Modularna aritmetika - rješenja

Metamath

2. listopada 2022.

1 Osnovni lanac

Zadatak 1

(Školjka) Ako je $x^2 \equiv y^2 \mod n$, je li nužno $x \equiv y \mod n$?

Prvo rješenje: Prebacimo sve na istu stranu

$$x^2 - y^2 \equiv 0 \pmod n$$
$$(x-y)(x+y) \equiv 0 \pmod n$$

Iz ovoga se jasno vidi da je i $x \equiv -y \pmod n$ rješenje. Naravno, potrebno je provjeriti je li moguće da je $x \equiv -x \pmod n$ za sve x. Ako vrijedi za sve x onda vrijedi i za $x = 1$

$$1 \equiv -1 \pmod n$$
$$2 \equiv 0 \pmod n$$

Dakle, ako je $n > 2$, nije nužno, no za $n = 1$ i $n = 2$ je.
Drugo rješenje: Sjetimo se činjenice da $x^2 = (-x)^2$. Ako su brojevi jednaki sigurno daju isti ostatak pri dijeljenju sa bilo kojim brojem n. Ponovno, odmah je očito da je $x \equiv -y \pmod n$ rješenje. Naravno, potrebno je provjeriti je li moguće da je $x \equiv -x \pmod n$ za sve x. Ako vrijedi za sve x onda vrijedi i za $x = 1$

$$1 \equiv -1 \pmod n$$
$$2 \equiv 0 \pmod n$$

Dakle, ako je $n > 2$, nije nužno, no za $n = 1$ i $n = 2$ je.
Priznaje se i rješenje kontraprimjerom, npr.

$$1^2 \equiv 2^2 \mod 3$$
$$1 \not\equiv 2 \mod 3$$

Zadatak 2

Postoji li broj koji je višekratnik od 2, ali ne i višekratnik od 4 i potpun je kvadrat?

Rješenje:
U obliku jednadžbe, problem je naći $n \in \mathbb{N}$ takav da

$$4n + 2 = x^2$$

Ako pogledamo obje strane jednadžbe modulo 4, dobijamo

$$x^2 \equiv 2 \mod 4$$

No prisjetimo se da ako je cijeli broj x paran, $x = 2k$, onda njegov kvadrat daje ostatak 0 pri dijeljenju sa četiri.

$$x^2 = 4k^2 \equiv 0 \mod 4$$

Ako je x neparan, $x = 2k + 1$, onda njegov kvadrat daje ostatak 1 pri dijeljenju s četiri.

$$x^2 = 4k^2 + 4k + 1 \equiv 1 \mod 4$$

Dakle, kvadrat nekog broja može davati jedino ostatke 0 ili 1 pri dijeljenju sa četiri.
Dakle, broj kakav se traži u zadatku ne postoji.

Zadatak 3

Neka je $p > 2$ prost broj i zbroj dvaju kvadrata. Pokaži da je $p-1$ djeljiv s 4.

Rješenje: Neka su $x, y \in \mathbb{N}$ takvi da

$$x^2 + y^2 = p$$

Ako su x i y oba parna ili oba neparna, onda su i x^2 i y^2 oba parna ili oba neparna, a onda je njihov zbroj paran, no jedini paran prost broj je 2, a $p > 2$. Dakle, x i y su različitih parnosti. Neka je $x = 2k$, $y = 2l + 1$ za $k, l \in \mathbb{N}$.

$$\begin{aligned}(2k)^2 + (2l+1)^2 &= p \\ 4k^2 + 4l^2 + 4l + 1 &= p\end{aligned}$$

Pogledajmo jednadžbu modulo 4 i vidimo

$$\begin{aligned}p &\equiv 1 \mod 4 \\ p - 1 &\equiv 0 \mod 4\end{aligned}$$

Što je trebalo pokazati.

Zadatak 4

Za koje brojeve $d \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ vrijedi svojstvo da za sve prirodne brojeve n vrijedi da d^n daje uvijek isti ostatak pri dijeljenju s 10?

Rješenje:
Kako bismo odmah eliminirali neke kandidate, pogledajmo za koje vrijedi $d^2 \equiv d \mod 10$.
Provjerom utvrđujemo da to vrijedi za $d = 0, 1, 5, 6$.
Za formalan dokaz da ako vrijedi $d^2 \equiv d \mod 10$, onda vrijedi i $d^n \equiv d \mod 10$ za svaki $n \in \mathbb{N}$ pričekajmo Metamath tjedan indukcije.

Zadatak 5

Dokaži da

$$\frac{21n-3}{4} \quad \text{i} \quad \frac{15n+2}{4}$$

ne mogu oba biti cijeli brojevi za isti $n \in \mathbb{N}$.

Rješenje:
Ako su oba cijeli brojevi, onda je i njihova razlika cijeli broj:

$$\frac{21n-3-15n-2}{4} = \frac{6n-5}{4}$$

No $6n-5$ nije djeljivo sa četiri.

$$6n-5 \equiv 6n+3 \equiv 2n+1 \equiv 1 \text{ ili } 3 \pmod 4$$

Zadatak 6

Pronađi prirodne brojeve x, y koji zadovoljavaju jednadžbu $x^2+4x+1=4y^2$.

Rješenje:
Zapišimo jednadžbu kao

$$x^2+1 = 4y^2-4x$$

te ju promotrimo modulo 4:

$$\begin{aligned} x^2+1 &\equiv 0 \pmod 4 \\ x^2 &\equiv -1 \pmod 4 \\ x^2 &\equiv 3 \pmod 4 \end{aligned}$$

No to je nemoguće jer smo pokazali da kvadrat broja daje ostatak 0 ili 1 pri dijeljenju sa četiri.
Dakle, nema prirodnih brojeva koji zadovoljavaju jednadžbu.

Zadatak 7

Dokažite da postoji prirodan broj koji započinje znamenkama 1938472638628, a djeljiv je brojem 2022.

Rješenje 1:
Broj 19384726386282022 daje neki ostatak k pri dijeljenju s 2022, tj.

$$19384726386282022 \equiv k \mod 2022 \quad (\text{za neki } k \in \{0, 1, 2, \ldots, 2021\})$$

$$19384726386282022 - k \equiv 0 \mod 2022$$

Budući da je $k < 2022$, tražene će znamenke u broju ostati iste, a traženi broj je onda

$$19384726386282022 - k$$

Rješenje 2: Od 2022 uzastopna broja

$$19384726386280000, 19384726386280001, \ldots, 19384726386282021$$

Sigurno će jedan biti djeljiv s 2022.

2 Ozbiljniji lanac

Zadatak 1

Koje su posljednje dvije znamenke broja 17^{2022}?

Rješenje:
Tražimo $17^{2022} \mod 100$.

$$\begin{aligned}
17^2 &\equiv 89 \mod 100 \\
17^4 &\equiv 21 \mod 100 \\
17^8 &\equiv 41 \mod 100 \\
17^{10} &\equiv 41 \cdot 89 \equiv 49 \mod 100 \\
17^{20} &\equiv 49^2 \equiv 1 \mod 100
\end{aligned}$$

Pa je

$$17^{2022} \equiv 17^{2020} \cdot 17^2 \equiv \left(17^{20}\right)^{101} \cdot 89 \equiv 89 \mod 100$$

Dakle, zadnje dvije znamenke su $\boxed{89}$.

Zadatak 2

Fibonaccijev niz je niz brojeva $1, 1, 2, 3, 5, 8, 13, \ldots$, gdje je svaki sljedeći broj zbroj dva prethodna. Koji je ostatak pri dijeljenju stotog člana Fibonaccijevog niza brojem 8?

Rješenje: Ne trebamo se mučiti zbrajati brojeve pa onda gledati mod 8. Zbog svojstva zbrajanja kongruencija, dovoljno je je početi od $1, 1$ i zbrajati $\mod 8$.

$$1 \mod 8 \tag{1}$$
$$1 \mod 8 \tag{2}$$
$$2 \mod 8 \tag{3}$$
$$3 \mod 8 \tag{4}$$
$$5 \mod 8 \tag{5}$$
$$0 \mod 8 \tag{6}$$
$$5 \mod 8 \tag{7}$$
$$5 \mod 8 \tag{8}$$
$$2 \mod 8 \tag{9}$$
$$7 \mod 8 \tag{10}$$
$$1 \mod 8 \tag{11}$$
$$0 \mod 8 \tag{12}$$
$$1 \mod 8 \tag{13}$$
$$1 \mod 8 \tag{14}$$
$$2 \mod 8 \tag{15}$$
$$3 \mod 8 \tag{16}$$
$$5 \mod 8 \tag{17}$$
$$\vdots \tag{18}$$

Primijetimo da smo u 13. i 14. članu niza opet došli do $1, 1$ pa će se uzorak ponavljati. Nakon 12 članova, opet smo kao na prvom članu. Zato će i $97. = 8 \cdot 12 + 1.$ član biti 1 pa će 98. član biti 1, 99. član će biti 2, a stoti član će biti 3.
Dakle, 100. član Fibonaccijevog niza daje ostatak 3 pri dijeljenju s 8.

Zadatak 3

U godini N, tristoti dan je utorak. U godini N+1, dvjestoti dan je također utorak. Koji dan u tjednu je bio na stoti dan godine N-1?

Rješenje:
Postoji ili $200 + 65 = 265$ ili $200 + 66 = 266$ dana između prva dva datuma, ovisno o tome je li godina prijestupna godina ili ne. Budući da je $266 \equiv 0 \mod 7$, moguće je da su oba dana utorak. Dakle, imamo prijestupnu godinu, a važna informacija je da $N - 1$ nije. Postoji $265 + 300 = 565$ dana između zadanih dana u godinama $N - 1$ i N. Budući da je

$$565 \equiv 5 \mod 7$$

i budući da oduzimamo dane, ostaje nam 5 dana prije utorka, a to je <u>četvrtak</u>.

Zadatak 4

(Školjka) Broj aabb je kvadrat prirodnog broja (a i b su znamenke). Koji je to broj?

Rješenje:
Prvo, kojom znamenkom uopće može završiti kvadrat broja? Ako je $n = 10x + y$, onda

$$n^2 \equiv (10x + y) \equiv 100x^2 + 20xy + y^2 \equiv y^2 \mod 10$$

Ako je $y \in \{0,1,2,3,4,5,6,7,8,9\}$, onda je $y^2 \in \{0,1,4,9,16,25,36,49,64,81\}$ pa zadnja znamenka kvadrata može biti samo 0, 1, 4, 5, 6 ili 9.
Zato i za naš b vrijedi $b \in \{0,1,4,5,6,9\}$.
Iz prethodnih rješenja znamo i da kvadrati daju ostatak 0 ili 1 pri dijeljenju s 4.
Provjerimo mogućnosti:

$$b = 0 \implies bb \equiv 00 \equiv 0 \mod 4 \qquad \text{Dakle, } b = 0 \text{ je mogućnost}$$
$$b = 1 \implies bb \equiv 11 \equiv 3 \mod 4 \qquad \text{Dakle, } b = 1 \text{ nije mogućnost}$$
$$b = 4 \implies bb \equiv 44 \equiv 0 \mod 4 \qquad \text{Dakle, } b = 4 \text{ je mogućnost}$$
$$b = 5 \implies bb \equiv 55 \equiv 3 \mod 4 \qquad \text{Dakle, } b = 5 \text{ nije mogućnost}$$
$$b = 6 \implies bb \equiv 66 \equiv 2 \mod 4 \qquad \text{Dakle, } b = 6 \text{ nije mogućnost}$$
$$b = 9 \implies bb \equiv 99 \equiv 3 \mod 4 \qquad \text{Dakle, } b = 99 \text{ nije mogućnost}$$

Sada imamo $b \in \{0,4\}$ Da bi kvadrat završavao na 00, broj kojeg kvadriramo mora biti djeljiv s 10. Brojevi koji su djeljivi s 10 čiji su kvadrati četveroznamenkasti su 40, 50, 60, 70, 80, 90. Niti jedan od njih ne daje kvadrat oblika *aabb*.
Dakle, $b = 4$.
Koje ostatke mogu davati kvadrati $\mod 9$?

n	0	1	2	3	4	5	6	7	8
n^2	0	1	4	0	7	7	0	4	1

Kvadrat broja može davati ostatke 0, 1, 4 i 7 pri dijeljenju s 9.
Prirodni je broj djeljiv s 9 ako mu je zbroj znamenki djeljiv s 9. Zbroj znamenki našeg broja je $2a + 8$.

...nastavak

Ako naš broj daje ostatak 0 pri dijeljenju s 9, vrijedi:

$$\begin{aligned} 2a + 8 &\equiv 0 \mod 9 \\ 2a &\equiv -8 \mod 9 \\ a &\equiv -4 \mod 9 \\ a &\equiv 5 \mod 9 \implies a = 5 \end{aligned}$$

Ako naš broj daje ostatak 1 pri dijeljenju s 9, vrijedi:

$$\begin{aligned} 2a + 8 &\equiv 1 \mod 9 \\ 2a &\equiv -7 \mod 9 \\ 2a &\equiv 2 \mod 9 \\ a &\equiv 1 \mod 9 \implies a = 1 \end{aligned}$$

Ako naš broj daje ostatak 4 pri dijeljenju s 9, vrijedi:

$$\begin{aligned} 2a + 8 &\equiv 4 \mod 9 \\ 2a &\equiv -4 \mod 9 \\ a &\equiv -2 \mod 9 \\ a &\equiv 7 \mod 9 \implies a = 7 \end{aligned}$$

Ako naš broj daje ostatak 7 pri dijeljenju s 9, vrijedi:

$$\begin{aligned} 2a + 8 &\equiv 7 \mod 9 \\ 2a &\equiv -1 \mod 9 \\ 2a &\equiv 8 \mod 9 \\ a &\equiv 4 \mod 9 \implies a = 4 \end{aligned}$$

Dobili smo da je $a \in \{1, 4, 5, 7\}$
Prisjetimo se i da je prirodni je broj djeljiv s 11 ako mu je razlika zbroja znamenki na neparnim mjestima odnosno na parnim mjestima, idući zdesna na lijevo, djeljiva s 11.
Očito je i naš broj djeljiv s 11, neovisno o vrijednostima a i b, a budući da je kvadrat, djeljiv je i s 11^2.
Sada treba za svakog od naših kandidata 1144, 4444, 5544 i 7744 provjeriti je li djeljiv s 11^2. Dobijamo da je jedini mogući kandidati 7744, i, zbilja,

$$7744 = 88^2$$

Zadatak 5

Dokaži da ne postoje cijeli brojevi x, y za koje vrijedi $x^2+3xy-2y^2=122$.

Rješenje:
Riješimo kvadratnom jednadžbom za x:

$$x^2+3xy-2y^2-122=0$$
$$x_{1,2}=\frac{-3y\pm\sqrt{9y^2-4\left(-2y^2-22\right)}}{2}$$
$$=\frac{-3y\pm\sqrt{17y^2+488}}{2}$$

Da bi postojao x, diskriminanta, $17y^2+488$ mora biti kvadrat nekog broja.
Koje ostatke mogu davati kvadrati $\mod 17$?

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
n^2	0	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

Dakle to mogu biti samo brojevi $0,1,2,4,8,9,13,15,16$, ali

$$17y^2+488\equiv 488\equiv 12 \mod 17$$

Što nije moguće.

3 Teorija brojeva mix - prva dva zadatka

Zadatak 1

Dani su jedinstveni prirodni brojevi a_2, a_3, a_4, a_5, a_6, a_7 takvi da

$$\frac{5}{7} = \frac{a_2}{2!} + \frac{a_3}{3!} + \frac{a_4}{4!} + \frac{a_5}{5!} + \frac{a_6}{6!} + \frac{a_7}{7!}$$

gdje $0 \leq a_i < i$ za $i = 2, 3, 4, 5, 6, 7$. Koliko je $a_2 + a_3 + a_4 + a_5 + a_6 + a_7$?

Rješenje:
Prvo pomnožimo sa 7!:

$$5 \cdot 6! = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6) + a_6 \cdot 7 + a_7$$

Budući da vrijedi $0 \leq a_i < i$ za svaki i, i svi članovi zdesna su su višekratnici broja 7, promotrimo jednadžbu modulo 7.

$$\begin{aligned} a_7 &\equiv 5 \cdot 6! \mod 7 \\ &\equiv 5 \cdot 720 \mod 7 \\ &\equiv 5 \cdot 6 \mod 7 \\ &\equiv 2 \mod 7 \end{aligned}$$

Budući da je $0 \leq a_7 < 7$, imamo $a_7 = 2$ i

$$5 \cdot 6! - 2 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6) + a_6 \cdot 7$$

Sada gledamo ovu jednadžbu modulo 6.

$$\begin{gathered} 7a_6 \equiv -2 \equiv 28 \mod 6 \\ a_6 \equiv 4 \mod 6 \implies a_6 = 4 \end{gathered}$$

Nastavljamo tako da sljedeću jednadžbu gledamo modulo 5

$$5 \cdot 6! - 2 - 4 \cdot 7 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5) + a_5(7 \cdot 6)$$

Što nam odmah daje $a_5 = 0$
Dobijamo

$$5 \cdot 6! - 2 - 4 \cdot 7 = a_2(7 \cdot 6 \cdot 5 \cdot 4 \cdot 3) + a_3(7 \cdot 6 \cdot 5 \cdot 4) + a_4(7 \cdot 6 \cdot 5)$$

pa dijeljenjem sa $7 \cdot 6 \cdot 5$ dobijamo

$$17 = 12a_2 + 4a_3 + a_4$$

Mogli bismo nastaviti uzimati modulo 4 i 3, ali već je iz ove jednadžbe primjetno $a_4 = a_3 = a_2 = 1$.
Zaključujemo

$$a_2 + a_3 + a_4 + a_5 + a_6 + a_7 = 1 + 1 + 1 + 0 + 4 + 2 = 9$$

Zadatak 2

Pronađite cjelobrojne vrijednosti x između -10 i 15 takve da je $P = 3x^3 + 7x^2$ kvadrat cijelog broja.

Rješenje:
Budući da je $P = 3x^3 + 7x^2 = x^2(3x + 7) = N^2$, ili je $x = 0$ ili je $3x + 7$ kvadrat broja. Neka je

$$
\begin{aligned}
3x + 7 &= K^2 \\
K^2 \equiv 3x + 7 &\equiv 7 \equiv 1 \mod 3
\end{aligned}
$$

Ako je broj K oblika $3k$, onda $K^2 \not\equiv 1 \mod 3$, ali ako je K oblika $3k + 1$ ili $3k + 2$, onda vrijedi $K^2 \equiv 1 \mod 3$.
Za $k = 0$ imamo $K = 1, 2$ pa je $x = -2, -1$. Za $k = 1$ imamo $K = 4, 5$ pa je $x = 3, 6$. Za $k = 2$ imamo $K = 7, 8$ pa je $x = 14, 19$
Dakle, traženi skup je $\{-2, -1, 0, 3, 6, 14\}$.