 7^{4k+3} \equiv 13 \equiv 3 \pmod{10}.$$

  Dokazali smo, da je izraz za vsak n kongruenten bodisi 3 bodisi 7 po modulu 10, kar pa pomeni, da ne more biti kvadrat nobenega števila (glaj nalogo 13).

17. Ker je $3^2 \equiv -1 \pmod{10}$, je $3^4 \equiv 1 \pmod{10}$. Sledi

$$3^{400} = \left(3^4\right)^{100} \equiv 1 \pmod{10}.$$

Števka na mestu enic je 1.

18. Hitro ugotovimo, da za $k \in \mathbb{N}$ velja

$$\begin{aligned} 2^{4k} &\equiv 6 \pmod{10} \\ 2^{4k+1} &\equiv 2 \pmod{10} \\ 2^{4k+2} &\equiv 4 \pmod{10} \\ 2^{4k+3} &\equiv 8 \pmod{10} \end{aligned}$$

Ker je $2^{400} = 2^{4 \cdot 100}$, velja

$$2^{400} \equiv 6 \pmod{10}.$$

Števka na mestu enic je 6.

19. Ker je

$$3^{20} = 3486784401 \equiv 1 \pmod{100}.$$

velja

$$3^{400} = 3^{20 \cdot 20} \equiv 1^{20} = 1 \pmod{100}.$$

Zadnji dve števki sta torej 01.

20. $7777 \equiv 2 \pmod 5 \quad \Rightarrow \quad 7777^2 \equiv 2^2 \equiv -1 \pmod 5$.
Sledi $7777^4 \equiv (-1)^2 \equiv 1 \pmod 5$ in $(7777^4)^{2222} = 7777^{8888} \equiv 1 \pmod 5$

21. $5|81n + 53$ natanko tedaj, ko je $81n + 53 \equiv 0 \pmod 5$.
Sledi

$$\begin{aligned} 81n &\equiv -53 \pmod 5 \\ n &\equiv 2 \pmod 5 \end{aligned}$$

Rešitev je oblike $n = 5k + 2, k \in \mathbb{Z}$.

22. Ker je $10 \equiv 1 \pmod 9$, velja $10^n \equiv 1 \pmod 9$. Zato je

$$10^{n+1} + 4 \cdot 10^n + 4 \equiv 1 + 4 \cdot 1 + 4 = 9 \equiv 0 \pmod 9$$

23. Zadosti je pokazati, da je izraz $5^{99} + 11^{99} + 17^{99}$ deljiv s 3 ter 11.

- deljivost s 3 :

  Ker je $5^{99} \equiv 2^{99} \pmod 3$,$11^{99} \equiv 2^{99} \pmod 3$,$17^{99} \equiv 2^{99} \pmod 3$, sledi $5^{99} + 11^{99} + 17^{99} \equiv 2^{99} + 2^{99} + 2^{99} = 3 \cdot 2^{99} \equiv 0 \pmod 3$.

- deljivost z 11 :

  Ker je $17 \equiv (-5) \pmod 3$, sledi $17^{99} \equiv (-5)^{99} \pmod 3$.
  $5^{99} + 11^{99} + 17^{99} \equiv 5^{99} + 0^{99} + (-5)^{99} \equiv 0 \pmod{11}$.

24. Podobno kot v nalogi 16 zaslutimo (s pomočjo ustrezne tabele) tri sorodne primere, ki jih obravnavamo ločeno:

- Naj bo $n = 3k$.

  Potem je

$$29^{3k} \equiv 3^{3k} = 27^k \equiv 1 \pmod{13},$$
$$16^{3k+1} = 16^{3k} \cdot 16 \equiv 3^{3k} \cdot 3 \equiv 3 \pmod{13},$$
$$42^{3k+2} = 42^{3k} \cdot 42^2 \equiv 3^{3k} \cdot 9 \equiv 9 \pmod{13}.$$

- Naj bo $n = 3k + 1$.

  Potem je

  $$29^{3k+1} \equiv 3^{3k+1} = 27^k \cdot 3 \equiv 3 \pmod{13},$$
  $$16^{(3k+1)+1} = 16^{3k} \cdot 16^2 \equiv 3^{3k} \cdot 3^2 \equiv 9 \pmod{13},$$
  $$42^{(3k+1)+2} = 42^{3k} \cdot 42^3 \equiv 3^{3k} \cdot 27 \equiv 1 \pmod{13}.$$

- Naj bo $n = 3k + 2$.

  Potem je

  $$29^{3k+2} \equiv 3^{3k} \cdot 9 = 27^k \equiv 9 \pmod{13},$$
  $$16^{(3k+2)+1} = 16^{3k} \cdot 16^3 \equiv 3^{3k} \cdot 1 \equiv 1 \pmod{13},$$
  $$42^{(3k+2)+2} = 42^{3k} \cdot 42^4 \equiv 3^{3k} \cdot 3 \equiv 3 \pmod{13}.$$

V vsakem primeru velja

$$29^n + 16^{n+1} + 42^{n+2} \equiv 1 + 3 + 9 \equiv 0 \pmod{13}$$

25. Mora veljati $3(n^2 + n) + 7 \equiv 0 \pmod{5}$.

Preoblikujemo $3n^2 + 3n + 7 \equiv 3n^2 + 3n - 3 \equiv 0 \pmod{5}$ oziroma $3(n^2 + n - 1) \equiv 0 \pmod{5}$. Ker je D(3,5)=1, lahko kongruenco delimo s 3:

$$(n^2 + n - 1) \equiv 0 \pmod{5}.$$

Imamo 5 možnosti (računano po mod 5)

$n \equiv 0$	$(n^2 + n - 1) \equiv 1$
$n \equiv 1$	$(n^2 + n - 1) \equiv 1$
$n \equiv 2$	$(n^2 + n - 1) \equiv 0$
$n \equiv 3$	$(n^2 + n - 1) \equiv 2$
$n \equiv 4$	$(n^2 + n - 1) \equiv -1$

Pogoj je izpolnjen le za naravne n oblike $n = 4k + 2$ oziroma množico

$$n \in \{2, 6, 10, \ldots\}.$$

26. Mora veljati kongrunca $x^2 \equiv -1 \pmod{13}$.

$$\begin{aligned} x \equiv 0 \pmod{13} &\Rightarrow x^2+1 \equiv 1 \pmod{13} \\ x \equiv 1 \pmod{13} &\Rightarrow x^2+1 \equiv 2 \pmod{13} \\ x \equiv 2 \pmod{13} &\Rightarrow x^2+1 \equiv 5 \pmod{13} \\ x \equiv 3 \pmod{13} &\Rightarrow x^2+1 \equiv 10 \pmod{13} \\ x \equiv 4 \pmod{13} &\Rightarrow x^2+1 \equiv 17 \equiv 4 \pmod{13} \\ x \equiv 5 \pmod{13} &\Rightarrow x^2+1 \equiv 26 \equiv 0 \pmod{13} \end{aligned}$$

Naravne rešitve so $x \in \{5, 18, 31, \ldots\}$.

27. Da bo število celo mora biti števec v ulomku $\frac{2m^3+3m^2+m}{6}$ deljiv s 6. Pokazati moramo, da velja $2m^3+3m^2+m \equiv 0 \pmod{6}$. Po trditvi 13 je kongruenca ekvivalentna

$$2m^3+3m^2+m = m(2m+1)(m+1) \equiv 0 \pmod{2}$$

in

$$2m^3+3m^2+m = m(2m+1)(m+1) \equiv 0 \pmod{3}$$

kar moramo tudi pokazati.

- Prva kongruenca je očitna, saj v primeru, da je m sod, trivialno velja, če je pa lih, pa je $2m+1$ sod, zato je produkt členov v obeh primerih sodo število.
- Če je v drugi kongruenci $m \equiv 0 \pmod{3}$, je tudi produkt $\equiv 0 \pmod{3}$.

  Če je $m \equiv 1 \pmod{3}$, je faktor $2m+1 \equiv 0 \pmod{3}$, zato je produkt $\equiv 0 \pmod{3}$.

  Če je $m \equiv 2 \pmod{3}$, je faktor $m+1 \equiv 0 \pmod{3}$, zato je produkt $\equiv 0 \pmod{3}$.

  Odtod sklepamo, da velja $2m^3+3m^2+m \equiv 0 \pmod{6}$.

28. Podobno kot v prejšnjem primeru, moramo pokazati veljavnost kongruence $3n^5+5n^3+7n \equiv 0 \pmod{15}$, kar je ekvivalentno

$$3n^5+5n^3+7n \equiv 0 \pmod{5} \quad \text{in} \tag{3}$$

$$3n^5+5n^3+7n \equiv 0 \pmod{3} \tag{4}$$

Če v (3) odštejemo $(5n^3 + 5n)$ dobimo $3n^5 + 2n \equiv -(5n^2 + 5n) \equiv 0 \pmod 5$

Če v (4) odštejemo $(3n^5+3n^3+6n)$ dobimo $2n^3+n \equiv -(3n^5+3n^3+6n) \equiv 0 \pmod 3$.

29. $n^3 - n = n(n+1)(n-1) \equiv 0(mod3)$, saj imamo produkt treh zaporednih celih števil, ta pa je deljiv s 3.

30. $n^5 - n = n(n+1)(n+2)(n-1)(n-2) \equiv 0 \pmod 3$, saj imamo produkt petih zaporednih celih števil, ta pa je deljiv s 5.

31. $n^7 - n = n(n+1)(n^2-n+1)(n-1)(n^2+n+1)$.
Velja $n^2 + n + 1 \equiv n^2 + n - 6 \pmod 7$, $n^2 - n + 1 \equiv n^2 - n - 6 \pmod 7$, zato je $n^7 - n \equiv n(n+1)(n^2-n-6)(n-1)(n^2+n-6) =$
$= n(n+1)(n-3)(n+2)(n-1)(n+3)(n-2) \equiv 0 \pmod 7$, saj imamo produkt sedmih zaporednih celih števil, ta pa je deljiv s 7.

32. $x = 23$