1 Дјељивост, НЗД...

1

●●●●

Познато је да полином $P(x)$ при дијељењу са $x-1$ даје остатак 3, а при дијељењу са $x-2$ даје остатак 5. Колики ће бити остатак полинома $P(x)$ при дијељењу са $(x-1)(x-2)$?

Доказ. $P(x)$ можемо записати у облику $P(x) = Q(x)(x-2)(x-1)+r(x)$ и важи да је степен полинома r мањи или једнак 1.

Како је $P(2) = 5$ и $P(1) = 3$, то имамо да је $r(1) = 3$ и $r(2) = 5$. Па рјешавањем система

$$a \cdot 1 + b = 3$$

$$a \cdot 2 + b = 5$$

Добијамо да је $r(x) = 2x + 1$

□

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

2

●●●●

Нека су a и b релативно прости природни бројеви. Нађи нзд$(a+b, a^2+b^2)$.

Доказ. Претпоставимо да прост број p дијели $a+b$ и a^2+b^2 . Како $p \mid a+b$ онда по дефиницији важи да је $a \equiv -b \pmod{p}$. Даље је $0 \equiv a^2+b^2 \equiv (-b)^2+b^2 \equiv 2b^2 \pmod{p}$ тј. $p \mid 2b^2$.

Ако је $p > 2$ тада p мора бити непаран број , из тога и из $p \mid 2b^2$ слиједи да мора важити да $p \mid b^2$. Пошто је p прост онда мора важити да је $p \mid b$, али онда даље вриједи $a \equiv -0 \pmod{p}$ тј. $p \mid a$. Међутим то је у контрадикцији са чињеницом да су a и b релативно прости бројеви. Дакле не постоји непаран прост број који је заједнички дјелилац за $a+b$ и a^2+b^2 , одавде закључујемо да се нзд$(a+b, a^2+b^2)$ може састојати само од простог фактора 2 , тј. нзд$(a+b, a^2+b^2)$ може бити $1, 2, 2^2, 2^3, \ldots$.

Даље, 2 дијели $a+b$ и a^2+b^2 ако и само ако су a и b исте парности. Како су a и b релативно прости , не могу бити оба парни , па 2 дијели $a+b$ и a^2+b^2 ако и само ако су a и b непарни.

Дакле , у случајевима a - паран , b - непаран и обратно 2 није заједнички дјелилац бројева $a+b$ и a^2+b^2 , па је онда нзд$(a+b, a^2+b^2)=1$.

Остаје још случај кад су a и b непарни , тада је 2 заједнички дјелилац $a+b$ и a^2+b^2. Доказаћемо да 2^2 није заједнички дјелилац за $a+b$ и a^2+b^2 и затим коначно закључити да је нзд$(a+b, a^2+b^2)=2$. Због непарности a и b постоје 4 могућа случаја:

$$\begin{array}{ll}
(1) & a \equiv b \equiv 1 \pmod 4 \implies a+b \equiv 2 \pmod 4 \implies 4 \nmid (a+b) \\
(2) & a \equiv b \equiv 3 \pmod 4 \implies a+b \equiv 6 \equiv 2 \pmod 4 \implies 4 \nmid (a+b) \\
(3) & a \equiv 1 \pmod 4 \, , \, b \equiv 3 \pmod 4 \implies a^2+b^2 \equiv 2 \pmod 4 \implies 4 \nmid (a^2+b^2) \\
(4) & a \equiv 3 \pmod 4 \, , \, b \equiv 1 \pmod 4 \implies a^2+b^2 \equiv 2 \pmod 4 \implies 4 \nmid (a^2+b^2)
\end{array}$$

Коначно је

$$\text{нзд}(a+b, a^2+b^2) = \begin{cases} 2 & , \ a \equiv b \equiv 1 \pmod 2 \\ 1 & , \ \text{иначе} \end{cases} .$$

☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`https://math.vanderbilt.edu/rolenl/IntroNTExam1S.pdf`

3

Нека су $F_0.F_1, F_2 \ldots$ Фибоначијеви бројеви, задати са $F_0 = F_1 = 1$ и $F_{n+1} = F_n + F_{n-1}$, $n \geq 1$. Доказати да је највећи заједнички дјелилац два узастопна Фибоначијева броја увијек 1 .

Доказ. Претпоставимо супротно

$$\text{нзд}(F_n, F_{n+1}) = a > 1.$$

Тада $a \mid F_n$ и $a \mid F_{n+1}$, а одатле $a \mid F_{n+1} - F_n$ тј. $a \mid F_{n-1}$. Даље $a \mid F_n - F_{n-1}$ тј. $a \mid F_{n-2}$. Настављајући овако добијамо да $a \mid F_1 = 1$, одатле слиједи да је $a = 1$. Контрадикција. ☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`https://math.vanderbilt.edu/rolenl/IntroNTExam1S.pdf`

4

Збир 49 природних бројева је једнак 999. Наћи највећу могућу вриједност њиховог највећег заједничког дјелиоца.

Доказ. Нека су $a_1, a_2, \ldots, a_{49}$ природни бројеви такви да

$$a_1 + a_2 + \cdots + a_{49} = 999\ ,\ \text{нзд}(a_1, a_2, \ldots, a_{49}) = d.$$

Знамо да $d \mid a_i \implies d \leq a_i\ ,\ i = 1, 2, \ldots, 49$. Осим тога можемо закључити и да $d \mid 999$. Даље

$$49d \leq a_1 + a_2 + \cdots + a_{49} = 999 \implies d \leq \frac{999}{49} < 21$$

Једини дјелиоци броја $999 = 3^3 \cdot 37$ мањи од 21 су $1, 3$ и 9 . Дакле , тражени вриједност је $d = 9$. Осим тога вриједност $d = 9$ се достиже за

$$\underbrace{9 + 9 + \cdots + 9}_{48} + 567 = 999.$$

$\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет из збирке задатака
Теорија бројева М.Станић Н.Икодиновић

5

Нека су a, b, c, d цијели бројеви такви да $a \mid b$, $b \mid c$ и $c \mid d$. Доказати да $a^3 \mid bcd$.

Доказ. Будући да $a \mid b$, $b \mid c$ и $c \mid d$ онда је $b = an$, $c = bm$, $d = ck$, $n, m, k \in \mathbb{Z}$. Даље је $c = (an)m$, $d = (anm)k$ и

$$bcd = (an)(anm)(anmk) = a^3 t \ \text{ гдје је } \ t = n^3 m^2 k \in \mathbb{Z}.$$

Одатле по дефиницији $a^3 \mid bcd$. $\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`https://www.math.ksu.edu/~pinner/math506/Spring2020/506S20Ex1Sols.pdf`

6

Доказати сљедећа својства
(а) $\text{нзд}(n, n+1) = 1$ за сваки природан број n
(б) $\text{нзд}(n, n+2) = 1$ за сваки непаран број природан број n
(ц) $\text{нзд}(a, b) = \text{нзд}(a, b-a)$ за све природне бројеве a и b
(д) $\text{нзд}(n, n+3) = 1$ за сваки природнан број n за које је $n \not\equiv 0 \pmod 3$

Доказ. (а) Нека је d заједнички дјелилац бројева n и $n+1$ тада $d \mid n$ и $d \mid (n+1)$ одакле слиједи

$$d \mid (n+1) - n \quad \text{tj.} \quad d \mid 1 \implies d = 1 \implies \text{нзд}(n, n+1) = 1$$

(б) Нека је d заједнички дјелилац бројева n и $n+2$, гдје је n непаран природан број . Тада

$$d \mid (n+2)-n \quad \text{tj.} \quad d \mid 2 \implies d = 1 \quad \text{ili} \quad d = 2$$

Како су n и $n+2$ непарни бројеви $d \neq 2 \implies d = 1 \implies \text{нзд}(n, n+2) = 1$.

(ц) Нека је $d = \text{нзд}(a,b)$ и $k = \text{нзд}(a, b-a)$.Тада

$$\begin{aligned} d \mid a \;\wedge\; d \mid b &\implies d \mid a \;\wedge\; d \mid b-a \overset{*}{\implies} d \mid k \\ k \mid a \;\wedge\; k \mid b-a &\implies k \mid a \;\wedge\; k \mid b \overset{*}{\implies} k \mid d \end{aligned}$$

Одатле закључујемо да $d = k$ што је и требало доказати . Импликације са $*$ су тачне јер је познато да сви заједнички дјелиоци за m и n дијеле $\text{нзд}(m,n)$, $m, n \in \mathbb{N}$.

(д) Користећи дио задатка под (ц) добијамо

$$\text{нзд}(n, n+3) = \text{нзд}(n, n+3-n) = \text{нзд}(n, 3)$$

Како важи услов $n \not\equiv 0 \pmod 3$ тј. $3 \nmid n$, закључујемо да је $1 = \text{нзд}(n,3) = \text{нзд}(n, n+3)$. ☐

(**Велимир Ђоровић 5/19 Б**) формулисан и ријешен због потреба другог задатка

7

Ако је p прост број већи од 2, доказати да вриједи да је бројилац сведеног разломка $1 + \frac{1}{2} + ... + \frac{1}{p-1}$ дјељив са p.

Доказ. Посматрајмо разломке

$$\begin{aligned} 1 + \frac{1}{p-1} &= \frac{p}{1*(p-1)}, \\ \frac{1}{2} + \frac{1}{p-2} &= \frac{2}{2*(p-2)}, \\ &\cdots \\ \frac{1}{k} + \frac{1}{p-k} &= \frac{p}{k*(p-k)} \end{aligned}$$

Како имамо паран број разломака који учествују у сууми, то ће сваки имати одговарајући пар. Па је

$$1 + \frac{1}{2} + \ldots + \frac{1}{p-1} = \frac{p}{1*(p-1)} + \frac{p}{2*(p-2)} + ... + \frac{p}{k*(p-k)}$$

Како сви разломци у бројиоцу имају p то можемо да га издвојимо испред суме. Како је p прост и сви чиниоци у имениоцу су мањи од p, то p неће моћи да се скрати са неким од њих. Па ће бројилац сведеног разломка бити дјељив са p. ☐

(**Велибор Дошљак 15/19 Б**) задатак са домаћег

8

Доказати да збир цифара потпуног квадрата не може бити 2012.

Доказ. Нека је n^2 број чија је сума цифара 2012. n може бити облика $3t, 3t+1$ или $3t-1$. Ако је н облика $3t$ тада је $n^2 = 9t^2$ дјељив са 3. Али тада је и његов збир цифара дјељив са 3, што је контрадикција јер 2012 није дјељив са 3.
Ако је н облика $3t+1$ тада је $n^2 = 9t^2 + 6t + 1$, па је $n^2 - 1$ дјељив са 3, али тада је и његов збир цифара дјељив са 3. Нека је n^2 облика $a_1a_2 \ldots a_n$ тако да $a_n > 0$. Тада је сума цифара броја $n^2 - 1$ једнака 2011 дјељива са 3 што је контрадикција. Ако је $a_n = 0$, тада $n^2 - 1$ облика $a_1a_2 \ldots (a_k - 1)99999$, па је сума цифара $2012 - 1 + (n-k) \cdot 9$ дјељива са 3, што је контрадикција. Исто важи и за n облика $3t - 1$ ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

9

Дужине страница правоуглог троугла су цијели бројеви. Могу ли дужине катета бити непарни бројеви?

Доказ. Нека су a, b, c дужине катета и хипотенузе респективно. Претпоставимо да је хипотенуза парне дужине. Тада $a = 2a^{'} + 1, b = 2b^{'} + 1, c = 2c^{'}$

$$(2c^{'})^2 = (2a^{'} + 1)^2 + (2b^{'} + 1)^2$$

$$4c^{'^2} = 4a^{'^2} + 4a^{'} + 1 + 4b^{'^2} + 4b^{'} + 1$$

А одавде закључујемо да би 4 морало да дијели 2 па имамо контрадикцију. Слиједи да је немогуће да хипотенуза буде парне дужине и катете непарних дужина.
Слично ако претпоставимо да је хипотенуза непарне дужине имамо

$$(2c^{'} + 1)^2 = (2a^{'} + 1)^2 + (2b^{'} + 1)^2$$

$$4c^{'^2} + 4c^{'} + 1 = 4a^{'^2} + 4a^{'} + 1 + 4b^{'^2} + 4b^{'} + 1$$

А одавде закључујемо да би 4 морало да дијели 1 па имамо контрадикцију. Слиједи да је немогуће да хипотенуза буде непарне дужине и катете непарних дужина.

Закључујемо да је немогуће да у троуглу са цјелобројним дужинама страница катете буду непарне дужине.

☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

10

●○○○

Ако је n природан број који има непаран број дјелилаца, тада је n потпун квадрат.

Доказ. Запишимо n као производ простих чинилаца.

$$n = {p_1}^{a_1}{p_2}^{a_2}...{p_k}^{a_k}$$

Тада је број дјелилаца броја n једнак $(a_1 + 1)(a_2 + 1)\cdots(a_n + 1)$. Како је број дјелилаца непаран свако $a_i + 1$ је непарно, па је a_i парно. Закључујемо да је n потпун квадрат. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

11

●●○○

Наћи највећи петоцифрени палиндром који је дјељив са 101. За природан број кажемо да је палиндром ако је једнак броју записаном истим цифрама у обрнутом редоследу .

Доказ. Нека је $abcba$ највећи петоцифрени палиндром који је дјељив са 101. Тада

$$\begin{aligned} abcba &= a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + b \cdot 10 + a = \\ &= a \cdot 10001 + b \cdot 1010 + c \cdot 100 = \\ &= 101 \cdot (99a + 10b + 1) + 2a - c \end{aligned}$$

Одавде закључујемо да је $2a - c \equiv 0 \pmod{101}$, даље $2a - c = 0$ зато што је $|2a - c| < 101$. Једначина $2a = c$ намеће услов $a \leq 4$ јер је $c \in \{0, 1, \dots, 9\}$. Како је $abcba$ највећи то имплицира да је $a = 4$. Одатле је $c = 8$. За цифру b нема никаквих услова тако да узимамо највећу могућу вриједност $b = 9$. Дакле , тражени број је 49 894. ☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет из збирке задатака
Теорија бројева М.Станић Н.Икодиновић

12

●●●○

Одредити све парове (a, b) природних бројева такве да је број $a^2b + a + b$ дјељив са $ab^2 + b + 7$.

Доказ. Нека пар (a, b) задовољава услов задатка, тј. нека

$$ab^2 + b + 7 \mid a^2b + a + b.$$

Размотримо најприје случајеве $b = 1$ и $b = 2$.

За $b = 1$ добија се да $a + 8 \mid a^2 + a + 1$.

Како је $a^2 + a + 1 = (a+8)(a-7) + 57$, то $a + 8 \mid 57 = 3 \cdot 19$, па постоје двије могућности $a = 11$ и $a = 49$. Провјером се показује да парови (11, 1) и (49, 1) задовољавају услов задатка.

За $b = 2$ добијамо услов $4a + 9 \mid 2a^2 + a + 2$.

Како је $8(2a^2 + a + 2) = (4a + 9)(4a - 7) + 79$ слиједи да $4a + 9 \mid 79$, што је очигледно немогуће, па у овом случају нема решења.

Нека је сада $b \geq 3$. Како је

$$b(a^2b + a + b) = a(ab^2 + b + 7) + b^2 - 7a,$$

то слиједи да $ab^2 + b + 7 \mid b^2 - 7a$. При том број $b^2 - 7a$ не може бити позитиван, јер је, због $a \geq 1$, $b^2 - 7a < ab^2 + b + 7$. С друге стране је (због $b \geq 3$)

$$7a - b^2 < 7a < 9a \leq ab^2 + b + 7,$$

а како је број $7a - b^2$ дјељив са $ab^2 + b + 7$, то ни он не може бити позитиван. Дакле $b^2 = 7a$. Одатле слиједи да $7 \mid b$, па је $b = 7k$, $k \in \mathbb{N}$. При провјери добијамо да сваки пар облика $(7k^2, 7k)$, $k \in \mathbb{N}$ задовољава услов задатка.

Дакле, сва решења су: (11, 1), (49, 1) и $(7k^2, 7k)$, $k \in \mathbb{N}$.

□

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

13

Ако је збир неких 2016 природних бројева дјељив са 6, онда је и збир њихових кубова дјељив са 6. Доказати.

Доказ. За сваки природан број a важи да је број $a^3 - a = a(a-1)(a+1)$ дјељив са 6.Дакле, број $a_1^3 - a_1 + a_2^3 - a_2 + \ldots + a_{2016}^3 - a_{2016}$ је дјељив са 6. Дати израз можемо написати у облику $(a_1^3 + a_2^3 + \ldots + a_{2016}^3)$ - $(a_1 + a_2 + \ldots + a_{2016})$. Како је збир $a_1 + a_2 + \ldots + a_{2016}$ дјељив са 6 , онда је и збир кубова $a_1^3 + a_2^3 + \ldots + a_{2016}^3$ дјељив са 6. □

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://www.pmf.ni.ac.rs/mii-content/2016-3-2/Zadaci%20sa%20brojem%202016.pdf`

14

Одреди цифре a, b и c тако да број $a2016bc$ буде највећи могући, дјељив са 12 и да све његове цифре буду различите.

Доказ. Знамо да је број дјељив са 12 акко је дјељив и са 3 и са 4. Број је дјељив са 4 ако му је двоцифрени завршетак дјељив са 4, одакле закључујемо да је цифра c парна. Због услова о различитости цифара, једине могућности за цифру c су 4 и 8. Како двоцифрени завршетак мора бити дјељив са 4 и цифре различите, једине могућности за b су такође цифре 4 и 8. Дакле, последње двије цифре, односно b и c су, редом бројеви 8 и 4. Да би број био дјељив са 3, збир цифара $a+2+0+1+6+8+4 = a+21$ мора бити дјељив са 3. Како би и овај услов важио, једине преостале могућности за цифру a су 3 и 9, одакле због услова да тражени број буде највећи могући, добијамо број 9201684. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://www.pmf.ni.ac.rs/mii-content/2016-3-2/Zadaci%20sa%20brojem%202016.pdf`

15

Доказати да је број $1^{2015}+2^{2015}+3^{2015}+\ldots+2015^{2015}$ дјељив са 2015.

Доказ. У овом збиру један сабирак, 2015^{2015} је дјељив са 2015. Ако уочимо да се преосталих 2014 сабирака могу груписати у групе од по два сабирка, 1^{2015} и 2014^{2015}, 2^{2015} и 2013^{2015}, $\ldots$ и искористимо познату релацију $a^{2n+1}+b^{2n+1} = (a+b)(a^{2n}-a^{2n-1}\cdot b+\ldots+a\cdot b^{2n-1}-b^{2n})$, $n\in\mathbb{N}$, добићемо још 1007 сабирака дјељивих са 2015, па ће цијели збир бити дјељив са 2015. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://www.pmf.ni.ac.rs/mii-content/2015-3-1/Zadaci%20sa%20brojevima%202015%20i%202016.pdf`

16

Наћи све тројке природних бројева (a, b, c) такве да производ свака два броја даје остатак 1 при дјељењу са трећим.

Доказ. Услов задатка можемо формулисати на следећи начин: постоје цијели бројеви α, β, γ тако да је

$$ab-1=\gamma c,\quad bc-1=\alpha a,\quad ca-1=\beta b,$$

за посматране природне бројеве a, b, c. Примијетимо да при томе a, b, c морају бити различити од 1. Множењем горњих једнакости, добијамо:

$$\alpha\beta\gamma abc=(abc)^2-abc(a+b+c)+ab+bc+ca-1.$$

Пребацујући на једну страну све чланове који садрже a, b, c, закључујемо да постоји природан број μ тако да је

$$\mu abc=ab+bc+ca-1. \tag{1.1}$$

Даље, разликујемо два случаја: ако су нека два броја једнака, нпр. $a=b$ тада важи $\alpha a = ac-1$. Слиједи $a=1$ што је немогуће. Значи могућ је само други случај, када су бројеви

a, b, c различити. Нека је нпр. $a < b < c$. Тада имамо, на основу горње једнакости и управо усвојеног поретка:

$$abc < ab + bc + ca < 3bc,$$

Па је $a < 3$, тј. $a = 2$. Убрштавајући у (1.1) имамо:

$$(2\mu - 1)bc = 2(b + c) - 1,$$

па закључујемо:

$$bc < 2(b + c) < 4c,$$

тј. $b < 4$. Како је $b > a = 2$, мора бити $b = 3$. Отуда слиједи

$$\gamma c = 5,$$

па је $c = 5$. Сада се сва решења задатка добијају као пермутације тројке $(2, 3, 5)$. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет из
Елементарна теорија бројева Игор Долинка

17
●●●●

Доказати да је за сваки природан број n број $2^{3^n} + 1$ дјељив са 3^{n+1} и није дјељив са 3^{n+2}.

Доказ. Доказ оба тврђења изводимо идукцијом по n.

За $n = 1$, непосредно се провјерава да $3^2 \mid 2^3 + 1$.

Претпоставимо да $3^{n+1} \mid 2^{3^n} + 1$. Тада $(3^{n+1})^3 \mid (2^{3^n} + 1)^3$, тј.

$$3^{3n+3} \mid 2^{3^{n+1}} + 1 + 3 \cdot 2^{3^n} \cdot (2^{3^n} + 1).$$

Како је $3n + 3 > n + 2$, из горње формуле слиједи да

$$3^{n+2} \mid 2^{3^{n+1}} + 1 + 3 \cdot 2^{3^n} \cdot (2^{3^n} + 1).$$

По индуктивној претпоставци $3^{n+1} \mid 2^{3^n} + 1$, па $3^{n+2} \mid 3 \cdot (2^{3^n} + 1)$. Дакле, $3^{n+2} \mid 2^{3^{n+1}} + 1$.

Такође, за $n = 1$ непосредно провјеравамо да $3^3 \nmid 2^3 + 1$.

Претпоставимо да $3^{n+2} \nmid 2^{3^n} + 1$, за неки природни број n. Поступајући као у доказу претходног тврђења добијамо да важи:

$$3^{n+3} \mid 2^{3^{n+1}} + 1 + 3 \cdot 2^{3^n} \cdot (2^{3^n} + 1).$$

Сада, ако $3^{n+3} \mid 2^{3^{n+1}} + 1$, онда $3^{n+3} \mid 3 \cdot 2^{3^n} \cdot (2^{3^n} + 1)$, одакле слиједи да $3^{n+2} \mid 2^{3^n} + 1$, супротно индуктивној претпоставци. Дакле, 3^{n+3} не дијели $2^{3^{n+1}} + 1$, чиме је доказ индукцијом завршен. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

18

●●●●

Наћи све природне бројеве који се завршавају двијема истим цифрама којима се завршавају њихови квадрати.

Доказ. Нека се a и a^2 завршавају двијема истим цифрама тј. $a^2 \equiv a \pmod{100}$.
Тада $100 \mid a^2 - a = a(a-1)$, па постоји природан број k т.д. је $a(a-1) = 100 \cdot k = 4 \cdot 25 \cdot k$.
Како је нзд$(a, a-1) = 1$ имамо 2 могућности:

$$(25 \mid a \wedge 4 \mid a-1) \vee (4 \mid a \wedge 25 \mid a-1)$$

У случају да $25 \mid a \wedge 4 \mid a-1$, двоцифрени завршетак броја a је из скупа $(25, 50, 75, 00)$, па је двоцифрени завршетак броја $a-1$ из скупа $(24, 49, 74, 99)$. Једино у случају када се a завршава са 25, $a-1$ је дјељиво са 4.
У другом случају, двоцифрени завршетак броја $a-1$ је из скупа $(25, 50, 75, 00)$, па је двоцифрени завршетак броја a из скупа $(26, 51, 76, 01)$. Једино у случају када се $a-1$ завршава са 75, односно a завршава са 76, a је дјељиво са 4.
Специјално, ако $100 \mid a$ тада се a завршава са 00 или ако $100 \mid a-1$, a се завршава са 01.
Закључујемо да су то сви природни бројеви чије су последње двије цифре из скупа $(25, 76, 00, 01)$.
□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

19

●●●●

Нека су a и b цијели бројеви .Доказати да ако $21 \mid a^2 + b^2$ онда $441 \mid a^2 + b^2$
.

Доказ. Довољно је доказати сљедеће

$$\begin{aligned} &(\mathrm{I}) \quad 3 \mid a^2 + b^2 \implies 9 \mid a^2 + b^2 \\ &(\mathrm{II}) \quad 7 \mid a^2 + b^2 \implies 49 \mid a^2 + b^2 \end{aligned}$$

Прво доказујемо (I) . Примјетимо да

$$\begin{aligned} 0^2 &\equiv 0 \pmod{3} \\ 1^2 &\equiv 1 \pmod{3} \\ 2^2 &\equiv 1 \pmod{3} \end{aligned}$$

Одатле видимо да релација $a^2 + b^2 \equiv 0 \pmod{3}$ важи ако и само ако $a \equiv 0 \pmod{3}$ и $b \equiv 0 \pmod{3}$. Дакле , a и b имају облик $3k$ односно $3l$ гдје су $l, k \in \mathbb{Z}$.Тада

$$a^2 + b^2 = 9k^2 + 9l^2 = 9(k^2 + l^2) \implies 9 \mid a^2 + b^2$$

Симе је (I) доказано . Слично доказујемо (II) . Примјетимо

$$\begin{aligned}
0^2 &\equiv 0 \pmod 7,\\
1^2 &\equiv 1 \pmod 7,\\
2^2 &\equiv 4 \pmod 7,\\
3^2 &\equiv 2 \pmod 7,\\
4^2 &\equiv 2 \pmod 7,\\
5^2 &\equiv 4 \pmod 7,\\
6^2 &\equiv 1 \pmod 7.
\end{aligned}$$

Одатле видимо да релација $a^2 + b^2 \equiv 0 \pmod 7$ важи ако и само ако $a \equiv 0 \pmod 7$ и $b \equiv 0 \pmod 7$. Дакле , a и b имају облик $7k$ односно $7l$ гдје су $l, k \in \mathbb{Z}$.Тада

$$a^2 + b^2 = 49k^2 + 49l^2 = 49(k^2 + l^2) \implies 49 \mid a^2 + b^2$$

Како $9 \mid a^2 + b^2$, $49 \mid a^2 + b^2$ и нзд$(9, 49) = 1$ слиједи да $9 \cdot 49 = 441 \mid a^2 + b^2$. $\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`http://nasport.pmf.ni.ac.rs/materijali/175/Teorija_Brojeva_Vezbe.pdf`

20

Ако је p прост број већи од 3, доказати да $24 \mid p^2 - 1$.

Доказ. Прости бројеви већи од 3 су: 5, 7, ...Када уврстимо прва два таква броја имамо $24 \mid 5^2 - 1$, односно $24 \mid 7^2 - 1$. Интуитивно нам је јасно да овај израз $p^2 - 1$ за свако p које је прост број већи од 3 садржи 24. Такође, примијетимо да важи $(p^2 - 1) = (p-1)(p+1)$.

Рекли смо да је p прост број. Он мора бити непаран (ако би био паран имао би за дјелиоце бројеве 1, 2 и самог себе а то већ значи да није прост број).

По услову задатка $p > 3$. Тако да су бројеви $p - 1$, p, $p + 1$ три узастопна природна броја, а то већ значи да је један од њих дјељив са 3. Број p не може (навели смо услов задатка). Значи или $p-1$ или $p+1$ је дјељиво бројем 3, а то уједно значи и да је производ $(p-1)(p+1)$ дјељив бројем 3. Дакле, $3 \mid p^2 - 1$.
С друге стране $p - 1$ и $p + 1$ су два узастопна парна броја, па је њихов производ дјељив са 8. Значи $8 \mid (p - 1)(p + 1) \rightarrow 8 \mid p^2 - 1$.
Како $3 \mid p^2 - 1$ и $8 \mid p^2 - 1$, тада имамо да $3 \cdot 8 \mid p^2 - 1 \rightarrow 24 \mid p^2 - 1$.
Тиме је доказ завршен.

$\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

21 ●●●●

Доказати да за сваки природан број n, $584 \mid 8^n + 8^{n+1} + 8^{n+2}$.

Доказ. У овом примјеру подразумијеваћемо да $0 \notin \mathbb{N}$.

За $n = 1$: $584 \mid 8^1 + 8^{1+1} + 8^{1+2} \rightarrow 584 \mid 584$, па трвђење важи.
За $n = 2$: $584 \mid 8^2 + 8^{2+1} + 8^{2+2} \rightarrow 584 \mid 4672$, па трвђење важи.

Можемо уочити да избором било којег природног броја n на десној страни добијамо степен броја 584. Зато нам је циљ да цијели израз $8^n + 8^{n+1} + 8^{n+2}$ представимо као садржалац броја 584. Тако да имамо:

$$8^n + 8^{n+1} + 8^{n+2} = 8^{n-1} \cdot (8 + 8^2 + 8^3) = 8^{n-1} \cdot 584.$$

□

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

22 ●●●●

Доказати да сваки сложен број n има прости фактор $p \leq \sqrt{n}$.

Доказ. Нека је p најмањи дјелилац броја n, а који је већи од 1. Самим тим p је прост број. Примијетимо да постоји $m \in \mathbb{N}$ тако да важи $n = p \cdot m$. Како је $m \geq p$ onda dobijamo da je $p \leq \sqrt{n}$. Тиме је доказ завршен.

□

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Увод у теорију бројева (скрипта), Андреј Дујела, ПМФ - Загреб

23 ●●●●

Нека је број $2^n - 1$ прост. Доказати да је тада и број n прост.

Доказ. Претпоставимо да је број n сложен. Тада се он може написати као $n = a \cdot b$, при чему је $a > 1$, $b > 1$.
Примијенимо дату трансформацију броја n, па имамо следеће:
$2^n - 1 = (2^a)^b - 1^b$.
Можемо примијетити да је број $(2^a)^b - 1^b$ дјељив бројем $(2^a) - 1$, па смо добили да није прост.
Тиме је доказ завршен.

Занимљивост: Бројеви $M_p = 2^p - 1$ гдје је p прост, зову се Мерсенови бројеви (енг. Mersenne prime). Неки Мерсенови бројеви су прости (нпр. $M_7 = 127$), а неки сложени (нпр. $M_1 = 2047 = 23 \cdot 29$). Највећи познати прости Мерсенов број је $M_{43112609}$. То је уједно и највећи познати прост број данас. Има 12978189 цифара, а открили су га Смит (Smith), Волтман (Woltman) и Куровски (Kurowski) 23.08.2008. године у склопу ГИМПС пројекта. $\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Увод у теорију бројева (скрипта), Андреј Дујела, ПМФ - Загреб

24

Доказати да за сваки природан број n постоји n узастопних сложених бројева.

Доказ. До рјешења долазимо ако уочимо правило да је $(n+1)! + j$ дјељиво са j, за $j = 2, 3, \ldots, n+1$.
Тако да за рјешење овог задатка имамо следеће бројеве:

$$\begin{gathered}(n+1)! + 2,\\ (n+1)! + 3,\\ \vdots\\ (n+1)! + n,\\ (n+1)! + n + 1.\end{gathered}$$

$\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Увод у теорију бројева (скрипта), Андреј Дујела, ПМФ - Загреб

25

(а) Ако је a цијели, а n природан број, доказати да је број $a(a^{2n}-1)$ дјељив са 6.
(б) Ако је a непаран цијели број, а n природан број, доказати да је број $a(a^{2n}-1)$ дјељив са 24.

Доказ. (а) За произвољне бројеве x, y и природан број n важи да $(x-y) \mid (x^n - y^n)$, па специјално, $(a^2-1) \mid ((a^2)^n - 1)$.
Посматрајмо израз $a(a^2-1) = a(a-1)(a+1)$. Међу три дата узастопна броја сигурно ће макар један бити паран и један дјељив са 3, па имамо дјељивост са 6. Како $6 \mid a(a^2-1)$ и $(a^2-1) \mid ((a^2)^n - 1) \Rightarrow 6 \mid a(a^{2n}-1)$.

(б) Ако је a непаран број, тада је $a = 2m+1$, за неко m. Као и у првом примјеру, доказиваћемо дјељивост $a(a^2-1)$ са 24.

$$a(a^2-1)=a(a-1)(a+1)=(2m+1)2m(2m+2)=4m(m+1)(2m+1).$$

Један од бројева $m, m+1$ биће паран па имамо дјељивост са 2. Јасна је дјељивост са 4. Остаје да покажемо да је један од бројева $m, m+1, 2m+1$ дјељив са 3.
Разликујемо случајеве:
(1) Ако је $m \equiv 0 \pmod 3$, јасно $3 \mid m(m+1)(2m+1)$
(2) Ако је $m \equiv 1 \pmod 3$, тада је $(2m+1) \equiv 0 \pmod 3$ па $3 \mid m(m+1)(2m+1)$
(3)Ако је $m \equiv 2 \pmod 3$, тада је $(m+1) \equiv 0 \pmod 3$ па $3 \mid m(m+1)(2m+1)$

Дакле, и $3 \mid a(a^2-1) \Rightarrow 24 \mid a(a^2-1) \Rightarrow 24 \mid a(a^{2n}-1)$.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

26

(а) Наћи остатак при дијељењу квадрата непарног цијелог броја са 8.

(б) Нека су $b, a_1, a_2, a_3, a_4, a_5$ цијели бројеви такви да важи

$${a_1}^2+{a_2}^2+{a_3}^2+{a_4}^2+{a_5}^2=b^2.$$

Доказати да је тада бар један од ових бројева паран.

Доказ. (а) Ако је n непаран број, тада је $n=2k+1$ за неко k, па ће

$$(2k+1)^2=4n^2+4n+1=4n(n+1)+1.$$

Пошто $4n(n+1) \equiv 0 \pmod 8$, јер $2 \mid n(n+1)$, то онда $4n(n+1)+1 \equiv 1 \pmod 8$. Дакле, n даје остатак 1 при дијељењу са 8.

(б) Лако се показује да је за сваки природан број n, n непаран $\Leftrightarrow n^2$ непаран.
Нека су $b, a_1, a_2, a_3, a_4, a_5$ цијели бројеви такви да важи:

$${a_1}^2+{a_2}^2+{a_3}^2+{a_4}^2+{a_5}^2=b^2.$$

Разматрамо двије могућности:
1. b је паран број. Јасно, важи тврђење.
2. b је непаран број $\Rightarrow b^2$ непаран број. Тада према а) важи $b^2 \equiv 1 \pmod 8$. Ако би сви бројеви $a_i, i=1\dots5$ били непарни важило би да је ${a_i}^2 \equiv 1 \pmod 8$, тј.

$${a_1}^2+{a_2}^2+{a_3}^2+{a_4}^2+{a_5}^2 \equiv 5 \pmod 8$$

што је немогуће јер је $b^2 \equiv 1 \pmod 8$.
Дакле, сигурно је барем један од $a_i, i=1\dots5$ паран број.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

27

Доказати да $11 \cdot 31 \cdot 61 \mid 20^{15} - 1$.

Доказ. Довољно је показати, да сваки од бројева 11, 31 и 61 дијели $20^{15} - 1$. Имамо да је

$$(1) \qquad 2^5 \equiv -1 \pmod{11}$$

и

$$10 \equiv -1 \pmod{11}.$$

Такође, важи да је

$$(2) \qquad 10^5 \equiv -1 \pmod{11}$$

па из (1) и (2) слиједи да је

$$20^5 \equiv 1 \pmod{11}$$

што даље повлачи да је

$$20^{15} \equiv 1 \pmod{11}$$

па слиједи да $11 \mid 20^{15} - 1$.
Сада треба показати да 31 дијели $20^{15} - 1$. Имамо да је

$$20 \equiv -11 \pmod{31} \implies 20^2 \equiv 121 \equiv -3 \pmod{31}.$$

Даље, слиједи да је

$$20^3 \equiv (-11)(-3) = 33 \equiv 2 \pmod{31} \implies 20^{15} \equiv 2^5 \equiv 1 \pmod{31}.$$

Показали смо да 31 дијели $20^{15} - 1$, па нам остаје још да покажемо да 61 дијели $20^{15} - 1$. У овом случају имамо да је

$$3^4 \equiv 20 \pmod{61} \implies 20^{15} \equiv 3^{60} \equiv 1 \pmod{61}.$$

У овом последњем кораку искористили смо Фермаову теорему, чиме смо доказали да број 61 дијели $20^{15} - 1$, па отуда слиједи да број $11 \cdot 31 \cdot 61$ дијели $20^{15} - 1$. $\square$

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

28

Доказати да за сваки позитиван цијели број m и $a > 1$ важи

$$\text{нзд}(\tfrac{a^m-1}{a-1}, a-1) = \text{нзд}(a-1, m).$$

Доказ. Нека је $d = \text{нзд}(\frac{a^m-1}{a-1}, a-1)$. Даље важи да је

$$(1) \qquad \tfrac{a^m-1}{a-1} = (a^{m-1}-1) + (a^{m-2}-1) + \cdots + (a-1) + m.$$

С обзиром на чињеницу да $a-1 \mid a^k - 1$ за $k = 0, 1, 2, ...$, слиједи да $d \mid m$. Даље, ако бројеви $a-1$ и m имају заједничког дјелиоца $D > d$, тада слиједи да имамо, из (1), релацију $D \mid \frac{a^m-1}{a-1}$, и слиједи да бројеви $\frac{a^m-1}{a-1}$ и $a-1$ имају заједничког дјелиоца $D > d$, што није могуће. Из овога слиједи да је d највећи заједнички дјелилац за бројеве $a-1$ и m што је требало и да докажемо. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

29

Доказати да за сваки позитивни цијели број n важи

$$(2^n-1)^2 \mid 2^{(2^n-1)n} - 1.$$

Доказ. Рјешавање овог задатка ћемо прво свести на рјешавање општег случаја, а затим ћемо се вратити на конкретни проблем.
За почетак, докажимо да за сваки позитивни цијели број m важи

$$(1) \qquad m^2 \mid (m+1)^m - 1.$$

Користећи биномну формулу добијамо да је

$$(1+m)^m = 1 + \binom{m}{1}m + \binom{m}{2}m^2 + \cdots + \binom{m}{m}m^m.$$

На основу последње једнакости, слиједи да за свако $m > 1$, сви сабирци, почевши од трећег, садрже m са експонентом ≥ 2. Други сабирак једнак је $\binom{m}{1}m = m^2$, па слиједи да

$$m^2 \mid (m+1)^m - 1$$

што је и требало да докажемо у помоћном случају. Сада, вратимо се рјешавању почетног проблема.
Ако погледамо лијеву страну израза (1) и лијеву страну нашег проблема, можемо уочити, у овом случају, да је $m = 2^n - 1$, па из претходне једнакости и израза (1) добијамо да је

$$(2^n-1)^2 \mid (2^n-1+1)^{2^n-1} - 1 \implies (2^n-1)^2 \mid 2^{(2^n-1)n} - 1.$$

☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

30

Доказати да ако за неке цијеле бројеве a, b, c важи да $9 \mid a^3 + b^3 + c^3$, тада је барем један од бројева a, b, c дјељив са 3.

Доказ. Кубови цијелих бројева који нису дјељиви са 3 дају остатак 1 или -1 при дијељењу са 9. Дакле, ако међу бројевима a, b, c не постоји број који је дјељив са 3, тада број $a^3+b^3+c^3$ при дијељењу са 9 даје остатак $\pm 1 \pm 1 \pm 1$ који није дјељив са 9 за било коју комбинацију знакова + и −. Дакле, слиједи да ако $9 \mid a^3 + b^3 + c^3$, тада и $3 \mid abc$ што је и требало да докажемо. □

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

31

За сваки број $n = 0, 1, 2, \ldots, 1999$ број A_n дефинисан је са

$$A_n = 2^{3n} + 3^{6n+2} + 5^{6n+2}.$$

Наћи нзд$(A_0, \ldots, A_{1999})$.

Доказ. Како је $A_0 = 2^0+3^2+5^2 = 35$ то онда нзд$(A_0, \ldots, A_{1999})$ мора бити неки од дјелилаца броја 35. Са друге стране, како је $A_1 = 2^3 + 3^8 + 5^8 \equiv 2^3 + 3^8 \equiv 4 \pmod 5$, закључујемо да A_1 није дјељив са 5, па самим тим ни нзд$(A_0, \ldots, A_{1999})$.

Дакле, нзд$(A_0, \ldots, A_{1999})$ је или 7 или 1. Покажимо да је сваки од $A_0, \ldots, A_{1999}$ дјељив са 7. Како важе следеће конгруенције:

$$2^{3n} \equiv 8^n \equiv 1 \pmod 7$$

$$3^{6n} \equiv 729^n \equiv 1 \pmod 7$$

$$5^{6n} \equiv (5^2 \cdot 5^2 \cdot 5^2)^n \equiv (4 \cdot 4 \cdot 4)^n \equiv 1 \pmod 7$$

$\Rightarrow An \equiv 1 + 3^2 + 5^2 \equiv 0 \pmod 7$ за свако $n = 0, 1, 2, \ldots, 1999 \Rightarrow$ нзд$(A_0, \ldots, A_{1999}) = 7$. □

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/` (JBMO 1999)

32

Доказати да је нзд$(a_n, b_n) = 1$, за сваки цијели број $n \geq 1$, ако су a_n и b_n цијели бројеви тако да је

$$a_n + b_n\sqrt{2} = (1 + \sqrt{2})^n$$

за сваки цијели број $n \geq 1$.

Доказ. У овом случају доказ ћемо извести помоћу индукције. За базни случај, када је $n = 1$, имамо да је $a_1 = 1, b_1 = 1$ па слиједи да је нзд$(a_n, b_n) = 1$.
За индуктивну хипотезу, претпоставимо да важи за $n = k$. Тада је $a_k + b_k\sqrt{2} = (1+\sqrt{2})^k$, тј. важи да је нзд$(a_k, b_k) = 1$. Сада, треба да докажемо да важи за $n = k+1$. Слиједи да је

$$\begin{aligned} a_{k+1} + b_{k+1}\sqrt{2} &= (1+\sqrt{2})^{k+1} \\ &= (1+\sqrt{2})(1+\sqrt{2})^k \\ &= (1+\sqrt{2})(a_k + b_k\sqrt{2}) \\ &= (a_k + 2b_k) + \sqrt{2}(a_k + b_k). \end{aligned}$$

Из последње једнакости слиједи да је $a_{k+1} = a_k + 2b_k$, а $b_{k+1} = a_k + b_k$. Сада нам још остаје да докажемо да је нзд$(a_{k+1}, b_{k+1}) = 1$. Користећи Еуклидов алгоритам добијамо да је

$$\text{нзд}(a_k + 2b_k, a_k + b_k) = \text{нзд}(b_k, a_k + b_k) = \text{нзд}(b_k, a_k) = 1.$$

Дакле, на основу индукције показали смо да $n = k \implies n = k+1$. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://s3.amazonaws.com/aops-cdn.artofproblemsolving.com/resources/articles/olympiad-number-`
`pdf`

33

(а) Доказати да $(n+1) \mid \binom{2n}{n}$, за све $n \in \mathbb{N}$.
(б) За све $k \in \mathbb{Z}$, наћи најмањи природан број C_k такав да

$$(n+k+1) \mid C_k\binom{2n}{n+k},$$

за све $n \geq k$.

Доказ. (а) Имамо да важи:

$$\frac{1}{n+1}\binom{2n}{n} = \frac{(2n)!}{(n+1)!n!} = \frac{1}{n} = \binom{2n}{n-1},$$

одакле добијамо

$$n\binom{2n}{n} = (n+1)\binom{2n}{n-1}.$$

Како је нзд$(n, n+1) = 1$, то слиједи да $(n+1) \mid \binom{2n}{n}$.

(б) Из претходног слиједи да је $C_0 = 1$, па зато претпоставимо да је $k > 0$. Ако је $n = k$ тада је $\binom{2n}{n+k} = 1$, што значи да мора бити $C_k \geq 2k+1$.

Покушаћемо да покажемо да је баш $C_k = 2k+1$, тј. да важи

$$(n+k+1) \mid (2k+1)\binom{2n}{n+k},$$

за све $n \geq k$. Како је

$$(2k+1)\binom{2n}{n+k} = [(n+k+1)-(n-k)]\binom{2n}{n+k},$$

довољно је показати да

$$(n+k+1) \mid (n-k)\binom{2n}{n+k}.$$

Међутим, на аналоган начин као под (а), добијамо:

$$(n-k)\binom{2n}{n+k} = \frac{(2n)!}{(n+k)!(n-k-1)!} = (n+k+1)\binom{2n}{n-k-1},$$

одакле слиједи жељени закључак.

$\square$

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

34

Нека су $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$ природни бројеви такви да је нзд$(a_i, b_i) = 1$, за све $i, 1 \leq i \leq k$. Нека је m најмањи заједнички садржалац бројева $b_1, b_2, \ldots, b_k$, а $c_i = a_i \cdot \frac{m}{b_i}, 1 \leq i \leq k$. Доказати:

$$\text{нзд}(a_1, a_2, \ldots, a_k) = \text{нзд}(c_1, c_2, \ldots, c_k).$$

Доказ. Нека је p прост број који дијели бар један од датих бројева $a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_k$. Нека су α_i, β_i редом највиши степени којима p дијели a_i, односно b_i. Тада је највиши степен којим p дијели m једнак $\mu = \max_j \beta_j$, док је највиши степен којим p дијели c_i једнак $\gamma_i = \alpha_i + \mu - \beta_i$. Имајући у виду произвољност простог фактора p, тврђење задатка је еквивалентно једнакости

$$\min_i \alpha_i = \min_i(\alpha_i + \mu - \beta_i) = \mu + \min_i(\alpha_i - \beta_i). \tag{1.2}$$

При томе, због нзд$(a_i, b_i) = 1$ важи $\alpha_i \neq 0 \implies \beta_i = 0$.

Ради краћег записа дефинишемо $\delta_i = \alpha_i - \beta_i$. С обзиром на уочени однос експонената α_i и β_i важи:

$$\delta_i = \begin{cases} -\beta_i, \alpha_i = 0 \\ \alpha_i, \alpha_i \neq 0. \end{cases}$$

Сада, разликујемо два случаја:

- $\exists i_0, \alpha_{i_0} \implies \min_i \alpha_i = 0$
  С друге стране, $\min_i \delta_i = -\max_i \beta_i = -\mu$, па тада и десна страна у (1.2) има вриједност 0.

- $\alpha_i > 0, \forall\, 1 \leq i \leq k$.
  Али, тада је $\beta_i = 0, \forall\, 1 \leq i \leq k$, па је $\mu = 0$ и $\delta_i = \alpha_i, \forall\, 1 \leq i \leq k$.

Видимо да је једнакост (1.2) тачна у оба случаја, па је њен доказ комплетан.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

35

Нека су p и q природни бројеви такви да је

$$\frac{p}{q} = 1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{1318} + \frac{1}{1319}.$$

Доказати да $p \mid 1979$.

Доказ. Уочимо на почетку да је број 1979 прост. Додајмо и одузмимо негативне чланове два пута

$$\begin{aligned} & 1 - \frac{1}{2} + \frac{1}{3} - \cdots - \frac{1}{1318} + \frac{1}{1319} = \\ & = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots + \frac{1}{1318} + \frac{1}{1319} - 2(\frac{1}{2} + \frac{1}{4} + \cdots + \frac{1}{1318}) = \\ & = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} \cdots + \frac{1}{1318} + \frac{1}{1319} - (1 + \frac{1}{2} + \cdots + \frac{1}{659}) = \\ & = \frac{1}{660} + \frac{1}{661} + \cdots + \frac{1}{1319} \end{aligned}$$

и примјетимо да $660 + 1319 = 1979$, $661 + 1318 = 1979$ .... Сабирајући парове први-посљедњи, други-претпосљедњи ... добијамо

$$1979 \cdot (\frac{1}{660 \cdot 1319} + \frac{1}{661 \cdot 1318} + \ldots).$$

Сабирајући елементе у загради добијамо рационалан број чији је именилац $660 \cdot 661 \cdot \cdots \cdot 1319$. Како је именилац настао множењем бројева мањих од 1979 онда важи $1979 \nmid (660 \cdot 661 \cdot \cdots \cdot 1319)$ (1979 је прост). Дакле, закључујемо $1979 \mid p$.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://imomath.com/srb/`

36

Ако су a, b, m, n природни бројеви, нзд$(a, b) = 1$ і $a > 1$, доказати импликацију

$$a^m + b^m \mid a^n + b^n \implies m \mid n.$$

Доказ. Претпоставимо да $m \nmid n$. Tada je $n = qm + r$, $0 < m < r$.

Напомена: $a - b \mid a^n - b^n$ за сваки природан број n и $a + b \mid a^n + b^n$, за сваки непаран број n.

Могућа су следећа два случаја:
1.случај: q је непаран;

$$\begin{aligned} a^n + b^n = a^{qm+r} + b^{qm+r} & \\ = \quad & a^{qm}a^r + b^{qm}b^r \\ = \quad & a^{qm}a^r + b^{qm}a^r + b^{qm}b^r - b^{qm}a^r \\ = \quad & ((a^m)^q + (b^m)^q)a^r + b^{mq}(b^r - a^r) \end{aligned}$$

$a^m + b^m \mid a^n + b^n$, по претпоставци,
$a^m + b^m \mid a^{mq} + b^{mq}$, јер је q непаран број
нзд$(b^{qm}, a^m + b^m) = 1$, јер је нзд$(a, b) = 1$
$|b^r - a^r| < |a^r + b^r| < a^m + b^m$, јер је r<m. Контрадикција.

2.случај: q је паран;

$$\begin{aligned} a^n + b^n = a^{ms}a^{m+r} + b^{ms}b^{m+r} & \\ = \quad & a^{ms}a^{m+r} + b^{ms}a^{m+r} + b^{ms}b^{m+r} \\ + \quad & a^m b^{ms+r} - b^{ms}a^{m+r} - a^m b^{ms+r} \\ = \quad & a^{m+r}((a^m)^s + (b^m)^s) + b^{ms+r}(b^m + a^m) \\ - \quad & a^m b^{ms}(a^r + b^r) \end{aligned}$$

Пошто је нзд$(a^m + b^m, a^m b^{ms}) = 1$ jer је нзд$(a, b) = 1$ сличним резоновањем као у случају под 1. долазимо до контрадикције.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

37

● ● ● ●

Доказати да постоји пребројиво много цијелих бројева n таквих да важи $n \mid 2^n + 2$.

Доказ. Желимо да докажемо да ако је n паран број, такав да важи $n \mid 2^n + 2$ и $n - 1 \mid 2^n + 1$ (на примјер, за $n = 2$), onda za broj $n_1 = 2^n + 2$ такође важи $n_1 \mid 2^{n_1} + 2$ и $n_1 - 1 \mid 2^{n_1} + 1$. Zapravo, ако $n \mid 2^n + 2$ и n је паран, онда је $2^n + 2 = nk$, гдје је k непаран број,па је:

$$2^{n+1} \mid 2^{nk} + 1 = 2^{2^n+2} + 1$$

За $n_1 = 2^n + 2$ имамо:

$$n_1 - 1 = 2^n + 1 \mid 2^{n_1} + 1$$

Добијамо да $n - 1 \mid 2^n + 1$, одакле слиједи $2^n + 1 = (n-1)m$, гдје је m непаран.
Даље,имамо да важи $2^{n-1} + 1 \mid 2^{(n-1)m} + 1 = 2^{2^n+1} + 1$, одакле слиједи $2^n + 2 \mid 2^{2^n+2} + 2$, или $n_1 \mid 2^{n_1} + 2$.
Како је $n_1 = 2^n + 2 > n$, то значи да постоји пребројиво много парних бројева n, који задовољавају наше услове.

Почевши од $n = 2$, успјешно добијамо $2, 6, 66, 2^{66} + 2, \ldots$.

☐

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

38

Нека су a и b природни бројеви,такви да је $a < b$. Доказати да се међу произвољних b узастопних природних бројева могу наћи два чији је производ дјељив са ab.

Доказ. Нека је $x_1, x_2, \ldots, x_b$ скуп од b узастопних природних бројева. Тада се међу њима налази број x_i дјељив са b и због $a < b$, број x_j дјељив са a. Ако је $i \neq j$ тада је производ $x_i x_j$ дјељив са ab.

Претпоставимо сада да је $i = j$. Означимо са d највећи заједнички дјелилац бројева a и b, а са s њихов најмањи заједнички садржалац. Тада је $ds = ab$ и $s \mid x_i$.

Докажимо да бар један од бројева $x_i + d$ и $x_i - d$ (који су дјељиви са d) припада скупу $x_1, x_2, \ldots, x_b$. Ако то не би био случај, било би $x_i + d > x_b$ и $x_i - d < x_1$, одакле би слиједило $2d > x_b - x_1 + 1 = b$. Међутим, због $d \mid b$, то би значило да је $d = b > a$, па не би могло да важи $d \mid a$, што је супротно дефиницији броја d.

Ако $x_i + d \in x_1, x_2, \ldots, x_b$, тада је производ $x_i(x_i + d)$ дјељив са $ds = ab$, а у супротном је $x_i(x_i - d)$ дјељиво са ab.

☐

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

39

Нека су a и b природни бројеви за које је нзд$(a, b) = 10$ и нзд$(a, b+2) = 12$. Израчунати нзд$(a, 2b)$ + нзд$(a, 3b)$.

Доказ. Како је нзд$(a, b) = 10$ закључујемо да је 5 највећи непаран заједнички дјелилац за a и b, па је 5 највећи непаран заједнички дјелилац за a и $2b$.
Да би израчунали нзд$(a, 2b)$ треба утврдити највећи степен двојке који дијели a и $2b$.

Из нзд$(a, b) = 10$ закључујемо да су a и b дјељиви са 2, али нијесу оба са 4. Са друге стране, из нзд$(a, b+2) = 12$ закључујемо да је a дјељив са 4, па b није дјељив са 4.
Дакле, a и $2b$ су дјељиви са 4, али $2b$ није дјељив са 8, па је:

$$\text{нзд}(a, 2b) = 4 \cdot 5 = 20$$

Слично, из нзд$(a, b) = 10$ закљључујемо да a и b не могу истовремено бити дјељиви са 3, а из нзд$(a, b+2) = 12$ да је a дјељив са 3 и b није дјељив са 3.
Дакле, a и $3b$ су дјељиви са 3, али $3b$ није дјељив са 9, па је:

$$\text{нзд}(a, 3b) = 3 \cdot 10 = 30$$

Коначно,

$$\text{нзд}(a, 2b) + \text{нзд}(a, 3b) = 50$$

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

40

(1) Ако је $a = bq + r$, онда нзд$(a, b) =$ нзд(b, r).
(2) Последњи остатак r_n који је различит од нуле у Еуклидовом алгоритму представља највећи заједнички дјелилац бројева a и b.

Доказ. (1) Нека је d заједнички дјелилац бројева a i b тј. $d \mid a$ и $d \mid b$.
$a = bq + r \implies r = a - bq \implies d \mid r.$
Слиједи да је d заједнички дјелилац бројева b и r.
Ако је c заједнички дјелилац бројева b и r тј. $c \mid b$ и $c \mid r$.
$a = bq + r \implies c|a$, па је c заједнички дјелилац бројева a и b.
Видимо да се скуп заједничких дјелилаца бројева a и b поклапа са скупом заједничких дјелилаца бројева b и r па су међусобно једнаки и њихови елементи $\implies$ нзд$(a, b) =$ нзд(b, r).
(2) На основу (1) важе следеће једнакости:
нзд$(a, b) =$ нзд$(b, r_1) =$ нзд$(r_1, r_2) = ... =$ нзд(r_{n-1}, r_n)
Пошто $r_n | r_{n-1} \implies$ нзд$(r_{n-1}, r_n) = r_n \implies$ нзд$(a, b) = r_n$

□

(**Милена Јововић 1/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

41

Доказати да:
а) за свако $n \in \mathbb{N}$ $3^n \mid \underbrace{aa\ldots a}_{3^n}$ за ма коју цифру a
б) за свако $n \in \mathbb{N}$ $133 \mid 11^{n+2} + 12^{2n+1}$

Доказ. а) Доказујемо индукцијом по n.
$n = 1 \implies 3 \mid aaa$
Претпоставимо да тврђење важи за неко $n \in \mathbb{N}$: $3^n \mid \underbrace{aa\ldots a}3^n$
Радимо за $n+1$:

$$\begin{aligned}\underbrace{aa\ldots a}_{3^{n+1}} &= \underbrace{aa\ldots a}_{3^n} \cdot \underbrace{aa\ldots a}_{3^n} \cdot \underbrace{aa\ldots a}_{3^n} = \\ &= 10^{2\cdot 3^n}\underbrace{aa\ldots a}_{3^n} + 10^{3^n}\underbrace{aa\ldots a}_{3^n} + \underbrace{aa\ldots a}_{3^n} = \\ &= (1\underbrace{00\ldots 0}_{3^n-1}1\underbrace{00\ldots 0}_{3^n-1}1)\underbrace{aa\ldots a}_{3^n}\end{aligned}$$

Како $3 \mid 1\underbrace{00\ldots 0}_{3^n-1}1\underbrace{00\ldots 0}_{3^n-1}1$ и из индукцијске претпоставке $3^n \mid \underbrace{aa\ldots a}_{3^n}$, закључујемо да $3^{n+1} \mid \underbrace{aa\ldots a}_{3^{n+1}}$.

б) Тврђење доказујемо индукцијом по n.
$n = 1 \implies 133 \mid 11^3 + 12^3 \implies 133 \mid 1331 + 1728\ (T)$
$1331 + 1728 = 3059 = 23 \cdot 133$
Претпоставимо да тврђење важи за неко $n \in \mathbb{N} : 133 \mid 11^{n+2} + 12^{2n+1}$
За $n+1$:

$$\begin{aligned}11^{n+1+2} + 12^{2(n+1)+1} &= 11^{n+3} + 12^{2n+3} = \\ &= 11 \cdot 11^{n+2} + 12^2 \cdot 12^{2n+1} = \\ &= 11 \cdot 11^{n+2} + 144 \cdot 12^{2n+1} = \\ &= 11(11^{n+2} + 12^{2n+1}) + 133 \cdot 12^{2n+1}\end{aligned}$$

Први сабирак је дјељив са 133 на основу индукцијске претпоставке.
Слиједи да за свако $n \in \mathbb{N}$ $133 \mid 11^{n+2} + 12^{2n+1}$.

□

(**Милена Јовoвић 1/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

42

Нека је n природан број. Доказати да је број

$$(n+1)(n+2)\cdot\ldots\cdot(n+n)$$

дјељив са 2^n, а није дјељив са 2^{n+1} .

Доказ. Доказаћемо индукцијом да се број 2 појављује тачно n пута као чинилац броја $(n+1)(n+2)\cdot\ldots\cdot(n+n)$.
За $n = 1$ имамо $1 + 1 = 2 = 2^1$
Претпоставимо да за неко $n \in \mathbb{N}$, број 2 у производу $(n+1)(n+2)\cdot\ldots\cdot(n+n)$ се појављује

као чинилац тачно n пута.
Радимо за $n+1$:

$$\begin{aligned}&(n+1+1)(n+1+2)\cdot\ldots\cdot(n+1+n-1)(n+1+n)(n+1+n+1) =\\ &= (n+2)(n+3)\cdot\ldots\cdot(n+n)(2n+1)(2n+2) =\\ &= 2(n+1)(n+2)(n+3)\cdot\ldots\cdot(n+n)(2n+1)\end{aligned}$$

Према индукцијској претпоставци, број 2 се појављује тачно n пута као чинилац у производу $(n+1)(n+2)\cdot\ldots\cdot(n+n)$, а чинилац $2n+1$ је непаран па он није дјељив са 2. Из последњег израза можемо закључити да се у производу $(n+1+1)(n+1+2)\cdot\ldots\cdot(n+1+n-1)(n+1+n)(n+1+n+1)$ број 2 као чинилац појављује тачно $n+1$ пута. ☐

(**Милена Јововић 1/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

43

Одредити нзд$(75,\ 625,\ 1050,\ 1400)$.

Доказ.

$$\begin{aligned}\text{нзд}(75,625,1050,1400) &= \text{нзд}(\text{нзд}(75,\ 625,\ 1050),1400) =\\ &= \text{нзд}(\text{нзд}(\text{нзд}(75,\ 625),1050),1400)\end{aligned}$$

Дакле, прво тражимо нзд$(75,625)$

$$\begin{aligned}625 &= 8\cdot 75+25\\ 75 &= 3\cdot 25\\ \Longrightarrow\ \text{нзд}(75,\ 625) &= 25\end{aligned}$$

нзд$(25,\ 1050) = ?$

$$\begin{aligned}25 &= 0\cdot 1050+25\\ 1050 &= 25\cdot 42\\ \Longrightarrow\ \text{нзд}(25,\ 1050) &= 25\end{aligned}$$

нзд$(25,\ 1400) = ?$
Аналогним поступком, нзд$(25,\ 1400) = 25$.
Дакле, нзд$(75,\ 625,\ 1050,\ 1400) = 25$

☐

(**Милена Јововић 1/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

44

Највећи заједнички дјелилац два природна броја је 24, а најмањи заједнички садржалац истих бројева је 504. Ниједан од тих бројева није дјељив са оним другим бројем. Који су то бројеви?

Доказ. Нека су та два броја a и b.
$\text{нзд}(a, b) = 24$
$\text{нзс}(a, b) = 504$
$a = 24x, \;\; b = 24y$
Користећи лему $\text{нзд}(a, b) \cdot \text{нзс}(a, b) = ab$ имамо

$$24 \cdot 504 = 24x \cdot 24y$$
$$\implies \quad xy = 21 \implies \quad x \in \{1, 3, 7, 21\}$$

За $x = 1$ добијамо $a|b$, а за $x = 21$ добијамо $b|a$ што не одговара услову задатка. Једине могућности су $(x, y) = (3, 7)$ и $(x, y) = (7, 3)$ одакле слиједи да су тражени бројеви 72 и 168. □

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/zadacinatj1.pdf`

45

Наћи пет последњих цифара броја 5^{1997}.

Доказ.

$$\begin{aligned}
5^{1997} &= 5^{249\cdot 8+5} = 5^5[(5^{249})^8 - 1 + 1] = \\
&= 5^5[(5^{249})^8 - (5^{249})^6 + (5^{249})^6 - (5^{249})^4 + (5^{249})^4 - (5^{249})^2 + (5^{249})^2 - 1 + 1] = \\
&= 5^5[((5^{249})^6 + (5^{249})^2 + (5^{249})^4 + 1)((5^{249})^2 - 1) + 1] = \\
&= 5^5[((5^{249})^2 + 1)((5^{249})^4 + 1)((5^{249})^2 - 1) + 1] = \\
&= 5^5[(5^{249} - 1)(5^{249} + 1)(5^{498} + 1)(5^{996} + 1) + 1]
\end{aligned}$$

Први чинилац у средњој загради дјељив је са 4, а остали са 2. Тада је њихов производ са 5^5 дјељив са $5^5 \cdot 2^2 \cdot 2 \cdot 2 \cdot 2 = 10^5$, тј. завршаваће се са 5 нула. Дакле, последњих пет цифара броја 5^{1997} су исте као и броја 5^5, тј. 03125. □

(**Милена Јововић 1/19 Б**) задатак преузет са
"Бројеви, нестандардни задаци"Ратко Тошић, Драгољуб Милошевић

46

Одредити три последње цифре броја 7^{9999}.

Доказ. Примјетимо да је $7^4 = 2401$. Зато је

$$7^{4n} = 2401^n = (1 + 2400)^n = 1 + n \cdot 2400 + \binom{n}{2} 2400^n + \ldots$$

гдје се сви чланови у овом развоју бинома, почев од трећег, завршавају са бар 4 нуле и не утичу на последње 3 цифре броја 7^{4n}. Три последње цифре одређене су са

$$1 + n \cdot 2400 = 24n \cdot 100 + 1$$

.

За $n = 2500$ број $24n$ завршава се нулом, тј. број $7^{4n} = 7^{10000}$ завршава се са 001. Дакле, $7^{10000} = 1000k + 1$ за неки природан број k, тј. $7^{10000} = 1000(k-1) + 1001$. Дијелећи са 7 добијамо да је

$$7^{9999} = \frac{1000(k-1)}{7} + 143$$

.

Како десна страна мора бити цијели број, $7 \mid 1000(k-1)$.
Међутим, $7 \nmid 1000$, па мора $7 \mid k-1$, тј. за неки природан број p је $7^{9999} = 1000p + 143$. Како се број $1000p$ завршава са 000, слиједи да се број 7^{9999} завршава са 143. ☐

(**Милена Јововић 1/19 Б**) задатак преузет са
"Бројеви, нестандардни задаци"Ратко Тошић, Драгољуб Милошевић

47

Нека је n позитивни цијели број. Показати да било који број већи од $\frac{n^4}{16}$ се може записати на највише један начин као производ два од свих својих дјелиоца чија разлика није већа од n.

Доказ. Претпоставимо супротно, тј. да постоје $a > c \geq d > b$, $a - b \leq n$ и $ab = cd > \frac{n^4}{16}$.
Нека је нзд$(a, c) = p$. Можемо наћи позитивне цијеле бројеве p, q, r, s такве да $a = pq$, $c = pr$, $b = rs$, $d = qs$.
Како је
$a > c$ тј. $pq > pr \implies q > r$
$a > d$ тј. $pq > qs \implies p > s$
па

$$n \geq a - b = pq - rs \geq (s+1)(r+1) - rs = r + s + 1 \geq 2\sqrt{b} + 1$$

јер $r + s \geq 2\sqrt{rs} = 2\sqrt{b}$
Према томе,

$$\begin{aligned} 2\sqrt{b} + 1 &\leq n \\ 2\sqrt{b} &\leq n - 1 \\ b &\leq (\frac{n-1}{2})^2 < \frac{n^2}{4} \end{aligned}$$

Слично,

$$2\sqrt{b}+1 \leq a-b$$
$$a \leq (\frac{n-1}{2})^2 + n = (\frac{n+1}{2})^2$$

Па,

$$ab \leq (\frac{n^2-1}{4})^2 < \frac{n^4}{16}$$

што је контрадикција са претпоставком.

$\square$

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

48

За природан број кажемо да је палинром (или да је симетричан)ако је једнак броју записаном истим цифрама у обрнутом редоследу.(На примјер, бројеви 121,1 331,56 788 765,45 699 654 су палиндроми.) Наћи највећи заједнички дјелилац свих десетоцифрених палиндрома.

Доказ. Сваки десетоцифрени палиндром је дјељив са 11. Поред тога како је

$$9999999999 = 11 \cdot 909090909$$

и

$$1000000001 = 11 \cdot 90909091,$$

а 90909091 и 909090909 су узајамно прости бројеви $(90909091 \cdot 10 - 909090909 = 1)$, слиједи да је највећи заједнички дјелилац 11. $\square$

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

49

Дати су полиноми
$p_1(x) = 3x^3 - 2x^2 + x + 2$ и
$p_2(x) = x^2 - x + 1$
Одредити полиноме $q_1(x)$ и $q_2(x)$ тако да је
$p_1(x)q_2(x) + p_2(x)q_1(x) = 1$

Доказ. Еуклидов алгоритам за полиноме $p_1(x)$ и $p_2(x)$ дат је следећим једнакостима:

$$3x^3 - 2x^2 + x + 2 = (3x+1)(x^2 - x + 1) + (-x+1),$$
$$x^2 - x + 1 = (-x+1)(-x) + 1.$$

Највећи заједнички дјелилац полинома $p_1(x)$ и $p_2(x)$ је 1, па су они узајамно прости. Стога,задату једначину можемо ријешити примјеном Еуклидовог алгоритма из кога добијамо да је
$= x^2 - x + 1 + x(-x+1) =$
$= x^2 - x + 1 + x[(3x^3 - 2x^2 + x + 2) - (3x+1)(x^2 - x + 1) + (-x+1)] =$
$(3x^3 - 2x^2 + x + 2) \cdot x + (x^2 - x + 1) \cdot (-3x^2 - x + 1)$, па је
$q_1(x) = x$
$q_2(x) = -3x^2 - x + 1$ □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://operator.pmf.ni.ac.rs/www/pmf/publikacije/Mii/2008-2009/broj%201%20sveska%201-2/mii1-4.pdf`

50

Постоје ли природни бројеви a, b, c и d такви да важи $a^2 + b^2 = 5cd$ и $c^2 + d^2 = 5ab$?

Доказ. Без смањења општости претпоставимо да је нзд$(a, b, c, d) = 1$. Сабирањем датих једначина и одузимајући $2(ab + cd)$ са обије стране добијамо:

$$a^2 + b^2 + c^2 + d^2 - 2(ab + cd) = 3(cd + ab) \Rightarrow (a-b)^2 + (c-d)^2 = 3(ab + cd)$$

Како је десна страна једнакости дјељива са 3 и лијева страна мора бити дјељива, па $3 \mid (a-b)^2$ и $3 \mid (c-d)^2$, а одавде пошто је 3 прост број важи да $3 \mid (a-b)$ и $3 \mid (c-d)$ односно 3 дијели сваки од бројева a, b, c и d, што је контрадикција са полазном претпоставком.

□

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

51

За које природне бројеве n се може скратити разломак
а) $\frac{8n+71}{5n+46}$ б) $\frac{4n-7}{2n+3}$ в) $\frac{n+7}{2n+3}$.

Доказ. а) Нека су бројилац $a = 8n + 71$ и именилац $b = 5n + 46$ дјељиви са d. Тада d дијели сваку линеарну комбинацију бројева а и b, па и $5a - 8b = -13$. Ово значи да $13 \mid 5 \cdot (8n + 71)$ и $13 \mid 8 \cdot (5n + 46)$. Како је 13 узајамно прост број са 5 и са 8, то значи да $13 \mid 8n + 71$ и $13 \mid 5n + 46$. Одавде закључујемо да се разломак може кратити са 13. Сада је довољно наћи

вриједности n за које је a (или b) дјељиво са 13.
Због **алгоритма дијељења** јасно је да је да 13 дијели $5n+46$ акко дијели $5n+20$, а одавде слиједи да 13 дијели $n+4$. Претходним закључцима, долазимо до тога да је разломак $\frac{8n+71}{5n+46}$ могуће скратити акко је n природан број који при дијељењу са 13 даје остатак 9.
б) Рјешење: Разломак се може скратити акко је n природан број који при дијељењу са 13 даје остатак 5.
в) Рјешење: Разломак се може скратити акко је n природан број који при дијељењу са 11 даје остатак 4. □

(**Лазар Шћекић 6/19 Б**) задатак из збирке задатака
Задачи по теории чисел: учебное пособие / Т. В. Азовская, В. В. Севостьянова. — Самара: Издательство «Самарский университет», 2009. — 72 с.

52
●●●●

Доказати да је $1^{2019}+2^{2019}+...+2019^{2019}$ дјељиво са $1+2+...+2019$.

Доказ. Доказаћемо да за произвољан непаран број $n=2m-1$, сума $S=1^n+2^n+...+n^n$ дјељива са $1+2+...+n=\frac{n\cdot(n+1)}{2}=\frac{n\cdot 2m}{2}=n\cdot m$.
Лако је наћи линеарну комбинацију бројева n и m која је једнака 1:

$$-1\cdot(2m-1)+2\cdot m=1,$$

па закључујемо да су они узајамно прости. Зато је довољно доказати да је S дјељиво са m и са n.
$S=(1^n+n^n)+(2^n+(n-1)^n)+...+((m-1)^n+(m+1)^n)+m^n$. Сума у сваком сабирку, осим посљедњег, је дјељива са $n+1=2m$. Закључујемо да је S дјељиво са m.
С друге стране, $S=(1^n+(n-1)^n)+(2^n+(n-2)^n)+...+((m-1)^n+m^n)+n^n$, па слиједи да је S дјељиво са n. Тиме смо доказали уопштење задатка, па важи да је $1^{2019}+2^{2019}+...+2019^{2019}$ дјељиво са $1+2+...+2019$. □

(**Шћекић Лазар 6/19 Б**) задатак са интернета
Олимпиадные задачи «Теория чисел»

53
●●●●

Са колико нула се завршава број $99^{99}+1$?

Доказ. Користећи биномну формулу, записаћемо 99^{99} као:

$$(100-1)^{99}=\sum_{k=0}^{99}\binom{99}{k}100^k(-1)^{99-k}.$$

Обзиром на то да је биномни коефицијент природан број, а да је један од чинилаца у суми степен броја 100, а други степен броја -1, јасно је да 99^{99} даје остатак 99 при дијељењу са 100. То је лако показати рачунањем чланова Биномног развоја за $k=0$ и $k=1$. Тако за

$k = 0$ добијамо вриједност -1, а за $k = 1$ добијамо вриједност 9900. Сви остали чланови у развоју ће сигурно бити већи од 100 по апсолутној вриједности и посљедње 2 цифре биће нуле. То онда значи да ће се 99^{99} завршавати са 99, тј. остатак при дијељењу са 100 ће бити 99, односно $99^{99} \equiv 99 \pmod{100}$, што је еквивалентно са $99^{99} \equiv -1 \pmod{100}$. Зато је $99^{99} + 1$ дјељив са 100. Ово није довољно да закључимо са колико нула се завршава овај број.
Уочимо да је сваки члан у развоју дјељив са 1000, осим првог и другог (за $k = 0$ и $k = 1$). Први члан је једнак -1, а други 9900. Зато се цијела сума завршава са 899. То значи да $99^{99} + 1$ даје остатак 900 при дијељењу са 1000.
Дакле, број $99^{99} + 1$ се завршава са 2 нуле. $\square$

(**Лазар Шћекић 6/19 Б**) задатак са интернета `http://forum.matemanija.com/viewtopic.php?f=44&t=4459`

54

Наћи све парове природних бројева $(a,\ b)$, у којима је $a > b$ и важи

$$\text{нзс}(a, b) - \text{нзд}(a, b) = 2019.$$

Доказ. Означимо $d = \text{нзд}(a, b)$ и $a = da_1$, $b = db_1$, при чему је $\text{нзд}(a_1, b_1) = 1$. Тада је $\text{нзс}(a, b) = da_1b_1$, па дата једначина постаје $da_1b_1 - d = 2019$, тј. $d(a_1b_1 - 1) = 2019 = 3 \cdot 673$ (број 673 је прост). Имамо следеће могућности.
(1) $d = 1, a_1b_1 = 2020 = 2^2 \cdot 5 \cdot 101$. Пошто је $\text{нзд}(a_1, b_1) = 1$, пар $(a, b) = (a_1, b_1)$ може бити $(2020, 1), (505, 4), (404, 5)$ или $(101, 20)$.
(2) $d = 3, a_1b_1 = 674 = 2 \cdot 337$. Пар (a_1, b_1) може бити $(674, 1)$ или $(337, 2)$, а одговарајући парови (a, b) су $(2022, 3)$ и $(1011, 6)$.
(3) $d = 673, a_1b_1 = 4$. Мора бити $(a_1, b_1) = (4, 1)$, па је $(a, b) = (2692, 673)$
(4) $d = 2019, a_1b_1 = 2$. Мора бити $(a_1, b_1) = (2, 1)$, па је $(a, b) = (4038, 2019)$.
Укупно добијамо 8 рјешења и то: $(2020, 1), (505, 4), (404, 5), (101, 20), (2022, 3), (1011, 6), (2692, 673)$ и $(4038, 2019)$. $\square$

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

55

Доказати да за природне бројеве a и b важи

$$\text{нзд}(a, b) + \text{нзс}(a, b) = a + b$$

ако и само ако је један од бројева a и b дјељив другим.

Доказ. Означимо $d = \text{нзд}(a, b)$ и $a = da_1, b = db_1$ при чему је $\text{нзд}(a_1, b_1) = 1$. Тада је $\text{нзс}(a, b) = da_1b_1$, па дата једнакост постаје

$$da_1b_1 + d = da_1 + db_1 \Leftrightarrow 0 = da_1b_1 - da_1 - db_1 + d = d(a_1 - 1)(b_1 - 1)$$

Слиједи да је $a_1 = 1$ или $b_1 = 1$, тј. $a = d \mid b$ или $b = d \mid a$

$\square$

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb/`

56

Доказати да производ два цијела позитивна броја,од којих је сваки мањи од простог броја p,није дељив са p.

Доказ. Претпоставимо да постоје два цијела позитивна броја x и y која су оба мања од простог броја p,таква да $p \mid x \cdot y$. Даље претпоставимо да за њих важи да је њихов производ дјељив са простим бројем p. Уколико је то тачно,даље ће постојати најмањи позитиван број $y_1 \leq y$, који при множењу са x даје садржалац броја p. Дијељењем y_1 са p добијамо:

$$y_1 = p \cdot m + n, n < y_1 < p$$

Одатле слиједи

$$n = y_1 - p \cdot m$$

Множењем лијеве и десне стране са x добија се:

$$x \cdot n = y_1 \cdot x - p \cdot m \cdot x$$

Одатле се види да је $x \cdot n$ дјељиво са p јер је производ $y_1 \cdot x$ дјељив са p по претпоставци да је y_1 најмањи број за који то важи,а $p \cdot m \cdot x$ је дјељив са p јер је p један његов чинилац. Међутим, $n < y_1$,па y_1 неће бити најмањи позитиван број којим треба помножити x да се добије садржалац броја p,као што је изречено у претпоставци.Дакле,добијамо контрадикцију и отуда слиједи да производ $x \cdot y$ није дјељив са p.

$\square$

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

57

Доказати да је број $7 + 7^2 + ... + 7^{4k}$, $k \in N$, дјељив са 400.

Доказ. Дата сума се може записати на сљедећи начин:

$$(7 + 7^2 + 7^3 + 7^4) + (7^5 + 7^6 + 7^8 + 7^9) + ... + (7^{4k-3} + 7^{4k-2} + 7^{4k-1} + 7^{4k})$$

Извлачењем првог чиониоца се добија:

$$(7 + 7^2 + 7^3 + 7^4)(1 + 7^4 + 7^8 + ... + 7^{4k-4})$$

Сума $7 + 7^2 + 7^3 + 7^4$ једнака је $7 \cdot 400$ па је дјељива са 400, а самим тим је и читав израз дјељив са 400.

$\square$

(**Лазар Шћекић 6/19 Б**) задатак са интернета
Олимпиадные задачи «Теория чисел»

58

●●●●

Два двоцифрена броја записана један за другим чине четвороцифрени број који је дјељив са њиховим производом. Наћи те бројеве.

Доказ. Нека су тражени бројеви x и y. Тада мора важити да је

$$100x + y = kxy, k \in N$$

Из $y = x(ky - 100)$ слиједи да $x \mid y$.
Нека је $y = ux$. Како је $u = \frac{y}{x} \leq 99/10$ имамо да $u \in \{1, 2, \dots, 9\}$
Уврштавањем добијамо: $100 = u(kx - 1)$. Дакле $u \mid 100$ па је $u \in \{1, 2, 4, 5\}$
Надаље,мора важити $k \geq 2$, јер за $k = 1$ имамо $u(x - 1) < xu = y < 100$
Ако је $u = 1$ онда је $kx = 101$,што је немогуће јер је $k \geq 2$ и x двоцифрен.
Ако је $u = 2$ онда је $kx = 51$,одакле је $k = 3, x = 17, y = 34$.
Ако је $u = 4$ онда је $kx = 26$,одакле је $k = 2, x = 13, y = 52$.
Ако је $u = 5$ онда је $kx = 21$,што нема рјешење за $k \geq 2$ и x двоцифрен.
Дакле, рјешења су
$(x, y) = (17, 34)$
$(x, y) = (13, 52)$. □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/zadacinatj1.pdf`

59

●●●●

Показати да ако је k непаран број, онда 2^{n+2} дијели $k^{2^n} - 1$ за све природне бројеве n.

Доказ. За случај $n = 1$ имамо да је $k^2 - 1 = (k - 1)(k + 1)$ дјељиво са 8, јер због непарности броја к имамо да су $(k - 1)$ и $(k + 1)$ парни бројеви од којих је један дјељив са 4, а како су парни оба су дјељива са 2.

Сада претпоставимо да $2^{n+2} | k^{2^n} - 1$, покажимо да $2^{n+3} | k^{2^{n+1}} - 1$

Познато нам је да важи:

$$k^{2^{n+1}} - 1 = (k^{2^n} - 1)(k^{2^n} + 1)$$

Како из индуктивне претпоставке знамо да $2^{n+2} | k^{2^n} - 1$ онда је довољно показати да

$$2 | k^{2^n} + 1$$

Знајући да је због непарности k израз k^{2^n} такође непаран, па је онда $k^{2^n} + 1$ паран, што је било потребно показати.

□

(**Андрија Бошковић 14/19 Б**)задатак преузет са

60

Показати да 169 дијели израз $3^{3n+3} - 26n - 27$ за сваки природан број n.

Доказ. Доказ ћемо спровести уз помоћ математичке индукције.

За $n = 1$ евидентно имамо:

$$3^6 - 53 = 676 = 169 \cdot 4$$

.

Претпоставимо сада да тврђење важи за $n-1, n > 1$, то значи да важи и сљедећи израз:

$$3^n - 26n - 1 = 169 \cdot N$$

при чему је N неки природан број.

$$3^{3n+3} - 26n - 27 = 27 \cdot 3^n - 26n - 27 = 27 \cdot (3^n - 26n - 1) + 676 \cdot n = 27 \cdot 169 \cdot N + 4 \cdot 169$$

Из посљедње једнакости смо закључили да је $3^{3n+3} - 26n - 27$ заиста дјељиво са 169, што је требало и показати.

□

(**Андрија Бошковић 14/19 Б**)задатак преузет са

61

Наћи све природне бројеве за које важи $3^{n-1} + 5^{n-1} | 3^n + 5^n$

Доказ. Јасно је да важи сљедеће:

$$3^{n-1} + 5^{n-1} | 5(3^{n-1} + 5^{n-1}) = 3^n + 2 \cdot 3^{n-1} + 5^n$$

Како тражимо оне природне бројеве за које важи $3^{n-1} + 5^{n-1} | 3^n + 5^n$, претпоставићемо да ово важи. Тако имамо да онда:

$$3^{n-1} + 5^{n-1} | (3^n + 2 \cdot 3^{n-1} + 5^n) - (3^n + 5^n)$$

Остало је још да сазнамо за које случајеве важи $3^{n-1} + 5^{n-1} | 2 \cdot 3^{n-1}$.

За $n > 1$ важи да $3^{n-1} + 5^{n-1} > 2 \cdot 3^{n-1}$, па не може важити претпоставка.

Случај $n = 1$ је једини који задовољава почетни услов.

□

(**Андрија Бошковић 14/19 Б**)задатак преузет са

62

Нека су x и y природни бројеви и $xy = 2013^{2014}$. Доказати да број $x+y$ није дјељив бројем 2012.

Доказ. Јасно је да је 2013^{2014} непаран број, из чега слиједи да су x и y непарни бројеви. (производ два непарна броја је непаран број, па је јасно да је и производ више непарних бројева непаран број). $x+1$ и $y+2$ су онда парни, тј. дјељиви са 2, па слиједи да је производ $(x+1)(y+1) \equiv 0 \pmod 4$, односно да је:

$$(x+1)(y+1) = xy + x + y + 1 = 2013^{2014} + x + y + 1 \equiv 0 \pmod 4.$$

Како је $2013 \equiv 1 \pmod 4$, то је и $2013^{2014} \equiv 1 \pmod 4$, одакле је $2013^{2014} + 1 \equiv 2 \pmod 4$. (све ово закључујемо из својстава модуларне аритметике).
Сада, пошто имамо да је $2013^{2014}+x+y+1 \equiv 0 \pmod 4$ и $2013^{2014}+1 \equiv 2 \pmod 4$, слиједи да мора важити $x+y \equiv 2 \pmod 4$. Како $4 \mid 2012$, то значи да због претходне једнакости $x+y$ није дјељиво са 2012. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`https://www.pmf.ni.ac.rs/mii-content/2014/Broj%202014%20u%20zanimljivim%20zadacima.pdf`

63

Претпоставимо да је x природан број такав да бројеви x и x^2 имају исти k-тоцифрени завршетак. Доказати да тада сви степени броја x имају k-тоцифрени завршетак.

Доказ. По услову задатка је разлика $x^2 - x$ дјељива са 10^k. Доказ спроводимо индукцијом по n. За $n = 1$ јасно.
Претпоставимо да важи за n тј. да $x, x^2, \ldots, x^n$ имају исти k-тоцифрени завршетак.
За $n+1$ слиједи да је разлика $x^{n+1} - x^n = x^{n-1}(x^2 - x)$ такође дјељива са 10^k, што значи да бројеви x^n и x^{n+1} имају исти k-тоцифрени завршетак.
Индукцијом смо показали да бројеви $x^2, \ldots, x^n, \ldots$ имају исти k-тоцифрени завршетак. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

64

Показати да број 1002004008016032 садржи прост фактор $p > 250000$.

Доказ. Ако узмемо $a = 10^3$ и $b = 2$ онда,

$$1002004008016032 = a^5 + a^4b + a^3b^2 + a^2b^3 + ab^4 + b^5 = \frac{a^6 - b^6}{a - b}$$

$$\frac{a^6-b^6}{a-b}=(a+b)(a^2+ab+b^2)(a^2-ab+b^2)=1002\cdot 1002004\cdot 998004=4\cdot 4\cdot 1002\cdot 250501\cdot k$$

где је $k<250000$. Из претходне једнакости закључујемо да је тражено $p=250501$. ☐

(**Андрија Бошковић 14/19 Б**) задатак преузет са `https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

65

Дат је природан број n. Нека су $m, a, b, c \in \mathbb{N}$ такви да $a \mid b^n$, $b \mid c^n$ и $c \mid a^n$, али $abc \nmid (a+b+c)^m$. Одредити највећу могућу вриједност m.

Доказ. Посматрајмо неки прости број $p \mid a$. Нека $p^\alpha \| a$, $p^\beta \| b$ и $p^\gamma \| c$ и нека је без смањења општости $\gamma \leqslant \alpha, \beta$. По услову задатка је $\alpha < n\beta < n^2\gamma$, па је $\alpha+\beta+\gamma \leqslant (n^2+n+1)\gamma$. Како $p^\gamma \mid a+b+c$ и $p^{\alpha+\beta+\gamma} \| abc$ (што важи за свако p), слиједи да $abc \mid (a+b+c)^{n^2+n+1}$. Дакле, $m \leqslant n^2+n$.
С друге стране, за $a=c^{n^2}$ и $b=c^n$,$abc=c^{n^2+n+1}$ не дијели $(a+b+c)^{n^2+n}$. Овај примјер показује да је $\max m = n^2+n$. ☐

(**Сања Лончар 7/19 Б**) задатак преузет са `https://imomath.com/srb/dodatne/kanonska_faktorizacija_ddj.pdf`

66

Нека је n природан број такав да је број $2n$ има 28 позитивних дјелиоца, а број $3n$ има 30 позитивних дјелиоца. Колико позитивних дјелиоца има број $6n$?

Доказ. Како је $6=2\cdot 3$, када нађемо дјелиоце броја $2n$ и броја $3n$, комбинацијом та два ћемо лако пронаћи дјелиоце броја $6n$.Као што знамо сваки број можемо да прикажемо као производ својих простих дјелиоца, па ћемо то урадити и за $2n$ и $3n$,па на основу њих и за $6n$.
Број n прикажимо у облику

$$n=2^{e_1}\cdot 3^{e_2}\cdot {p_3}^{e_3}\cdots {p_k}^{e_k}$$

Тада је

$$2n=2^{1+e_1}\cdot 3^{e_2}\cdot {p_3}^{e_3}\cdots {p_k}^{e_k}$$

$$3n=2^{e_1}\cdot 3^{1+e_2}\cdot {p_3}^{e_3}\cdots {p_k}^{e_k}$$

$$6n=2^{1+e_1}\cdot 3^{1+e_2}\cdot {p_3}^{e_3}\cdots {p_k}^{e_k}$$

Према услову задатка је

$$(2+e_1)(e_2+1)(e_3+1)\cdots(e_k+1)=28$$

$$(1+e_1)(e_2+2)(e_3+1)\cdots(e_k+1)=30$$

Ставимо сада да је $t=(e_3+1)\cdots(e_k+1)$.Тада је

$$(2+e_1)(e_2+1)t=28$$

$$(1+e_1)(e_2+2)t=30$$

Дакле, t је заједнички дјелилац бројева 28 и 30 па је $t=1$ или $t=2$ (јер цу то једини заједнички дјелиоци за 28 и 30). Ако је $t=1$, онда је

$$(2+e_1)(e_2+1)=28$$

$$(1+e_1)(e_2+2)=30.$$

Одавде, рјешавајући систем, налазимо $e_1=5$ и $e_2=3$.Тада је:

$$\tau(6n)=(2+e_1)(e_2+2)t=7\cdot5\cdot1=35.$$

Ако је $t=1$, онда је

$$(2+e_1)(e_2+1)=14$$

$$(1+e_1)(e_2+2)=15.$$

Једноставно се провјерава да овај систем једначина нема рјешења у скупу цијелих бројева:

$$2e_2+2+e_1e_2+e_1=14$$

$$e_2+2+e_1e_2+2e_1=15$$

Када од друге једначине одузмемо прву добијамо:

$$-e_2+e_1=1$$

$$e_1=e_2+1$$

Замјеном овога у другу једначину система добијамо:

$$(e_2+5)^2=15$$

Одакле видимо да ова једначина нема цјелобројних рјешења.Дакле, 35 је једино рјешење.

$\square$

(**Сања Лончар 7/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

67

Доказати да не постоје цијели бројеви m и n такви да важи

$$(m+n+2)^2=3(mn+1).$$

Доказ. За сваки природан број k важи да ако $3 \mid k^2 \Rightarrow 3 \mid k$, тј. ако $3 \mid k^2 \Rightarrow 9 \mid k^2$. Ако би постојали цијели бројеви m и n за које важи $(m+n+2)^2 = 3(mn+1)$, слиједило би да $3 \mid (m+n+2)^2$ односно $3 \mid (m+n+2)$ тј. $3 \mid (mn+1)$. Из $3 \mid (mn+1)$ слиједи да ниједан од бројева m и n не може бити дјељив са 3, нити оба могу давати једнаке остатке при дијељењу са 3. Дакле, један од њих даје остатак 1 при дијељењу са 3, а други даје осатак 2. Ако је рецимо $m = 3p+1$ и $n = 3q+2$ за неке p и q, тада имамо $m+n+2 = 3(p+q+1)+2$, што је немогуће јер $3 \mid (m+n+2)$.
Дакле, не постоје цијели бројеви m и n са датим својством.

☐

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

68

Доказати да број чији се декадни запис састоји само од нула и двојки не може бити потпун квадрат.

Доказ. Означимо са n посматрани број. Нека се n завршава са тачно k нула, $k \geq 0$. Дакле, $n = x \cdot 10^k$ за неки природан број x који се завршава цифром 2. Како је $n = x \cdot 10^k = x(10^{\frac{k}{2}})^2$ да би n био потпун квадрат k мора бити паран број и x мора бити потпун квадрат. Уколико је x једноцифрен број, тј. 2 одмах имамо контрадикцију јер 2 није потпун квадрат. Одавде слиједи да x мора имати макар двије цифре.
Без обзира да ли је претпоследња цифра броја x 0 или 2, у оба случаја имамо да двоцифрени завршетак броја x није дјељив са 4, али јесте са 2. Како је x потпун квадрат, можемо га записати као $x = a^2$ за неки природан број a. x је дјељив са 2, па a мора бити дјељиво са 2 јер је 2 прост број. Одавде би x морало бити дјељиво са 4, а то је контрадикција. Дакле n не може бити потпун квадрат. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

69

Нека су a, b и c произвољни природни бројеви. Доказати неједнакост

$$\text{нзд}(a, b-1) \cdot \text{нзд}(b, c-1) \cdot \text{нзд}(c, a-1) \leq ab + bc + ca - a - b - c + 1,$$

као и да се једнакост достиже за бесконачно много тројки (a, b, c)

Доказ. Означимо са $d = \text{нзд}(a, b-1)$, $e = \text{нзд}(b, c-1)$ и $f = \text{нзд}(c, a-1)$.
Како $d \mid a$, $e \mid b$ и $f \mid c$, то онда $def \mid abc$. Такође, $d \mid b-1$, $e \mid c-1$ и $f \mid a-1$, тако да $def \mid (b-1)(c-1)(a-1)$. Дакле $def \mid abc - (b-1)(c-1)(a-1) = ab + bc + ca - a - b - c + 1$, одакле слиједи тражена неједнакост.

Са друге стране, узмимо $(a, b, c) = (n, n+1, n+2)$. Како је $def = n(n+1)\,\text{нзд}(n+2, n-1) =$

$n(n+1)$ нзд$(n+2, n+2-(n-1)) = n(n+1)$ нзд$(n+2,3)$ и $ab+bc+ca-a-b-c+1 = 3n(n+1)$ закључујемо да једнакост важи за сваки природан број n такав да $3 \mid n+2$, а таквих је бесконачно много, па самим тим и тројки $(a,b,c) = (n, n+1, n+2)$. ☐

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com`

70

Одредити најмањи природан број m такав да је $82^n + m \cdot 69^n$ дјељив с 1963 за све непарне природне бројеве n .

Доказ. Релација $1963|82^n + m \cdot 69^n$ мора важити за све непарне бројеве n, стога и за $n = 1$. Наћи ћемо најмањи број m такав да је испуњено $1963 = 13 \cdot 151|82 + m \cdot 69$.
Мора дакле бити

$$82 + m \cdot 69 = k(80 - 69)(82 + 69)$$

и одавде се добија да је m облика

$$m = (89 - 69)s - 1 = 13s - 1$$

$$m = (89 + 69)t + 1 = 151t + 1$$

те је за $s = 35$ и $t = 3$ најмањи такав $m = 3 \cdot 151 + 1 = 35 \cdot 13 - 1$
Доказаћемо да је то тражена вриједност за m, тј. да за сваки непарни број n важи

$$13 \cdot 151|82^n + (3 \cdot 151 + 1)69^n$$

tj.

$$13 \cdot 151|82^n + 69^n + 3 \cdot 151 \cdot 69^n.$$

Будући да је $151 = (82 + 69)|82^n + 69^n$ са сваки непаран број n, па преостаје показати да важи

$$13|82^{n-1} - 82^{n-2} \cdot 69 + 82^{n-3} \cdot 69^2 - \cdots - 82 \cdot 69^{n-1} + 3 \cdot 69^n$$

тј.

$$13|82^{n-2}(82 - 69) + \cdots + 82 \cdot 69^{n-3}(82 - 69) + 69^{n-1}(1 + 3 \cdot 69)$$

што је очигледно тачно, јер је сваки сабирак дјељив са 13.

☐

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://www.fer.unizg.hr/_download/repository/diskont1-11.pdf`

71

Доказати да је за сваки $n \in \mathbb{N}$ тачно један од бројева $2^{2n+1} - 2^{n+1} + 1$, $2^{2n+1} + 2^{n+1} + 1$ дјељив с 5.

Доказ. Довољно је показати да је производ A_n и B_n увијек дјељив са 5, а разлика $B_n - A_n$ то никад није.Тада је тачно један од бројева A_n, B_n дјељив са 5.

$$
\begin{aligned}
B_n \cdot A_n &= (2^{2n+1} - 2^{n+1} + 1)(2^{2n+1} + 2^{n+1} + 1) \\
&= 2^{4n+2} + 2 \cdot 2^{2n+1} + 1 - 2^{2n+2} \\
&= 2^{4n+2} + 1 = 4^{2n+1} + 1 \\
&= (5-1)^{2n+1} + 1 \equiv 0 \pmod 5
\end{aligned}
$$

$B_n - A_n = 2^{n+2}$ није конгруентно са 0 по модулу 5.Дакле, тачно један од бројева A_n, B_n дјељив са 5. $\square$

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://www.fer.unizg.hr/_download/repository/diskont1-11.pdf`

72

Подијелимо ли природан број бројем 6 остатак је 3. Колики је остатак ако број $3x$ подијелимо бројем 6?

Доказ. Означимо са x природан број, који при дијељењу са бројем 6 даје остатак 3. Сада према Теореми о дијељењу са остатком имамо да је:

$$x = 6k + 3,$$

за неки природан број k. Множењем једнакости са 3 добијамо:

$$3x = 18k + 9 = 6(3k + 1) + 3 = 6l + 3,$$

гдје је $l = 3k + 1$ очигледно природан број. Из тога закључујемо да је остатак при дијељењу броја $3x$ бројем 6 једнак 3.

$\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

73

Одредити највећи природан број n за који је $n^3 + 100$ дјељиво са $n + 10$.

Доказ. Ако $n + 10 \mid n^3 + 100$ онда је нзд$(n^3 + 100, n + 10) = n + 10$. Примјеном Еуклидовог алгоритма добијамо:

$$\text{нзд}(n^3+100, n+10) = \text{нзд}(-10n^2+100, n+10) = \text{нзд}(100n+100, n+10) = \text{нзд}(-900, n+10).$$

Дакле, $n + 10 \mid 900$. Највећи природан број за који $n + 10$ дијели 900 је 890. $\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

74

Одредити све четвороцифрене бројеве, чије су прве двије и задње двије цифре међусобно једнаке, а који су потпуни квадрати (тј. квадрати неког природног броја).

Доказ. Нека је тражени број квадрат броја n, дакле $n^2 = \overline{aabb}$. Имамо да важи:

$$\overline{aabb} = 1100a + 11b = 11 \cdot (100a + b) = 11 \cdot \overline{a0b},$$

при чему су a и b цифре, $a \neq 0$, тј. број $\overline{aabb} = n^2$ је дјељив са 11. Одавде закључујемо да је n дјељив са 11, тј. $n = 11k$, за неко $k \in \mathbb{N}$. То значи да је тражени број облика $121k^2$. Да би тај број био четвороцифрен мора бити $3 \leq k \leq 9$. Рачунамо редом:

k	3	4	5	6	7	8	9
$121k^2$	1089	1936	3025	4356	5929	7744	9801

Видимо да је једино рјешење број 7744 (квадрат броја 88).

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

75

Нека је r остатак при дијељењу бројева 1059, 1417 и 2312 бројем $d > 1$. Наћи вриједност израза $d - r$.

Доказ. Примјеном Теореме о дијељењу са остатком имамо:

$$\begin{aligned} 1059 &= q_1 d + r,\\ 1417 &= q_2 d + r,\\ 2312 &= q_3 d + r, \end{aligned}$$

за неке цијеле бројеве q_1, q_2, q_3. Из тога слиједи:

$$\begin{aligned} 358 = 1417 - 1059 &= (q_2 d + r) - (q_1 d + r) = d(q_2 - q_1),\\ 1253 = 2312 - 1059 &= (q_3 d + r) - (q_1 d + r) = d(q_3 - q_1),\\ 895 = 2312 - 1417 &= (q_3 d + r) - (q_2 d + r) = d(q_3 - q_1). \end{aligned}$$

Дакле,

$$\begin{aligned} d \mid 358 &= 2 \cdot 179,\\ d \mid 1253 &= 7 \cdot 179,\\ d \mid 895 &= 5 \cdot 179. \end{aligned}$$

Будући да је $d > 1$ закључујемо да је $d = 179$. Како је $1059 = 5 \cdot 179 + 164$ слиједи да је $r = 164$. Дакле, $d - r = 179 - 164 = 15$.

$\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

76

Колико има уређених парова природних бројева (m, k) за које важи

$$20m = k(m - 15k)?$$

Доказ. Изразимо ли m преко k добијамо:

$$m = \frac{15k^2}{k - 20}.$$

Одавде слиједи да је m природни број ако и само ако је $k > 20$ и $k - 20 \mid 15k^2$. Будући да је

$$\frac{15k^2}{k-20} = \frac{15(k-20)(k+20) + 20^2 \cdot 15}{k-20} = 15(k+20) + \frac{6000}{k-20},$$

m је природни број ако и само ако је $k > 20$ и $k - 20 \mid 6000$. Како је $6000 = 2^4 \cdot 3 \cdot 5^3$, сваки позитивни дјелилац броја 6000 је облика $2^a \cdot 3^b \cdot 5^c$, при чему је $a \in \{0, 1, 2, 3, 4\}$, $b \in \{0, 1\}$ и $c \in \{0, 1, 2, 3\}$. Зато је број дјелиоца броја 6000 једнак $5 \cdot 2 \cdot 4 = 40$. Закључујемо да тражених парова (m,k) има 40.

$\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

77

Доказати да постоји природан број n, који има тачно 2000 дјелиоца и за који важи $n \mid 2^n + 1$.

Доказ. Доказаћемо индукцијом по k да за свако $k \in \mathbb{N}$ постоји n_k, које има тачно k различитих простих дјелиоца, такав да $n_k \mid 2^{n_k} + 1$ и $3 \mid n_k$.

За $k = 1, n_1 = 3$ задовољава услов. Претпоставимо да је $k \geq 1$ и $n_k = 3^{\alpha} m$, гдје $3 \nmid m$, па m има $k - 1$ простих дјелиоца. Тада број $3n_k = 3^{\alpha+1}m$ има тачно k простих дјелиоца и $2^{3n_k} + 1 = (2^{n_k} + 1)(2^{2n_k} - 2^{n_k} + 1)$ је дјељиво са $3n_k$, јер $3 \mid 2^{2n_k} - 2^{n_k} + 1$. Одабраћемо прост број p који не дијели n_k, тако да буде $n_{k+1} = 3pn_k$. Довољно је узети p тако да $p \mid 2^{3n_k} + 1$ и $p \nmid 2^{n_k} + 1$.

Важи и јаче тврђење, да за сваки цијели број $a > 2$ постоји прост број p, који дијели $a^3+1 = (a+1)(a^2-a+1)$, а не дијели $a+1$. Заиста, важи нзд$(a^2-a+1, a+1) =$ нзд$(3, a+1)$, па ако $3 \nmid a+1$ довољно је узети $p = 3$. У супротном, ако је $a = 3b-1$ онда $a^2-a+1 = 9b^2-9b+3$ није дјељиво са 3^2, па за p можемо узети било који прост дјелиоц броја $\frac{a^2-a+1}{3}$. □

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/stepene%20kongruencije_ddj.pdf`

78

(а) Доказати да је број $2^{2^n} - 4$ дјељив са 12, за све $n \in \mathbb{N}$.
(б) Одредити највећи заједнички дјелилац бројева $2^{2006} - 1$ и $2^{2004} - 1$.
(в) Збир 49 природних бројева једнак је 999. Одредити највећу могућу вриједност њиховог највећег заједничког дјелиоца.
(г) Доказати да је број $2012^9 + 2016^9$ дјељив са 2014.

Доказ. (а) За $n \geq 1$ је $2^n \geq 2$, па је $2^{2^n} - 4 = 4(2^{2^n-1} - 1)$, односно дати број је дјељив са 4. Такође, број $2^{2^n} = (2^{2^{n-1}})^2$ није дјељив са 3, па како је потпун квадрат, даје остатак 1 при дијељењу са 3. Самим тим, дати број је дјељив и са 3 чиме је доказ завршен.

(б) Највећи заједнички дјелилац за дате бројеве је и дјелилац њихове разлике

$$2^{2006} - 2^{2004} = 2^{2004}(2^2 - 1) = 2^{2004} \cdot 3.$$

Пошто су задати бројеви непарни, остаје да се провјери да ли је

$$\text{нзд}(2^{2006} - 1, 2^{2004} - 1) = 1 \quad \vee \quad \text{нзд}(2^{2006} - 1, 2^{2004} - 1) = 3.$$

Лако се доказује да је $2^{2n} - 1$ увијек дјељив са 3.

Заиста, $2^{2n} - 1 = 4^n - 1$, па то слиједи нпр. из идентитета $x^n - 1 = (x-1)(x^{n-1} + \ldots + x + 1)$. Тачан одговор је

$$\text{нзд}(2^{2006} - 1, 2^{2004} - 1) = 3.$$

(в) Нека је d највећи заједнички дјелилац тих 49 бројева. Тада важи

$$d \mid 999 = 3^3 \cdot 37$$

и како мора бити $d \leq \frac{999}{49} < 21$, слиједи $d \in \{1, 3, 9\}$. Вриједност 9 се може постићи, нпр.

$$\underbrace{9 + 9 + \ldots + 9}_{48} + 567 = 999$$

и тада је нзд$(9, 9, \ldots, 9, 567) = 9$.

(г) Користимо факторизацију

$$a^3 + b^3 = (a+b)(a^2 - ab + b^2).$$

Из ње закључујемо да, ако су a и b цијели бројеви, онда $a + b \mid a^3 + b^3$. Такође, $a^3 + b^3 \mid a^9 + b^9$, па важи и $a + b \mid a^9 + b^9$.

Дакле, $2012 + 2016 \mid 2012^9 + 2016^9$.

Будући да је $2012 + 2016 = 4028 = 2 \cdot 2014$ закључујемо да $2014 \mid 2012^9 + 2016^9$. ☐

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imomath.com/srb/zadaci/2013_opstinsko.pdf`
`https://imomath.com/srb/zadaci/bilten2006.pdf`
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

79

●●●●

Доказати да је за сваки природан број n, $n > 0$ bpoj $3(1^5 + 2^5 + \cdots + n^5)$ дјељив са $1^3 + 2^3 + \cdots + n^3$

Доказ. За природан позитиван број n важи:

$$1^3 + 2^3 + \cdots + n^3 = \frac{n^2(n+1^2)}{4}$$

Доказ се врло једноставно изводи математичком индукцијом.

За $\underline{n = 1}$, очигледно:

$$1 = 1^3 = \frac{1^2 \cdot 2^2}{4} = \frac{4}{4} = 1$$

$\underline{n = k}$(IP)

$$\frac{k^2(k+1^2)}{4}$$

$\underline{n = k + 1}$

$$1^3+2^3+\cdots+k^3+(k+1)^3 = \frac{k^2(k+1^2)}{4}+(k+1)^3 = \frac{k^2(k+1^2)+4(k+1^3)}{4} = \frac{(k+1^2)(k^2+4k+4)}{4} = \frac{k+1^2(k+2^2)}{4}$$

чиме је доказ овог идентитета завршен.

На сличан начин показује се и да је:

$$1^5 + 2^5 + \cdots + n^5 = \frac{n^2(n+1^2)(2n^2+2n-1)}{12}$$

Користећи показано слиједи да је

$$3(1^5 + 2^5 + \cdots + n^5)/(1^3 + 2^3 + \cdots + n^3) = 2n^2 + 2n - 1$$

што је очигледно цио број, па је овим и доказ почетног проблема завршен. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

80

Наћи све позитивне цијеле бројеве x за које важи да је $x^{10}+1$ дјељиво са 10.

Доказ. Ако је x позитиван цио број, а r његов остатак при дијељењу са 10, тада

$$10 \mid (x^{10}+1) \iff 10 \mid (r^{10}+1)$$

Сада је довољно посматрати вриједности $r \in 0,1,2,\dots,9$ јер су то једини могући остаци при дијељењу броја са 10. За бројеве из овог скупа лако је провјерити да су само $3^{10}+1$ и $7^{10}+1$ дјељиви са 10. Дакле, сви бројеви x за које важи да је $x^{10}+1$ дјељиво са 10 су облика $10k+3$ и $10k+7$, за $k=0,1,2,\dots$. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf

81

Доказати да $(3!)^n \mid (3n)!$, $\forall n \geqslant 0$.

Доказ. За $\underline{n=1}$

$$\frac{(3\cdot 1)!}{(3!)^1}=1$$

$\underline{n=k}$(IP)

$$\frac{(3k)!}{(3!)^k}=l,\ l\in Z$$

$\underline{n=k+1}$

$$\frac{(3(k+1))!}{(3!)^{k+1}}=\frac{(3k+3)!}{(3!)^k(3!)}=\frac{(3k)!}{(3!)^k}\frac{(3k+3)(3k+2)(3k+1)}{6}=l\frac{3(k+1)(3k+2)(3k+1)}{6}=l\frac{(k+1)(3k+2)(3k+1)}{2}$$

Разликујемо два случаја:

1. k - парно $\Rightarrow k=2r \Rightarrow 3k+2=6r+2=2(3r+1) \Rightarrow 2 \mid 3k+2$
2. k - непарно $\Rightarrow k=2r+1 \Rightarrow k+1=2r+2=2(r+1) \Rightarrow 2 \mid 3k+1$

У оба случаја, десна страна претходне једнакости биће цио број, чиме смо доказали почетно тврђење. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-mo
pdf

82

Доказати да је за $\forall n \in N$, $(n!)!$ дјељиво са $n!^{(n-1)!}$.

Доказ. Прво покажимо следеће:

$$(mn)! \text{ је дјељиво са } n!^m.$$

$1 \cdot 2 \cdot 3 \cdots n = n!$ је дјељиво са n!.

Даље, $(n+1) \cdot (n+2) \cdot (n+3) \cdots 2n$ је дјељиво са n!. Ово се да закључити на основу биномног коефицијента $(\binom{n}{k=\frac{n(a-1)(a-2)\cdots(a-k+1)}{k!}})$ за чију вриједност знамо да је цио број.

Слично, $(2n+1) \cdot (2n+2) \cdot (2n+3) \cdots (2n+n)$ је дјељиво са n!.

$\vdots$

$((m-1)n+1) \cdot ((m-1)n+2) \cdots ((m-1)n+n)$ је дјељиво са n!.

$\Rightarrow (mn)!$ је дјељиво са $(n!)^m$.

За $m = (n-1)!$ важи почетно тврђење. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са `https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

83

●●●●

Наћи све парове природних бројева (x, p), таквих да је p прост број, $x \leqslant 2p$ и $x^{p-1} \mid (p-1)^x + 1$.

Доказ.
- За $x = 1$ то су парови облика $(1, p)$, p-прост број.
- За $x = 2$ то може бити само пар $(2, 2)$, јер је у овом случају x^{p-1} степен двојке, стога $(p-1)^x + 1$ мора бити парно, па је и p паран број, дакле 2 - једини паран прост број.
- За $x, p \geqslant 3$ знамо да је p непаран број, одакле закључујемо да је $(p-1)^x$ паран, тј. $(p-1)^x - 1$ непаран. Дакле, и x мора бити непаран број.

  Нека је q најмањи прости дјелилац од x (који такође мора бити непаран).

  $q \mid x \mid x^{p-1} \mid (p-1)^x + 1$, по услову задатка.

  Ово значи да је $(p-1)^x + 1 \equiv 0 \pmod{q}$, тј. $(p-1)^x \equiv -1 \pmod{q}$, односно $p-1$ и q су узајамно прости. Због овога, на основу Мале Фермаове теореме слиједи да је $(p-1)^{q-1} \equiv 1 \pmod{q}$.

  На основу тога како смо дефинисали q, важи: нзд$(x, q-1) = 1$.

  $\Rightarrow \exists a, b \in N$ тако да је $ax = b(q-1) + 1$ непарно $\Rightarrow a$ - непарно.

Сада, $p-1 \equiv (p-1)^{b(q-1)+1} = (p-1)^{ax} \equiv -1\ (\ (\bmod q)) \Rightarrow q \mid p$. Како су и q и p прости бројеви, то слиједи да је $p = q$.

На основу тога што је x непарно, $p = q \mid x$, и из услова да је $x \leqslant 2p$, закључујемо да је $x = p$, $\forall x, p \geqslant 3$.

Примијетимо да $p^{p-1} \mid (p-1)^p + 1 = p^2(mp+1)$, за неко m. Даље је $p - 1 \leqslant 2$, па је $x = p = 3$ једино рјешење.

$\square$

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.math.ust.hk/excalibur/v20_n2.pdf`

84
●●●●

Наћи све природне бројеве n такве да за сваки непаран број a за који важи да $a^2 \leq n$ онда $a \mid n$.

Доказ. Нека је a највећи непаран број такав да $a^2 \leq n$, стога $n \leq (a+2)^2$.

Ако је $a \geq 7$, онда $a-4, a-2, a$ су непарни бројеви који дијеле n.

Примјећујемо да је сваки пар наведених бројева узајамно прост. тако да $(a-4)(a-2)a$ дијели n. Из овога слиједи да $(a-4)(a-2)a \leq (a+2)^2$ тако да $a^3 - 6a^2 + 8a \leq a^2 + 4a + 4$.

Затим имамо да $a^3 - 7a^2 + 4a - 4 \leq 0$ или $a^2(a-7) + 4(a-1) \leq 0$. Ово је нетачно због тога што је $a \geq 7$, стога $a = 1, 3$ или 5.

Ако је $a = 1$, онда $1^2 \leq n \leq 3^2$, тако да $n \in \{1, 2, \ldots, 8\}$.

Ако је $a = 3$, онда $3^2 \leq n \leq 5^2$ и $1 \cdot 3 \mid n$, тако да $n \in \{9, 12, 15, 18, 21, 24\}$.

Ако је $a = 5$, онда $5^2 \leq n \leq 7^2$ и $1 \cdot 3 \cdot 5 \mid n$, тако да $n \in \{30, 45\}$.

Закључујемо да $n \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 12, 15, 18, 21, 24, 30, 45\}$.

$\square$

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

85
●○○○

Доказати да за непаран број n број $46^n + 296 \cdot 13^n$ дјељив са 1947.

Доказ. Тврђење доказујемо индукцијом по n. За $n = 1$ је

$$46 + 296 \cdot 13 = 3894 = 2 \cdot 1947.$$

Претпоставимо да тврђење важи за број n. Тада је

$$46^{n+2} + 296 \cdot 13^{n+2}$$

$$= (296 \cdot 13^n + 46) \cdot 13^n - 46^n \cdot 13^2 + 46^{n+2}$$

$$= (296 \cdot 13^n + 46^n) \cdot 13^2 + 46^n(46^2 - 13^2).$$

Како је $46^2 - 13^2 = 1947$, а израз у загради је по претпоставци дјељив са n,тиме је ово тврђење доказано.

☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`https://www.fer.unizg.hr/_download/repository/diskont1-11.pdf`

2 Конгруенције - рачун остатака

86

Нека је $p > 5$ прост број. Доказати да је

$$p^8 \equiv 1 \pmod{240}$$

Доказ.

$$204 = 2^4 \cdot 3 \cdot 5$$

Како је $p > 5$ прост број, то је он узајамно прост са $3,\ 2^4,\ 5$, па примјеном Ојлерове леме можемо да добијемо систем једначина

$$p^8 \equiv 1 \pmod{2^4}$$

$$p^8 \equiv 1 \pmod{3}$$

$$p^8 \equiv 1 \pmod{5}.$$

Замјеном $p^8 = x$ и рјешавајући систем примјеном Кинеске теореме о остацима имамо

$$n_1 = 15,\ n_2 = 80,\ n_3 = 54$$

и једначине

$$-x \equiv 1 \pmod{2^4}$$

$$2x \equiv 1 \pmod{3}$$

$$3x \equiv 1 \pmod{5}$$

Добијамо

$$x_1 = -1,\ x_2 = 2,\ x_3 = 2.$$

Односно $x_0 = -15+8\cdot 2+54\cdot 2 = 241$. Дакле, рјешења система су $x \equiv 241 \pmod{\text{нзс}(2^4, 3, 5)}$

$$x \equiv 1 \pmod{240}$$

$$p^8 \equiv 1 \pmod{240}.$$

□

(**Велибор Дошљак 15/19 Б**) задатак преузет из
104 Number Theory Problems From the Training of the USA IMO Team

87

Наћи све просте бројеве p, q, r који задовољавају једначину $p^q + q^p = r$.

Доказ. Видимо да не може да буде да су $p,\ q,\ r$ непарни бројеви. Неки од њих је паран, односно неки од њих је једнак 2. Видимо да r не може бити једнако 2. Закључујемо да је $p = 2$ или $q = 2$, и не може бити $p = q = 2$. Нека је без губљења општости $q = 2$.

$$2^p + p^2 = r$$

Ако је $p = 3$ видимо да је једнакост задовољена и да је $r = 17$. Ако $p \neq 3$, тада је $p = 3k+1$ или $3k-1$. У сваком случају имамо да $p^2 + 2^p \equiv 1+2 \pmod 3$=0, јер је p непаран па је $2^p \pmod 3 = (-1)^p \pmod 3 = 2$

Видимо да $3 \mid p^2 + 2^p = r$, па како је r прост то мора бити $r = 3$, што је немогуће јер је p прост број већи од 3.

Закључујемо да су једина рјешења $p = 3,\ q = 2,\ r = 17$, и $p = 2,\ q = 3,\ r = 17$

☐

(**Велибор Дошљак 15/19 Б**)задатак преузет са
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

88

Наћи све природне бројеве који су узајамно прости са сваким чланом низа $a_n = 2^n + 3^n + 6^n - 1$.

Доказ. Нека је броја b узајамно прост са сваким чланом низа a_n. Тада је и сваки од његових простих фактора узајамно прост са сваким елементом низа a_n. Нека је p прост број. Посматрајмо $6_{p-2} \pmod p$.

$$6a_{p-2} = 3 \cdot 2^{p+1} + 3 \cdot 3^{p-1} + 6^{p-1} - 6$$

Посматрајмо сада $6a_{p-2} \pmod p$. Како је p прост број, то на сваки од чланова суме можемо примијенити Малу Фермаову теорему.

$$6a_{p-2} \equiv\ 3 + 2 + 1 - 6 = 0 \pmod p$$

Како је p прост, $p \mid 6$ или $p \mid a_{p-2}$. Ако је $p > 3$ мораће да $p \mid a_{p-2}$. Закључујемо да нема простих бројева већих од 3 који су узајамно прости са сваким чланом низа a_n. Провјером закључујемо да $2 \mid p_1$ и $3 \mid p_2$. Како не постоје прости бројеви који су узајамно прости са сваким a_n, то не може постојати ни један природан број већи од 1 који је узајамно прост са сваким $_n$. ☐

(**Велибор Дошљак 15/19 Б**) задатак са IMO Shortlist 2005

89

●●●●

Ријешити наредну конгруенцију: $7x \equiv 12 \pmod{13}$.

Доказ. Све што треба јесте да са обије стране добијемо бројеве дјељиве бројем 7. То постижемо на начин да са десне стране додајемо 13 све док не добијемо жељени број (додавање броја 13 је исто као и додавање броја 0, тако да је то коректно). На тај начин добијамо редом: 25, 38, 51, 64, 77. Број 77 је први који нам одговара. Тако да имамо:

$$\begin{aligned} 7x &\equiv 12 \pmod{13} \\ 7x &\equiv 77 \pmod{13} \\ x &\equiv 11 \pmod{13}. \end{aligned}$$

□

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`http://discrete.openmathbooks.org/dmoi2/sec_addtops-numbth.html`

90

●●●●

Ријешити $17x \equiv 3 \pmod{29}$

Доказ. Прво провјеравамо да ли конгруенција има рјешење. Конгруенција $ax \equiv b \pmod{m}$ има рјешење ако нзд$(a, m) \mid b$. У нашем случају $a = 17$, $b = 3$, $m = 29$. Имамо да је $nzd(17, 29) = 1$, а како $1 \mid 3$ онда слиједи да конгруенција има рјешење. Тражимо мултипликативни инверз од 17 (по модулу 29). Тако да рјешавамо $17v + 29w = 1$.
Примијенимо Еуклидов алгоритам:

(1) $29 = 1 \cdot 17 + 12$
(2) $17 = 1 \cdot 12 + 5$
(3) $12 = 2 \cdot 5 + 2$
(4) $5 = 2 \cdot 2 + 1$

Ове једнакости можемо записати у следећем облику:

(5) $12 = 29 - 17$
(6) $5 = 17 - 12$
(7) $2 = 12 - 2 \cdot 5$
(8) $1 = 5 - 2 \cdot 2$

Користећи дате трансформације добијамо:

$1 = 5 - 2 \cdot 2$ уврстимо (7)
$1 = 5 - 2(12 - 2 \cdot 5)$
$1 = 5 - 2 \cdot 12 + 4 \cdot 5$
$1 = 5 \cdot 5 - 2 \cdot 12$ уврстимо (6)
$1 = 5(17 - 12) - 2 \cdot 12$
$1 = 5 \cdot 17 - 5 \cdot 12 - 2 \cdot 12$
$1 = 5 \cdot 17 - 7 \cdot 12$ уврстимо (5)
$1 = 5 \cdot 17 - 7(29 - 17)$
$1 = 5 \cdot 17 - 7 \cdot 29 + 7 \cdot 17$
$1 = 12 \cdot 17 - 7 \cdot 29$

Тражили смо $17v + 29w = 1$, а имамо $1 = 12 \cdot 17 - 7 \cdot 29$, тако да је $v = 12$, $w = -7$. Дакле,

$17 \cdot 12 \pmod{29}$, па је 12 мултипликативни инверз од 17 (по модулу 29). Имамо

$12 \cdot 17x \equiv 12 \cdot 3 \pmod{29}$, при чему је

$x \equiv 36 \pmod{29}$
$x \equiv 7 \pmod{29}$

Провјера: $17 \cdot 7 = 119 \equiv 3 \pmod{29}$ ☐

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`https://www.youtube.com/watch?v=4-HSjLXrfPs`

91 ●●●●

Одредити остатак који се добија дијељењем броја 3^{100} бројем 13.

Доказ. За рјешавање овог задатка потребна нам је следећа:

Лема: Нека су $a, b, c, d \in \mathbb{Z}$. Ako je $a \equiv b \pmod{m}$ i $c \equiv d \pmod{m}$ onda je $a \cdot c \equiv b \cdot d \pmod{m}$.

Сада смо спремни за рјешавање нашег задатка.

Како је $3 \equiv 3 \pmod{13}$ добија се $3^3 \equiv 27 \pmod{13}$.

Како је $27 \equiv 1 \pmod{13}$ такође је $3^3 \equiv 1 \pmod{13}$.

Одавде је $(3^3)^{33} \equiv 1^{33} \pmod{13}$, односно $3^{99} \equiv 1 \pmod{13}$.

А како је $3^{99} \cdot 3 \equiv 1 \cdot 3 \pmod{13}$, добијамо $3^{100} \equiv 3 \pmod{13}$.

Пошто је $0 \leq 3 < 13$ закључујемо да је 3 остатак при дијељењу броја 3^{100} бројем 13. ☐

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са `https://matematika.pmf.uns.ac.rs/wp-content/uploads/zavrsni-radovi/matematika/VojkoNestorovic`
`pdf`

92

Ријешити $555x \equiv 15 \pmod{5005}$

Доказ. (На вјежбама смо радили задатак користећи Бланкиншип методу, а у овом користићемо Еуклидов алгоритам). Како је нзд$(555, 5005) = 5$ и $5 \mid 15$ слиједи да конгруенција има рјешење. Осим тога, број 5 који смо добили као нзд$(555, 5005)$ говори нам да ћемо имати 5 рјешења, а уз то и да цијелу конгруенцију можемо подијелити бројем 5.

Тада рјешавамо следећу конгруенцију:

$$111x \equiv 3 \pmod{1001}$$

Ако конгруенцију записујемо као Диофантову једначину добијамо:

$$111x + 1001y = 3$$

Записујемо: $111x + 1001y = 1$ (памтимо 3) и примјењујемо Еуклидов алгоритам.

(1) $1001 = 9 \cdot 111 + 2$
(2) $111 = 55 \cdot 2 + 1$

Ове једнакости записујемо у следећем облику:

(3) $2 = 1001 - 9 \cdot 111$
(4) $1 = 111 - 55 \cdot 2$

Искористимо трансформације и добијамо:

$1 = 111 - 55 \cdot 2$ уврстимо (3)
$1 = 111 - 55(1001 - 9 \cdot 111)$
$1 = 496 \cdot 111 - 55 \cdot 1001$

Како смо тражили $111x + 1001y = 1$, а добили $1 = 496 \cdot 111 - 55 \cdot 1001$ одавде слиједи да је $x = 496$, $y = -55$. Дакле,

$111 \cdot 496 \equiv 1 \pmod{1001}$

Остаје још да све помножимо са 3

$111 \cdot 496 \cdot 3 \equiv 3 \pmod{1001}$, па је

$496 \cdot 3 \equiv 487 \pmod{1001}$.

Значи, једно рјешење је 487, а остала добијамо додавањем броја 1001, па су рјешења почетне конгруенције: 487, 1488, 2489, 3490, 4491. ☐

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Увод у теорију бројева (скрипта), Андреј Дујела, ПМФ - Загреб

93

Ријешити: а) $6x \equiv 2 \pmod 4$ б) $6x \equiv 3 \pmod{10}$

Доказ. а) нзд$(6, 4) = 2$ и $2 \mid 2$ па слиједи да конгруенција има рјешење. Како је нзд$(6, 4) = 2$ то значи да имамо 2 рјешења.

за $x = 1 \to 6 \equiv 2 \pmod 4$

за $x = 2 \to 12 \not\equiv 2 \pmod 4$

за $x = 3 \to 18 \equiv 2 \pmod 4$

Дакле, наша рјешења су $x_1 = 1$ и $x_2 = 3$.
Напомена: За $x = 5 \to 30 \equiv 2 \pmod 4$, али број 5 припада класи 1, јер је $5 \equiv 1 \pmod 4$, па 5 није јединствено рјешење.

б) нзд$(6, 10) = 2$ али $2 \nmid 3$ па кажемо да је конгруенција нерјешива. ☐

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`https://www.youtube.com/watch?v=fxwRrVcddww`

94

Доказати да је $\dfrac{2n^6 + 3n^2}{5}$ цио број за све $n \in \mathbb{Z}$.

Доказ. Потребно је доказати да је $2n^6+3n^2 \equiv 0 \pmod 5$ за све $n \in \mathbb{Z}$. Скуп $\{-2, 1, 0, 1, 2\}$ чини потпун систем остатака по модулу 5. Размотрићемо посебно случајеве $n \equiv 0 \pmod 5$, $n \equiv \pm 1 \pmod 5$ и $n \equiv \pm 2 \pmod 5$. Дакле:

$$\begin{aligned}
n \equiv 0 \pmod 5 &\implies 2n^6 + 3n^2 \equiv 2 \cdot 0^6 + 3 \cdot 0^2 \equiv 0 \pmod 5 \\
n \equiv \pm 1 \pmod 5 &\implies 2n^6 + 3n^2 \equiv 2 \cdot (\pm 1)^6 + 3 \cdot (\pm 1)^2 \equiv 5 \equiv 0 \pmod 5 \\
n \equiv \pm 2 \pmod 5 &\implies 2n^6 + 3n^2 \equiv 2 \cdot (\pm 2)^6 + 3 \cdot (\pm 2)^2 \equiv 140 \equiv 0 \pmod 5
\end{aligned}$$

Тиме је доказ завршен. ☐

(**Велимир Ћоровић 5/19 Б**) задатак преузет са
`https://www.math.ksu.edu/~pinner/math506/Spring2020/506S20Ex1Sols.pdf`

95

Наћи посљедњу цифру сљедећих бројева :
(а) 599^{455} (б) 2017^{2017} (ц) $3^{2019}+7^{2020}$.

Доказ. Посљедњу цифру броја $n \in \mathbb{N}$ добијамо рјешавањем једначине

$$n \equiv x \pmod{10}\ ,\ x \in \{0,1,\dots,9\}$$

У рјешавању овог задатка ћемо користити основна својства модуларне артиметике.

(а) Знајући да је $599 \equiv 9 \equiv -1 \pmod{10}$ добијамо

$$599^{455} \equiv (-1)^{455} \equiv -1 \equiv 9 \pmod{10}.$$

Дакле посљедња цифра броја 599^{455} је 9.

(б) Знајући је $2017 \equiv 7 \pmod{10}$ и $7^2 \equiv 49 \equiv -1 \pmod{10}$,одатле добијамо

$$2017^{2017} \equiv 7^{2017} \equiv 7^{2\cdot1008+1} \equiv 49^{1008}\cdot 7 \equiv (-1)^{1008}\cdot 7 \equiv 7 \pmod{10}$$

Дакле посљедња цифра броја 2017^{2017} је 7.

(ц) Одредићемо посебно посљедње цифре бројева 3^{2019} и 7^{2020} а затим их сабрати по модулу 10.

$$3^{2019} \equiv 3^{2\cdot1009+1} \equiv 9^{1009}\cdot 3 \equiv (-1)^{1009}\cdot 3 \equiv -3 \equiv 7 \pmod{10}$$
$$7^{2020} \equiv 49^{1010} \equiv 9^{1010} \equiv (-1)^{1010} \equiv 1 \pmod{10}$$

Одавде закључујемо да је $7+1=8$ посљедња цифра броја $3^{2019}+7^{2020}$. ☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`https://www.math.ksu.edu/~pinner/math506/Spring2020/506S20Ex1Sols.pdf`

96

Одредити све природне бројеве n за које је број 2^n-1 дјељив са 7.

Доказ. Посматрајмо неколико случајева природног броја n:

- $n=1$
  $2^1-1=1\equiv 1 \pmod 7$
- $n=2$
  $2^2-1=3\equiv 3 \pmod 7$
- $n=3$
  $2^3-1=7\equiv 0 \pmod 7$

- $n = 4$
  $2^4 - 1 = 15 \equiv 1 \pmod{7}$

- $n = 5$
  $2^5 - 1 = 31 \equiv 3 \pmod{7}$

- $n = 6$
  $2^6 - 1 = 63 \equiv 0 \pmod{7}$

- $n = 7$
  $2^7 - 1 = 127 \equiv 1 \pmod{7}$

Примјетимо, да се остаци при дијељењу броја $2^n - 1$ са бројем 7 понављају, тј. имају вриједности $1, 3, 0$. За нас су повољне ситуације када је остатак при дијељењу једнак нули, а то су случајеви када је:

- $n = 3$

- $n = 6$

- $n = 9$
  $\dots$

- $n = 3k$

Из претходно написаног слиједи, да је број $2^n - 1$ дјељив са бројем 7 за сваки природан број n који је облика $3k$. $\square$

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.docsity.com/sr/kongruencije-vezbe-teorija-brojeva-matematika/361263/`

97

Доказати да је број $20^n + 16^n - 3^n - 1$ дјељив са 323 за сваки паран природан број n.

Доказ. Како је $323 = 17 \cdot 19$, довољно је доказати да је дати израз дјељив са 17 и са 19. Како је n паран број имамо да је $n = 2k$, па је $16^n \equiv (-1)^{2k} \pmod{17} \implies 16^n \equiv 1 \pmod{17} \implies 16^n - 1 \equiv 0 \pmod{17}$. Даље имамо да је $20 \equiv 3 \pmod{17} \implies 20^n \equiv 3^n \pmod{17} \implies 20^n - 3^n \equiv 0 \pmod{17}$. Овим смо доказали да је дати израз дјељив са 17. Остаје нам још да докажемо да је израз дјељив са 19. На сличан начин, као и раније, имамо да је $20^n \equiv 1 \pmod{19} \implies 20^n - 1 \equiv 0 \pmod{19}$. Даље имамо да је $16^n \equiv (-3)^n \pmod{19}$. Пошто је n парно важи да је $16^n \equiv 3^n \pmod{19} \implies 16^n - 3^n \equiv 0 \pmod{19}$. Овим смо доказали да је дати израз дјељив са 19, па пошто је дјељив и са 17 и са 19 важи да је израз дјељив и са бројем 323. $\square$

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.docsity.com/sr/kongruencije-vezbe-teorija-brojeva-matematika/361263/`

98

Наћи последње три цифре збира

$$1^{100} + 2^{100} + ... + 99^{100}$$

Доказ. Посматрајмо бројеве облика $(i10 + j)^{100}$ Имамо да је

$$(i10 + j)^{100} = \sum_{k=0}^{100} \binom{100}{k} (10i)^k j^{100-k} \equiv$$

$$\binom{100}{2} (10i)^2 j^{98} + \binom{100}{1} (10i) j^{99} + j^{100} \equiv j^{100} \pmod{1000}$$

Сада трансформишимо суму $\sum_{k=1}^{99} k^{100}$

$$\sum_{k=1}^{99} k^{100} = \sum_{i=0}^{9} \sum_{j=0}^{9} (i10 + j)^{100} \equiv \sum_{i=0}^{9} \sum_{j=0}^{9} j^{100} \pmod{1000} =$$

$$10 \sum_{j=0}^{9} j^{100} \pmod{1000}$$

Сада можемо да ирачунамо за ових 9 бројева да је сума по мод 1000 једнака 133 па су последе три цифре тражене суме 330 ☐

(**Велибор Дошљак 15/19 Б**) задатак задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

99

Одредити три последње цифре броја $1^{2019} + 2^{2019} + \cdots + 1000^{2019}$

Доказ. Последње три цифре представљају остатак при дијељењу броја са 1000. Очигледно је $1000^{2019} \equiv 0 \pmod{1000}$. Даље, имамо да је и $500^{2019} \equiv 0 \pmod{1000}$. Сада, посматрајмо преостале сабирке датог израза на следећи начин:

- $1^{2019} \equiv 1^{2019} \pmod{1000}$
- $2^{2019} \equiv 2^{2019} \pmod{1000}$

  ...
- $499^{2019} \equiv 499^{2019} \pmod{1000}$
- $501^{2019} \equiv (-499)^{2019} = -499^{2019} \pmod{1000}$

  ...
- $998^{2019} \equiv (-2)^{2019} = -2^{2019} \pmod{1000}$

- $999^{2019} \equiv (-1)^{2019} = -1^{2019} \pmod{1000}$

Из претходно реченог, следи да је:

$1^{2019} + \cdots + 499^{2019} + 500^{2019} + 501^{2019} + \cdots + 998^{2019} + 999^{2019} + 1000^{2019} \equiv 1^{2019} + \cdots + 499^{2019} + 0 - 499^{2019} - \cdots - 2^{2019} - 1^{2019} - 0 = 0 \pmod{1000}$.

Пошто је дати израз дјељив са 1000 без остатка то значи да је троцифрени завршетак 000. ☐

(**Радоман Гледовић 6/19 Ц**)

100

🔴🔴🟡🟡

Одредити последње двије цифре броја $1! + 2! + 3! + \cdots + 2005!$

Доказ. Примјетимо прво да је 10! дјељив са бројем 100 и да 10! дијели 64 $k!$, за сваки природан број k не мањи од 10. Сада су последње двије цифре датог броја једнаке последњим двијема цифрама броја

$$1! + 2! + 3! + 4! + 5! + 6! + 7! + 8! + 9!$$

Даље, сваки од бројева $5!, 6!, 7!, 8!$ и $9!$ су дјељиви са 10, па је последња цифра броја једнака последњој цифри броја $1! + 2! + 3! + 4! = 33$, тј. последња цифра датог броја је 3. Такође, није тешко закључити да је претпоследња цифра датог броја једанка последњој цифри броја

$$\frac{5!+6!+7!+8!+9!}{10} + 3$$

Даље слиједи да је:

$\frac{5!+6!+7!+8!+9!}{10} + 3 = 12 \cdot (1 + 6 + 6 \cdot 7 + 6 \cdot 7 \cdot 8 + 6 \cdot 7 \cdot 8 \cdot 9) + 3 \equiv 2 \cdot (1 + 6 + 2 + 6 + 4) + 3 \pmod{10}$

Даље слиједи да је:

$2 \cdot (1 + 6 + 2 + 6 + 4) + 3 = 41 \equiv 1 \pmod{10}$

Сада је јасно да је двоцифрени завршетак овог броја једнак 13. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

101

🔴🟡🟡🟡

Наћи најмањи природан број n такав да је број: $n + 2$ дјељив са 3, $n + 3$ дјељив са 5, $n + 4$ дјељив са 7.

Доказ. Потребно је да нађемо најмањи природан број n такав да:

$$\begin{aligned} n &\equiv 2 \pmod 3 \\ n &\equiv 3 \pmod 5 \\ n &\equiv 4 \pmod 7 \end{aligned}$$

Користећи кинеску теорему о остацима
Имамо да је $m = 3 \cdot 5 \cdot 7 = 105$, и да су

$$n_1 = 5 \cdot 7 = 35,\ n_2 = 3 \cdot 7 = 21,\ n_3 = 3 \cdot 5 = 15$$

Па добијамо нове три једначине

$$\begin{aligned} 35n \equiv 2 \pmod 3 &\Leftrightarrow 2n \equiv 2 \pmod 3 \\ 21n \equiv 3 \pmod 5 &\Leftrightarrow n \equiv 3 \pmod 5 \\ 15n \equiv 4 \pmod 7 &\Leftrightarrow n \equiv 4 \pmod 7 \end{aligned}$$

Рејешавањем сваке од једначина појединачно дбоијамо

$$x_1 = 1,\ x_2 = 3,\ x_2 = 4$$

Па имамо да је $x_0 = n_1 \cdot x_1 + n_2 \cdot x_2 + n_3 \cdot x_3$, и да су сва рјешења почетне једначине облика $x_0 + t \cdot m$ гдје је t цио број.Тражено n је 58 за $t = -1$.

☐

(**Велибор Дошљак 15/19 Б**) задатак задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

102 ●●●●

Доказати да не постоји природан број n такав да $121 \mid n^2 + 3n + 5$.

Доказ. Неопходан услов за бројеве n које тражимо је да $11 \mid n^2 + 3n + 5$. Разликујемо више случајева:

$$\begin{aligned}
n \equiv 0 \pmod{11} &\implies n^2 + 3n + 5 \equiv 5 \pmod{11} \\
n \equiv 1 \pmod{11} &\implies n^2 + 3n + 5 \equiv 9 \pmod{11} \\
n \equiv 2 \pmod{11} &\implies n^2 + 3n + 5 \equiv 4 \pmod{11} \\
n \equiv 3 \pmod{11} &\implies n^2 + 3n + 5 \equiv 1 \pmod{11} \\
n \equiv 4 \pmod{11} &\implies n^2 + 3n + 5 \equiv 0 \pmod{11} \\
n \equiv 5 \pmod{11} &\implies n^2 + 3n + 5 \equiv 1 \pmod{11} \\
n \equiv 6 \pmod{11} &\implies n^2 + 3n + 5 \equiv 4 \pmod{11} \\
n \equiv 7 \pmod{11} &\implies n^2 + 3n + 5 \equiv 9 \pmod{11} \\
n \equiv 8 \pmod{11} &\implies n^2 + 3n + 5 \equiv 5 \pmod{11} \\
n \equiv 9 \pmod{11} &\implies n^2 + 3n + 5 \equiv 3 \pmod{11} \\
n \equiv 10 \pmod{11} &\implies n^2 + 3n + 5 \equiv 3 \pmod{11}
\end{aligned}$$

Дакле за природне бројеве n који не задовољавају $n \equiv 4 \pmod{11}$ важи да $121 \nmid n^2+3n+9$. Остало је да исто докажемо у случају $n \equiv 4 \pmod{11}$.

Ако $n \equiv 4 \pmod{11} \implies n = 11k+4\,,\ k \in \mathbb{Z}$ и тада је

$$n^2+3n+5 = (11k+4)^2+3(11k+4)+5 = 121k(k+1)+33$$

Одакле закључујемо да $121 \nmid n^2+3n+9$. Тиме смо доказали тврђење задатка. ☐

(**Велимир Ћоровић 5/19 Б**) задатак преузет са
`http://nasport.pmf.ni.ac.rs/materijali/175/Teorija_Brojeva_Vezbe.pdf`

103

●●●●

Нека су x и y природни бројеви такви да је $xy = 2013^{2012}$. Доказати да збир $x+y$ није дјељив са 2012.

Доказ. Број 2012 можемо записати као $2012 = 4 \cdot 503$. Да би број био дјељив са 2012 неопходно је да буде дјељив са 4. Претпоставимо супротно, тј. да је

$$x+y \equiv 0 \pmod{2012}$$

$$(1) \qquad x+y \equiv 0 \pmod{2012} \implies x+y \equiv 0 \pmod{4}$$

Како је $xy = 2013^{2012}$ непаран број, слиједи да су бројеви x и y непарни. Одавде слиједи да је

$$x+1 \equiv 0 \pmod{2}$$

и

$$y+1 \equiv 0 \pmod{2}$$

што значи да је

$$(x+1)(y+1) \equiv 0 \pmod{4} \iff [(xy+1)+(x+y)] \equiv 0 \pmod{4}.$$

Претходни израз еквивалентан је са

$$(2) \qquad [(2013^{2012}+1)+(x+y)] \equiv 0 \pmod{4}.$$

У даљем рјешавању користићемо се наредним својством
Својство: Уколико цијели бројеви a, b и m задовољавају услове $a \equiv 0 \pmod{m}$ и $a+b \equiv 0 \pmod{m}$ онда је $b \equiv 0 \pmod{m}$.

На основу претходног својства, из (1) и (2) слиједи да је

$$2013^{2012}+1 \equiv 0 \pmod{4}.$$

Међутим, како је $2013 \equiv 1 \pmod{4}$, онда је и $2013^{2012} \equiv 1 \pmod{4}$ па слиједи да је

$$2013^{2012}+1 \equiv 2 \pmod{4}$$

што је контрадикција. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`http://www.imvibl.org/dmbl/meso/mat_kol_19_3_2013/mat_kol_19_3_35_44.pdf`

104

●●●●

У години N 300. дан је уторак док је у години $N+1$ 200. дан такође уторак. Који ће дан бити 100. дан године $N-1$?

Доказ. Имамо $65+200=265$ или $66+200=266$ дана између прва два датума у зависности од тога је ли година N преступна или није. Како оба датума падају у уторак мора важити да су датуми конгруенти по модулу 7, тј. да разлика између њих буде дјељива са 7. Пошто $7 \mid 266$ закључујемо да је година N преступна , а онда година $N-1$ није преступна и има 365 дана.

Разлика између датума у години $N-1$ и години N је 565, 565 што није дјељиво са 7 па одговор није уторак.

Посматрајући разлику између 299. дан који је понеђељак у години N и датума у години $N-1$ добијамо да одговор није понеђељак јер 7 не дијели ту разлику. Настављајући тако долазимо до дана 295 године N који је четвртак и разлике 560, како $7 \mid 560$, слиједи да је одговор четвртак. □

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

105

●●●●

Нека је S скуп природних бројева између 1 и 2^{40} који у своjем бинарном запису имају тачно двије јединице. Случајно извлачимо број из скупа S, која је вјероватноћа да је тај број дјељив са 9 ?

Доказ. Природни бројеви између 1 и 2^{40} који имају тачно двије једнинице у бинарном запису су облика 2^a+2^b гдје су a и b различити бројеви из скупа $\{0,1,\ldots,39\}$.

Примјетимо да је $2^6=64\equiv 1 \pmod 9$, одатле закључујемо да степени двојке формирају циклус дужине 6 у модулу 9. Прецизније , за $n\in\mathbb{N}_0$ вриједи

$$2^{6n}\equiv 1 \pmod 9 \qquad 2^{6n+1}\equiv 2 \pmod 9 \qquad 2^{6n+2}\equiv 4 \pmod 9$$

$$2^{6n+3}\equiv 8\equiv -1 \pmod 9 \quad 2^{6n+4}\equiv 16\equiv -2 \pmod 9 \quad 2^{6n+5}\equiv 32\equiv -4 \pmod 9$$

Потребно је изабрати парове (a,b) тако да $2^a+2^b\equiv 0 \pmod 9$, па на основу горње табеле (a,b) морају имати сљедећи облик

$$(6c,6d+3)\ ,\ (6c+1,6d+4)\ ,\ (6c+2,6d+5)$$

Пошто разматрамо само бројеве од 1 до 2^{40}, за први пар нам одговарају могућности $c,d\in\{0,1,\ldots,6\}$ тј. имамо $7\cdot 7=49$ могућности. Слично добијамо да имамо по $6\cdot 7=42$ могућности за други и трећи пар.

Дакле укупно повољних избора имамо $49+42+42=133$. Како бројева између 1 и 2^{40} који имају тачно двије јединице у бинарном запису има $\binom{40}{2}=780$, тражени одговор је $\dfrac{133}{780}$. ☐

(**Велимир Ћоровић 5/19 Б**) задатак преузет са
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

106

●●●●

Нека је $(a_n)_{n\in\mathbb{N}}$ низ природних бројева

$$3, 15, 24, 48, \ldots$$

који се састоји од позитивних умножака броја 3 који су за 1 мањи од потпуног квадрата . Колики се остатак добија када се a_{1994} подјели са 1000?

Доказ. Најприје одредимо општи члан низа $(a_n)_{n\in\mathbb{N}}$. Желимо да $3 \mid (n^2-1) = (n-1)(n+1)$, одатле добијамо да је неопходно да $3 \mid (n-1)$ или $3 \mid (n+1)$ тј. $n=3k+1$ или $n=3k-1$ јер је 3 прост број .

Закључујемо да низ $3k-1$, $k=1,2,\ldots$ генерише бројеве $n=(3k-1)^2-1$ који се налазе на непарним мјестима низа $(a_n)_{n\in\mathbb{N}}$. Такође низ $3k+1$, $k=1,2,\ldots$ генерише бројеве $n=(3k+1)^2-1$ којисе налазе на парним мјестима низа $(a_n)_{n\in\mathbb{N}}$.

Нама је потребан a_{1994} , њега добијамо када ставимо $k=997$ у низу који генерише $3k+1$, $k=1,2,\ldots$. Коначно

$$a_{1997} = ((3\cdot 997)+1)^2-1 \equiv ((3\cdot(-3))+1)^2-1 \equiv 8^2-1 \equiv 63 \pmod{1000}$$

Дакле , тражени остатак је 63 . ☐

(**Велимир Ћоровић 5/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

107

●●●●

За сваки природан број n, број $n+3n^3+7n^7+9n^9$ је дјељив са 10. Доказати.

Доказ. Довољно је доказати да је дати број дјељив са 2 и са 5.
Јасно је да ако је n паран, онда је и $n+3n^3+7n^7+9n^9$ паран. Ако је n непаран сваки од n, $3n^3$, $7n^7$, $9n^9$ непаран па ће збир бити паран. У оба случаја имамо дјељивост са 2.
Ако је n дјељиво са 5, дати број је дјељив са 5. У осталим варијантама, по малој Фермаовој теореми биће $n^5 \equiv n \pmod 5$, па како је нзд$(n,5)=1 \Rightarrow n^4 \equiv 1 \pmod 5$. Тада је:

$$n+3n^3+7n^7+9n^9 \equiv n+3n^3+7n^3+9n \equiv 10n+10n^3 \equiv 0 \pmod 5$$

У сваком случају имамо дјељивост са 5, па важи тврђење.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

108

●●●●

На табли су записани бројеви 1 и 2. Нове бројеве дописујемо на следећи начин: Ако на табли већ постоје различити бројеви a и b можемо да допишемо број $ab - 5a + 7b$. Можемо ли примјеном овог поступка икада записати број: (а) 2020 (б) 2019?

Доказ. (а) Примијетимо да ако су један или оба броја a и b непарни, $ab - 5a + 7b$ биће непаран број. Пошто је на табли само један паран број $ab - 5a + 7b$ биће непаран, односно никада нећемо записати други паран број. Самим тим, ни 2020.

(б) Покажимо да ће сви записани бројеви давати остатак 2 при дијељењу са 3. Заиста, кад год један од бројева a или b даје остатак 2 при дијељењу са 3 тада ће $(a + 7)(b - 5) = ab - 5a + 7b - 35$ бити дјељив са 3. Одавде, $ab - 5a + 7b \equiv 2 \pmod 3$. Пошто је на табли записан један број који даје остатак 2 при дијељењу са 3, а 2019 је дјељив са 3, никада нећемо моћи да запишемо број 2019.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

109

●●●●

Ријешити у скупу простих бројева једначину:

$$x^y - y^x = x \cdot y^2 - 19.$$

Доказ. Примијетимо да је $y^x \equiv 19 \pmod x$ и $x^y \equiv -19 \pmod y$. По малој Фермаовој теореми, пошто су x и y прости бројеви важи да је $y^x \equiv y \pmod x$ и $x^y \equiv x \pmod y$ па је:

$$y - 19 \equiv 0 \pmod x \ \wedge \ x + 19 \equiv 0 \pmod y$$

$$\text{тј. } x \mid y - 19 \ \wedge \ y \mid x + 19 \ \mathbf{(1)}$$

Претпоставимо да је $y \leq 19$. Испробавајући све просте бројеве мање од 19 и користећи **(1)** добијамо да су у овом случају једина могућа решења парови (2,3) и (2,7).

Претпоставимо сада да је $y > 19$. Како $x \mid y - 19 \Rightarrow x \leq y - 19 \Rightarrow x < y$.

$$\Rightarrow 2y > y + 19 > x + 19. \ \mathbf{(2)}$$

Из **(1)** и **(2)** $\Rightarrow y = x + 19$. Одавде закључујемо да су x и y различите парности, а како су по претпоставци прости бројеви, $x = 2$ је једино решење. Међутим, тада је $y = 21$, што није прост број, па за $y > 19$ једначина нема решења.

Дакле, једина решења су парови (2,3) и (2,7).

$\square$

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/` (ВМО 2004)

110

●●●●

Нека су m и n позитивни цијели бројеви и

$$A(m,n) = m^{3^{4n}+6} - m^{3^{4n}+4} - m^5 + m^3.$$

Наћи све бројеве n са својством да је број $A(m,n)$ дјељив са 1992 за свако m.

Доказ. Примијетимо да је $A(m,n) = m^3(m^2-1)(m^{3^{4n}+1}-1)$. Како је $1992 = 8 \cdot 3 \cdot 83$, довољно је наћи n т.д. да је број $A(m,n)$ дјељив са 8, 3 и 83 за свако m.

Како квадрат непарног броја даје остатак 1 при дијељењу са 8 (доказано у 1. поглављу), то онда $m^3(m^2-1)$ је увијек дјељиво са 8. Заиста,

$$\begin{aligned}&\text{m непаран} \Rightarrow m^2 - 1 \equiv 0 \pmod 8\\ &\text{m паран} \Rightarrow m^3 = 8k^3 \Rightarrow m^3 \equiv 0 \pmod 8\end{aligned}$$

Имамо дјељивост $A(m,n)$ са 8, за свако m.

Ако је m дјељиво са 3 онда је и m^3 дјељиво са 3. Са друге стране, како квадрат броја који није дјељив са 3 даје остатак 1 при дијељењу са 3 (лако се показује), важи да је $m^2 - 1$ дјељиво са 3.
Имамо дјељивост $A(m,n)$ са 3, за свако m.

Сада се задатак своди на тражење броја n т.д. је $A(m,n)$ дјељиво са 83 за сваки природан број m.

Посматрајмо $m^{3^{4n}+1} - 1$ и примијетимо да ако је $3^{4n} + 1 \equiv 0 \pmod{82}$ онда је, користећи малу Фермаову теорему, $m^{3^{4n}+1} - 1 \equiv 0 \pmod{83}$. Како је $3^{4n} + 1 = 81^n + 1$ то је онда $3^{4n} + 1 \equiv 0 \pmod{82}$ ако је n паран.

Нека је n непаран. Покажимо да у том случају постоји m за које $A(m,n)$ неће бити дјељиво са 83.
Нека је m такав да $m(m^2-1)$ није дјељив са 83 тј. такав да $m \not\equiv 0 \pmod{83}, m \not\equiv 1 \pmod{83}, m \not\equiv -1 \pmod{83}$. .
Докажимо да тада ни $m^{3^{4n}+1} - 1$ није дјељиво са 83.
За n непарно, $n - 1$ је парно, па по претходном имамо да је:

$$m^{3^{4(n-1)}+1} - 1 \text{ дјељиво са } 83. \ (1)$$

Множећи (1) са m^{81}:

$$m^{3^{4n}+81} - m^{81} \text{ дјељиво са } 83 \ (2)$$

Ако би претпоставили супротно тј. да је $m^{3^{4n}+1} - 1$ дјељиво са 83:

$$m^{3^{4n}+81} - m^{80} \text{ дјељиво са } 83. \ (3)$$

Одузимајући (2) - (3):

$$m^{81} - m^{80} = m^{80}(m-1) \text{ дјељиво са } 83.$$

а то је у контрадикцији са претпоставком да $m(m^2-1)$ није дјељив са 83.

Дакле, ако је n парно, број $A(m,n)$ је дјељив са 1992 за свако m.

$\square$

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/` (ВМО 1991)

111

●●●●

Доказати да је број $2^{157} \cdot 3^{417} - 17^{524} \cdot 11^{704}$ дјељив са 5.

Доказ. Одредимо прво остатак при дијељењу броја 2^{157} са 5. Како је $(2,5)=1$, на основу Ојлерове теореме слиједи да је $2^{\varphi(5)} \equiv 1 \pmod 5$. Имамо:

$$\varphi(5) = 5 \cdot \left(1 - \frac{1}{5}\right) = 4.$$

Добијамо $2^4 \equiv 1 \pmod 5$. Како је $157 = 4 \cdot 39 + 1$, слиједи $(2^4)^{39} \equiv 1 \pmod 5$, односно $2^{157} \equiv 2 \pmod 5$.

Одредимо остатак при дијељењу броја 3^{417} са 5. Како је $(3,5)=1$, слиједи да је $3^{\varphi(5)} \equiv 1 \pmod 5$. Већ смо показали да је $\varphi(5) = 4$, па добијамо $3^4 \equiv 1 \pmod 5$.
Како је $417 = 4 \cdot 104 + 1$ слиједи $(3^4)^{104} \equiv 1 \pmod 5$ односно $3^{417} \equiv 3 \pmod 5$.

Одредимо остатак при дијељењу броја 17^{524} са 5. Како је $(17,5) = 1$, слиједи да је $17^{\varphi(5)} \equiv 1 \pmod 5$. Знамо да је $\varphi(5) = 4$, па добијамо $17^4 \equiv 1 \pmod 5$. Како је $524 = 4 \cdot 131$, слиједи $(17^4)^{131} \equiv 1 \pmod 5$.

Одредимо остатак при дијељењу броја 11^{704} са 5. Како је $(11,5) = 1$ слиједи да је $11^{\varphi(5)} \equiv 1 \pmod 5$. Знамо да је $\varphi(5) = 4$ па добијамо $11^4 \equiv 1 \pmod 5$. Како је $704 = 4 \cdot 176$, слиједи $(11^4)^{176} \equiv 1 \pmod 5$.

Дакле, $2^{157} \cdot 3^{417} - 17^{524} \cdot 11^{704} \equiv 2 \cdot 3 - 1 \cdot 1 \pmod 5$, односно $2^{157} \cdot 3^{417} - 17^{524} \cdot 11^{704} \equiv 0 \pmod 5$.

$\square$

(**Невена Гиговић 1/19 Ц**) задатак преузет са `https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf`

112

Нека су a и b природни бројеви. Ако је $(a, 65) = 1$ и $(b, 65) = 1$, доказати да $65 \mid a^{12} - b^{12}$.

Доказ. Важи $65 = 5 \cdot 13$. Пошто је $(a, 65) = 1$ и $(b, 65) = 1$, слиједи $(a, 5) = 1$, $(a, 13) = 1$, $(b, 5) = 1$ и $(b, 13) = 1$. Важи и $\varphi(5) = 4$ и $\varphi(13) = 12$.

Како је $(a, 5) = 1$, на основу Ојлерове теореме је $a^{\varphi(5)} \equiv 1 \pmod 5$. Добијамо $a^4 \equiv 1 \pmod 5$, па је $(a^4)^3 \equiv 1 \pmod 5$, односно $a^{12} \equiv 1 \pmod 5$.

Како је $(b, 5) = 1$, на основу Ојлерове теореме је $b^{\varphi(5)} \equiv 1 \pmod 5$. Добијамо $b^4 \equiv 1 \pmod 5$, па је $(b^4)^3 \equiv 1 \pmod 5$, односно $b^{12} \equiv 1 \pmod 5$.

Дакле, $a^{12} - b^{12} \equiv 1 - 1 \pmod 5$, односно $a^{12} - b^{12} \equiv 0 \pmod 5$.

Како је $(a, 13) = 1$, на основу Ојлерове теореме је $a^{\varphi(13)} \equiv 1 \pmod{13}$. Добијамо $a^{12} \equiv 1 \pmod{13}$.

Како је $(b, 13) = 1$, на основу Ојлерове теореме је $b^{\varphi(13)} \equiv 1 \pmod{13}$. Добијамо $b^{12} \equiv 1 \pmod{13}$.

Дакле, $a^{12} - b^{12} \equiv 1 - 1 \pmod{13}$, односно $a^{12} - b^{12} \equiv 0 \pmod{13}$.

Како је $a^{12} - b^{12} \equiv 0 \pmod 5$ и $a^{12} - b^{12} \equiv 0 \pmod{13}$ и $(5, 13) = 1$, слиједи $a^{12} - b^{12} \equiv 0 \pmod{65}$. □

(**Невена Гиговић 1/19 Ц**) задатак преузет са `https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf`

113

Показати да је $2^{n-1} \equiv 1 \pmod n$ за $n = 73 \cdot 37$.

Доказ. Како су 73 и 37 прости бројеви и $73 \nmid 2$ и $37 \nmid 2$, на основу мале Фермаове теореме је $2^{72} \equiv 1 \pmod{73}$ и $2^{36} \equiv 1 \pmod{37}$.

Тада добијамо $2^{72} \equiv (2^{36})^2 \equiv 1^2 \equiv 1 \pmod{37}$. Сада је $2^{72} \equiv 1 \pmod{73}$ и $2^{72} \equiv 1 \pmod{37}$, одакле добијамо $2^{72} \equiv 1 \pmod{73 \cdot 37}$, па је и $2^{72 \cdot 37} \equiv 1^{37} \pmod{73 \cdot 37}$. Дакле,

$$2^{n-1} = 2^{73 \cdot 37 - 1} = 2^{72 \cdot 37 + 37 - 1} = 2^{72 \cdot 37} \cdot 2^{36} \equiv 1 \cdot 2^{36} \equiv 1 \pmod{73 \cdot 37}.$$

□

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf`

114

Ако је p прост број, доказати да $p^3 \mid (p!)^2 - p^2$.

Доказ.

$$\begin{aligned}(p!)^2 - p^2 &= (p! - p)(p! + p)\\ &= ((p-1)! \cdot p - p)((p-1)! \cdot p + p)\\ &= p^2((p-1)! - 1)((p-1)! + 1).\end{aligned}$$

На основу Вилсонове теореме знамо да је $(p-1)! \equiv -1 \pmod p$.
Из чињенице да је $(p-1)! - 1 \equiv -2 \pmod p$ и $(p-1)! + 1 \equiv 0 \pmod p$ слиједи да

$$((p-1)! - 1)((p-1)! + 1) \equiv (-2) \cdot 0 \equiv 0 \pmod p.$$

Такође, из $p \mid ((p-1)! - 1)((p-1)! + 1)$ и $p^2 \mid p^2$ слиједи да

$$p^3 \mid ((p-1)! - 1)((p-1)! + 1)$$

чиме смо доказ завршили. □

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf`

115

У соби се налазе столице са 3 и са 4 ноге, када на све столице сједу људи у соби је укупно 69 ногу. Колико има столица са 3 ноге, а колико са 4 ноге?

Доказ. Са x означимо број столица са 3 ноге, а са y столице са 4 ноге. Како сваки човјек има двије ноге, једначину можемо поставити као:

$$3x + 4y + 2(x + y) = 69.$$

Сређивањем добијамо

$$5x + 6y = 69.$$

Како $3 \mid 69$ и $3 \mid 6y$ закључујемо да $3 \mid 5x$. Знамо да је $(3,5) = 1$, па $3 \mid x$, одакле је $x = 3k$, $k \in \mathbb{N}$. Замјеном у једначини добијамо $5 \cdot 3k + 6y = 69$, скраћивањем са 3 добијамо, $5k + 2y = 23$ тј. $5k = 23 - 2y$, одакле се очигледно види да $5k \in \{0, 5, 10, 15, 20\}$. Размотримо све могуће случајеве:

- $5k = 0$
  Одакле је $k = 0$, па је $x = 0$, а $y = \frac{23}{2}$, што је немогуће.

- $5k = 5$
  Одакле је $k = 1$, па је $x = 3$, а $y = 9$. Дакле, прво решење ће бити 3 столице са 3 ноге и 9 столица са 4 ноге.

- $5k = 10$
  Одакле је $k = 2$, па је $x = 6$, а $y = \frac{13}{2}$, што је немогуће.

- $5k = 15$
  Одакле је $k = 3$, па је $x = 9$, а $y = 4$. Дакле, друго решење ће бити 9 столица са 3 ноге и 4 столице са 4 ноге.

- $5k = 20$
  Одакле је $k = 4$, па је $x = 12$, а $y = \frac{3}{2}$, што је немогуће.

Дакле, добили смо два решења:
1) 3 столице са 3 ноге и 9 столица са 4 ноге
2) 9 столица са 3 ноге и 4 столице са 4 ноге.

□

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf`

116
●●●●

Посматрајмо све парове природних бројева (m, n), $m < n$, са особином да се последње три цифре у декадном запису бројева 1978^m и 1978^n поклапају. Наћи све такве парове (m, n) за које је $m + n$ минимално.

Доказ. Услов задатка можемо записати као

$$1978^m(1978^{n-m} - 1) = 1000q = 2^3 5^3 q,$$

за неко $q \geq 1$, одакле добијамо $8 \mid 1978^m$ и $125 \mid (1978^{n-m} - 1)$. Како је $1978 = 2 \cdot 989$, то први услов даје $m \geq 3$. Из другог услова имамо:

$$1 \equiv 1978^{n-m} \equiv (-2)^{n-m} \pmod 5,$$

што је могуће само ако је $n - m = 4k$ за неки природан број k. Преостаје да одредимо најмањи природан број k за који је $1978^{4k} - 1$ дјељиво са 125. Непосредно добијамо

$$1978^4 \equiv 6 \pmod{125},$$

па се посматрани услов своди на

$$6^k \equiv 1 \pmod{125}.$$

Из Ојлерове теореме слиједи

$$6^{100} = 6^{\varphi(125)} \equiv 1 \pmod{125}.$$

Како је $6^{100} - 1 = (6^{50} - 1)(6^{50} + 1)$ и последња цифра броја $6^{50} + 1$ је 7, слиједи да $125 \mid (6^{50} - 1)$. Понављајући овај аргумент још једном у односу на $6^{50} - 1 = (6^{25} - 1)(6^{25} + 1)$, добијамо да $125 \mid (6^{25} - 1)$. Због тога, најмање k за које $125 \mid (6^k - 1)$ задовољава $k \mid 25$, тј. $k \in \{1, 5, 25\}$. Директно провјеравамо да $6^5 - 1$ није дјељиво са 125(као ни $6^1 - 1$). Стога је $k = 25$ најмањи број са траженом особином, па је сума $m + n$ минимална за $n = 103$, $m = 3$. □

(**Невена Гиговић 1/19 Ц**) задатак преузет из
Елементарна теорија бројева Игор Долинка

117

Наћи све природне бројеве n за које постоји пермутација $(p_1, \ldots, p_n)$ бројева $(1, ..., n)$ таква да скупови $\{p_i + i \mid 1 \le i \le n\}$ и $\{p_i - i \mid 1 \le i \le n\}$ чине потпун систем остатака по модулу n.

Доказ. Претпоставимо да таква пермутација постоји. Како је $\{p_i + i \mid 1 \le i \le n\}$ потпун систем остатака по модулу n и $(p_1, \ldots, p_n)$ пермутација бројева $(1, ..., n)$ онда је:

$$\sum_{k=1}^{n} k \equiv \sum_{i=1}^{n} (p_i + i) \equiv \sum_{i=1}^{n} p_i + \sum_{i=1}^{n} i \equiv 2 \cdot \sum_{k=1}^{n} k \pmod{n}$$

Одавде је:

$$\sum_{k=1}^{n} k = \frac{n(n+1)}{2} \equiv 0 \pmod{n} \Rightarrow 2 \nmid n$$

Штавише, важи да је:

$$2\sum_{k=1}^{n} k^2 \equiv \sum_{k=1}^{n} (p_i + i)^2 + \sum_{k=1}^{n} (p_i - i)^2 \equiv \sum_{i=1}^{n} 2{p_i}^2 + 2i^2 \equiv 4\sum_{k=1}^{n} k^2 \pmod{n}$$

Одавде је:

$$2\sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{3} \equiv 0 \pmod{n} \Rightarrow 3 \nmid n$$

Дакле, то су сви природни бројеви n такви да $6 \nmid n$.
Дакле, ако је нзд$(n, 6) = 1$ и $p_i - i \equiv i \pmod{n}$ тј. $p_i \equiv 2i \pmod{n}$, $p_i \in \{1, 2, \ldots, n\}$ тада је $(p_1, \ldots, p_n)$ пермутација скупа $(1, \ldots, n)$ и задовољава услове јер су $\{p_i + i \mid 1 \le i \le n\} \equiv \{3i \mid 1 \le i \le n\}$ и $\{p_i - i \mid 1 \le i \le n\} \equiv \{i \mid 1 \le i \le n\} \pmod{n}$ потпуни системи остатака по модулу n.
Заиста, да покажемо да је $\{3i \mid 1 \le i \le n\}$ потпун систем остатака по модулу n, претпоставимо супротно тј. да постоје $i, j \in \{1, 2, \ldots, n\}$ такви да $3i \equiv 3j \pmod{n}$ тј. $i \equiv j \pmod{\frac{n}{\text{нзд}(n,3)}}$. Одавде, јер је нзд$(n, 3) = 1$ добијамо $i \equiv j \pmod{n}$. Међутим, то је немогуће јер је $\{1, 2, \ldots, n\}$ потпун систем остатака по модулу n. Овим је доказ завршен.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

118

Странице једне књиге нумерисане су бројевима од 1 до 100 на уобичајен начин. Из књиге је истргнут извјестан број листова и при томе се испоставило да збир бројева којим су нумерисане истргнуте странице износи 4949. Колико листова је истргнуто?

Доказ. Сваки лист нумерисан је бројевима $2n-1$ и $2n$ за неко $1 \leqslant n \leqslant 50$.
Њихов збир је $4n-1$. Обиљежимо са k број листова који су остали. Тада је
$(4n_1-1)+(4n_2-1)+\ldots+(4n_k-1)=(1+2+\ldots+100)-4949$,
односно $4(n_1+n_2+n_k)-k=100$.
Обзиром на то да је $101 \equiv 1 \pmod 4$, то је $k \equiv 3 \pmod 4$.
Дакле, $k \in \{1,2,3,\ldots,97\}$.
Како је $4(n_1+n_2+n_k)-k \geq 105 > 101$ за $k \geq 7$, остаје $k=7$.
То је могуће,јер је на примјер збир бројева којима су нумерисане странице првог,другог и 23. листа,$(1,2)$, $(3,4)$,$(45,46)$ управо 101.
Дакле,остала су 3 листа, тј. истргнуто је 47 листова. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

119

Дат је низ бројева $mp+1, mp^3+1, mp^5+1, \ldots$ гдје је p прост, а m природан број.
(а) Доказати да се у овом низу налази највише један потпун квадрат.
(б) Да ли се у овом низу мора налазити потпун квадрат?

Доказ. (а) Претпоставимо да дати низ садржи барем два потпуна квадрата и нека је

$$mp^k+1=a^2 \quad \wedge \quad mp^l+1=b^2$$

гдје је $k<l$, а a,b природни бројеви. Из ових једнакости добијамо:

$$(a^2-1)p^{2s}=b^2-1=(b-1)(b+1) \ \ (*)$$

гдје је $l-k=2s$. Како је нзд$(b-1,b+1)$ или 1 или 2 (у зависности од тога да ли је b паран или непаран број), разликујемо случајеве:

1) $p \neq 2 \Rightarrow p^{2s} \mid b-1 \ \vee p^{2s} \ \mid b+1$
2) $p=2 \Rightarrow 2 \mid a^2-1 \Rightarrow 2^{2s} \mid b-1 \ \vee \ 2^{2s} \mid b+1$ Самим тим, у оба случаја мора бити $b+1 \geq p^{2s}$.
Једнакост (*) може се даље записати као:

$$a^2p^{2s}-b^2=p^{2s}-1 \Leftrightarrow (ap^s-b)(ap^s+b)=p^{2s}-1$$

па $ap^s + b \mid p^{2s} - 1$. Међутим, $ap^s + b > b \geq p^{2s} - 1$ што је контрадикција. Дакле, у датом низу налази се највише један потпун квадрат.

(б) Не. Нека је $p = 2$ и $m = 2$. Како је $2 \cdot 2^{2k+1} + 1 \equiv 2 \pmod 3$ то сваки члан низа даје остатак 2 при дијељењу са 3, па не може бити потпун квадрат (потпуни квадрати дају остатак 0 или 1 при дијељењу са 3).

☐

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

120 ●●●●

Наћи најмањи позитивни цијели број такав да када се подијели са $3, 5, 7$, добијемо остатке $1, 4, 6$ редом.

Доказ. Нека је x тражени број.
Добијамо систем конгруенција.

$$x \equiv 1 \pmod 3 \tag{2.1}$$
$$x \equiv 4 \pmod 5 \tag{2.2}$$
$$x \equiv 6 \pmod 7 \tag{2.3}$$

$(1) \implies x = 3k + 1, \quad k \in \mathbb{Z}$
Убацимо у (2)

$$\begin{aligned} 3k + 1 &\equiv 4 \pmod 5 \\ 3k &\equiv 3 \pmod 5 \\ k &\equiv 1 \pmod 5 \\ k &= 5l + 1, \quad l \in \mathbb{Z} \end{aligned}$$

$\implies x = 3(5l + 1) + 1 = 15l + 4$
Сада ово убацимо у (3)

$$\begin{aligned} 15l + 4 &\equiv 6 \pmod 7 \\ 15l &\equiv 2 \pmod 7 \\ l &\equiv 2 \pmod 7 \\ l &= 7m + 2, \quad m \in \mathbb{Z} \end{aligned}$$

$\implies x = 15(7m + 2) + 4 = 105m + 34$
x је најмање када је $m = 0$ па слиједи да је тражено решење 34.
(**Милена Јововић 1/19 Б**)задатак преузет са
`https://www.youtube.com/watch?v=LInNgWMtFEs`

☐

121

Доказати да је број $2222^{5555} + 5555^{2222}$ дјељив са 7.

Доказ. Како $2222 \equiv 3 \pmod 7$, $3^6 \equiv 1 \pmod 7$, $5555 \equiv 5 \pmod 6$

$$\begin{aligned} \Longrightarrow \quad 2222^{5555} &= 2222^{6\cdot925+5} = (2222^6)^{925} \cdot 2222^5 \equiv \\ &\equiv (3^6)^{925} \cdot 3^5 \equiv 1 \cdot 3^5 \equiv 5 \pmod 7 \end{aligned}$$

Слично, из $5555 \equiv 4 \pmod 7$, $4^3 \equiv 1 \pmod 7$, $2222 \equiv 2 \pmod 3$

$$\begin{aligned} \Longrightarrow \quad 5555^{2222} &= 5555^{3\cdot740+2} = (5555^3)^{740} \cdot 5555^2 \equiv \\ &\equiv (4^3)^{740} \cdot 4^2 \equiv 1 \cdot 4^2 \equiv 2 \pmod 7 \end{aligned}$$

Сада можемо да видимо да

$$2222^{5555} + 5555^{2222} \equiv 5 + 2 \pmod 7$$

☐

(**Милена Јовović 1/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

122

Доказати да ако важи $a \equiv b \pmod n$, да онда за свако $e > 0$, $e \mid a$, $e \mid b$, $e \in \mathbb{Z}$ важи

$$\frac{a}{e} = \frac{b}{e} \pmod{\frac{n}{\text{нзд}(n,e)}}$$

Доказ. Нека је $a = ce$, $b = de$ за неко $c, d \in \mathbb{Z}$
Онда,

$$\begin{aligned} a \equiv b \pmod n \quad &\Longrightarrow \quad a - b = mn \\ &\Longrightarrow \quad ce - de = mn \\ &\Longrightarrow \quad (c-d)e - mn = 0 \\ &\Longrightarrow \quad (c-d)\frac{e}{\text{нзд}(n,e)} + (-m)\frac{n}{\text{нзд}(n,e)} = 0 \end{aligned}$$

Како су $\frac{e}{\text{нзд}(n,e)}$ и $\frac{n}{\text{нзд}(n,e)}$ релативно прости, коефицијент једног је садржалац другог и обрнуто. Дакле,
$(c-d)$ је садржалац од $\frac{n}{\text{нзд}(n,e)}$, тј.

$$\begin{aligned} c - d \equiv 0 \pmod{\frac{n}{\text{нзд}(n,e)}} \Longrightarrow c &\equiv d \pmod{\frac{n}{\text{нзд}(n,e)}} \\ \frac{a}{e} &\equiv \frac{b}{e} \pmod{\frac{n}{\text{нзд}(n,e)}} \end{aligned}$$

□

(**Милена Јововић 1/19 Б**) задатак преузет са
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-13-15-solutions.pdf`

123
●●●●

Нека је

$$n!! = n!(\frac{1}{2!} - \frac{1}{3!} + ... + \frac{(-1)^n}{n!})$$

Доказати да за сваки природан број $n,\ n > 3$

$$n!! \equiv n! \pmod{(n-1)}$$

Доказ.

$$\begin{aligned} n! - n!! &= n! - n!(\frac{1}{2!} - \frac{1}{3!} + ... + \frac{(-1)^n}{n!}) = \\ &= n!(1 - \frac{1}{2!} + \frac{1}{3!} + ... + \frac{(-1)^{n-1}}{(n-1)!} + \frac{(-1)^n}{n!}) = \\ &= n(n-1)(n-2)!(1 - \frac{1}{2!} + \frac{1}{3!} + ... + \frac{(-1)^{n-1}}{(n-1)!} + \frac{(-1)^n}{n!}) = \\ &= (n-1)(m + \frac{(-1)^{n-1}n}{n-1} + \frac{(-1)^n}{n-1}) = \\ &= (n-1)(m + (-1)^{n-1}) \end{aligned}$$

гдје m представља неки цијели број јер $(n-2)!$ је дјељиво са $k!,\ k \le n-2$. □

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

124
●●●●

(2002 Руска математичка олимпијада) Наћи најмањи позитивни цијели број који може бити записан на оба начина:
(1) као сума 2002 позитивних цијелих бројева (не морају обавезно бити сви бројеви различити) таквих да сви бројеви имају једнаку суму цифара
(2) као сума 2003 позитивних цијелих бројева (не морају обавезно бити сви бројеви различити) таквих да сви бројеви имају једнаку суму цифара

Доказ. Тражени број је 10010. Покажимо да је заиста тако.
$10010 = 2002 \cdot 5$ (1)
$10010 = 1781 \cdot 4 + 222 \cdot 13$ (2)
Видимо да $4 = 1 + 3$ и $1781 + 222 = 2003$ па је у потпуности испуњен и други услов у

једнакости (2).
Дакле, број 10010 можемо записати као суму 2002 петица или као суму 1781 четворки и 222 тринаестица.
Желимо да покажемо да је то заиста најмањи позитивни цијели број који задовољава наведене услове.
Посматрајмо да је неки број конгруентан по $\mod 9$ суми својих цифара па 2 позитивна цијела броја са једнаком сумом цифара припадају истој класи остатака по $\mod 9$. Нека је:
k_1 =сума цифара од 2002 бројева
k_2 =сума цифара од 2003 бројева
Онда, $4k_1 \equiv 2002k_1 \equiv 2003k_2 \equiv 5k_2 \pmod 9$
Ако је $k_1 \geq 5$, онда сума 2002 бројева износи бар 10010.
Ако је $k_2 \geq 5$, онда сума 2003 бројева је већа од 10010.
Међутим, решења $k_1 \equiv 1, 2, 3, 4 \pmod 9$ дају $k_2 \equiv 8, 7, 6, 5$ редом из чега видимо да у пару (k_1, k_2) једна од тих вриједности је већа или једнака 5 што нас доводи до закључка да је 10010 заиста најмањи цијели број који задовољава наведене услове задатка.

☐

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

125 ●●●●

Доказати да је за сваки цијели број n број $n^3 + 11n$ дјељив са 6.

Доказ. Раставимо $n^3 + 11n$ на сљедећи начин:

$$n^3 + 11n = n^3 - n + 12n.$$

Сабирак $12n$ је дјељив са 6, па остаје да докажемо да је $n^3 - n$ дјељиво са 6.

$$n^3 - n = n(n^2 - 1) = n(n-1)(n+1) = (n-1)n(n+1)$$

Видимо да је $n^3 - n$ производ три узастопна цијела броја, па је према томе дјељив са 6. Тиме смо доказали да је израз $n^3 + 11n$ дјељив са 6, за свако $n \in Z$. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`https://element.hr/artikli/file/3351/mmb-3-elementarna-teorija-brojeva/15013`

126 ●●●●

Да ли је $232^{554} + 554^{232} + 5$ дјељиво са 7?

Доказ. Да би ова сума била дјељива са 7, потребно је да збир остатака при дијељењу свих сабирака са 7 буде такође дјељив са 7. Да бисмо лакше урадили задатак, користићемо малу

Фермаову теорему, која гласи:
За свако $a \in Z$ и p-прост број, важи:

$$a^{p-1} \equiv 1 \pmod p$$

Због тога је:

$$232^{7-1} \equiv 1 \pmod 7$$

$$232^{6} \equiv 1 \pmod 7$$

Треба да нађемо остатак сваког сабирка при дијељењу са 7. Тражимо остатак при дијељењу броја 232^{554} са 7. Користићемо својства модуларне аритметике:

$$\underbrace{232^6 \cdots 232^6}_{92} \equiv \underbrace{1 \cdots 1}_{92} \pmod 7$$

$$232^{552} \equiv 1 \pmod 7$$

Остатак при дијељењу 232 са 7 је 1, па је онда и

$$232^{2} \equiv 1 \pmod 7.$$

И коначно имамо:

$$232^{552} \cdot 232^{2} \equiv 1 \cdot 1 \pmod 7$$

$$232^{554} \equiv 1 \pmod 7.$$

Сада ћемо наћи остатак при дијељењу 554^{232} са 7.

$$\underbrace{554^6 \cdots 554^6}_{38} \equiv \underbrace{1 \cdots 1}_{38} \pmod 7$$

$$554^{228} \equiv 1 \pmod 7$$

Јасно је да:

$$554^{4} \equiv 1 \pmod 7,$$

па је:

$$554^{232} \equiv 1 \pmod 7.$$

Дакле, остаци прва два сабирка при дијељењу са 7 су 1, а остатак трећег сабирка (5) при дијељењу са 7 је 5, па је збир остатака једнак 7, што јесте дјељиво са 7. Закључујемо да је сума дјељива са 7. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
Збирка задатака из математике за студенте учитељских студија

127

Доказати да важи

$$n \equiv 1 \pmod 2 \implies (n^2 \equiv 1 \pmod 8) \iff 8 \mid n^2 - 1).$$

Доказ. Како је остатак при дијељењу броја n са 2 једнак 1, то значи да је он непаран, па се може записати у облику $n = 2q + 1$. Даље је

$$n^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1$$

Пошто је тачно један од бројева q и $q + 1$ дјељив са 2 (узастопни бројеви), то значи да је:

$$n^2 = 8r + 1.$$

Одатле је квадрат било ког непарног броја конгруентан са 1 по модулу 8. Ова чињеница се често користи у задацима. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

128

Збир цифара броја 9^{2011} је a. Збир цифара броја a једнак је b, збир цифара броја b једнак је броју c. Одредити број c.

Доказ. Број 9^{2011} је дјељив са 9 и његов збир цифара a је број који је дјељив са 9,при чему је $a < 2011 \cdot 9 = 18099$. Како је a петоцифрен број, његов збир цифара $b < 1+8+9+9+9 = 36$.Како је b, као збир цифара броја a, такође дјељив са 9, то је b један од бројева 27,18 или 9. Тада је број c као збир цифара броја b у сваком случају једнак $2 + 7 = 1 + 8 = 9$.. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`https://informatematika.weebly.com/uploads/2/6/6/2/26628539/kongruencije-po-modulu.pdf`

129

Извести правило за дјељивост цијелог броја са: а) 9; б) 11 .

Доказ. а) Природан број M написан у децималном систему има облик:

$$M = a_0 + 10a_1 + ... + 10^n a_n,$$

гдје су a_i цифре, за свако i. Сабирањем релација

$$a_0 \equiv a_0 \pmod 9, 10a_1 \equiv a_1 \pmod 9, ..., 10^n a_n \equiv a_n \pmod 9$$

добијамо $M \equiv (a_0 + a_1 + ... + a_n) \pmod 9$.
Значи да је број дјељив са 9 ако и само ако је збир цифара тог броја дјељив са 9.
б) Како је $M \equiv -1 \pmod{11}$, имамо да је:

$$10^2 \equiv 1 \pmod{11}, 10^3 \equiv -1 \pmod{11}, ..., 10^n \equiv (-1)^n \pmod{11}$$

Број M је представљен у облику:

$$M = a_0 + 10a_1 + ... + 10^n a_n.$$

Нека је

$$Q = a_0 - a_1 + ... + (-1)^n a_n$$

Тада је

$$M - Q = (10 + 1)a_1 + ... + (10^{n-1} - (-1)^{n-1})a_{n-1} + (10^n - (-1)^n)a_n$$

С обзиром да је $10^k - (-1)^k \equiv 0 \pmod{11}$, закључујемо да је

$$M - Q \equiv 0 \pmod{11},$$

што значи да је број M дјељив са 11 ако и само ако је и број Q дјељив са 11.
Дакле, правило гласи: ако је дат природан број M, израчунати збир његових цифара, са наизмјеничним знацима $+$, -, и то полазећи од цифре јединица ка цифри највеће тежине. Ако је такав број дјељив са 11, онда је и M дјељив са 11. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

130

Доказати:
а) Ако је a цијели број који није дјељив са 7, тада је $a^{12} \equiv 1 \pmod 7$.
б) Нека су a и b цијели бројеви који нису дјељиви ни са 5 ни са 13. Показати да тада важи $a^{12} - b^{12} \equiv 0 \pmod{65}$.

Доказ. а) По Малој Фермаовој теореми $a^6 \equiv 1 \pmod 7$, па је и $a^{12} \equiv 1 \pmod 7$.
б) Како је $a^{12} \equiv b^{12} \equiv 1 \pmod{13}$ и $a^4 \equiv b^4 \equiv 1 \pmod 5$, то је и $a^{12} \equiv b^{12} \equiv 1 \pmod 5$. Пошто су 5 и 13 узајамно прости, то је $a^{12} \equiv b^{12} \equiv 1 \pmod{65}$, тј. $a^{12} - b^{12} \equiv 0 \pmod{65}$. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

131

Мала Фермаова теорема. Нека је $a \in N$ и p-прост број. Тада важи:

$$a^p \equiv a \pmod p$$

У случају да су a и p узајамно прости бројеви, важи:

$$a^{p-1} \equiv 1 \pmod p.$$

Доказ. Из $c_i \equiv d_i \pmod{p}, i = 1, 2, ..., n$ слиједи $c_1 c_2 ... c_n \equiv d_1 d_2 ... d_n \pmod{p}$.
Нека је нзд$(a, p) = 1$. Формирамо низ:
$a, 2a, 3a, ..., (p-1)a$.
Никоја два елемента овог низа нису међусобно конгруентна по модулу p зато што за произвољне $1 \leq i,\ k \leq p-1$ важи:

$$ia \equiv ka \pmod{p} \implies i \equiv k \pmod{p} \implies i = k.$$

Има $p-1$ чланова формираног низа и сви дају различите остатке при дијељењу са p. Притом, сви ти бројеви су узајамно прости са p, зато што нзд$(a, p) = 1$ и нзд$(i, p) = 1$ за свако $1 \leq i \leq p-1$. Одатле закључујемо да је сваки од бројева из формираног низа конгруентан са тачно једним бројем из низа $1, 2, ..., p-1$. Када примијенимо својство наведено на почетку доказа, добија се:

$$a^{p-1} \cdot 1 \cdot 2 \cdots (p-1) \equiv 1 \cdot 2 \cdots (p-1) \pmod{p},$$

а пошто је нзд$((p-1)!, p) = 1$, примијенимо правило "скраћивања"и добија се

$$a^{p-1} \equiv 1 \pmod{p}$$

□

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

132

Нека су $x_1, x_2, \ldots, x_{2014}$ природни бројеви за које важи да је

$$\sum_{i=1}^{2013} x_i^2 = x_{2014}^2.$$

Доказати да су бар два од тих бројева парна.

Доказ. Претпоставимо да су сви бројеви непарни. Ако је n непаран број, $n = 2k+1$, онда је $n^2 = 4k(k+1) + 1 \equiv 1 \pmod{8}$, јер је један од бројева k и $k+1$ сигурно паран. Зато је $x_{2014}^2 \equiv 1 \pmod{8}$.

С друге стране имамо да је

$$\sum_{i=1}^{2013} x_i^2 \equiv 5 \pmod{8},$$

што је контрадикција.

Претпоставимо да је тачно један од датих бројева паран. Ако је то x_{2014}, онда је сваки од бројева $x_1, x_2, \ldots, x_{2013}$ непаран. Слиједи да је непаран и збир њихових квадрата, што је контрадикција.

Ако је неки од бројева $x_1, x_2, \ldots, x_{2013}$ паран, рецимо x_1, онда је паран и број x_1^2 једнак броју

$$x_{2014}^2 - \sum_{i=2}^{2013} x_i^2,$$

који је очигледно непаран, што је контрадикција.

Из претходног слиједи да међу бројевима, који задовољавају услов задатка, морају бити барем два парна броја.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са `https://www.pmf.ni.ac.rs/mii-content/2014/Broj%202014%20u%20zanimljivim%20zadacima.pdf`

133

Доказати да је број $2222^{5555} + 5555^{2222}$ дјељив са 3.

Доказ. Знамо да је:

$$2222 \equiv 2 \pmod 3 2222^{5555} \equiv 2^{5555} \pmod 3$$

Како је $2^2 = 4 \equiv 1 \pmod 3$ то је:

$$2^{5555} = (2^2)^{2777} \cdot 2 \equiv 1 \cdot 2 = 2 \pmod 3$$

Слично,

$$\begin{gathered} 5555 \equiv 2 \pmod 3 \\ 5555^{2222} \equiv 2^{2222} \pmod 3 \\ 2^2 = 4 \equiv 1 \pmod 3 \\ 2^{2222} \equiv (2^2)^{1111} \equiv 1 \pmod 3 \\ 2222^{5555} + 5555^{2222} \equiv 2 + 1 = 0 \pmod 3 \end{gathered}$$

Како нема остатака при дијељењу $2222^{5555}+5555^{2222}$ са 3 слиједи да је број $2222^{5555}+5555^{2222}$ дјељив са 3.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

134

Доказати да $13 \mid 2^{70} + 3^{70}$.

Доказ. Како је нзд$(2, 13) = 1$, по Малој Фермаовој теореми имамо да важи $2^{12} \equiv 1 \pmod{13}$,

$$70 = 12 \cdot 5 + 10,$$
$$2^{70} \equiv (2^{12})^5 \cdot 2^{10} \pmod{13},$$

па је

$$2^{70} \equiv 2^{10} \pmod{13},$$
$$2^{10} = 1024,$$
$$1024 \equiv -3 \pmod{13},$$

одакле слиједи да је

$$2^{70} \equiv -3 \pmod{13}.$$

Како је нзд$(3, 13) = 1$, по Малој Фермаовој теореми је $3^{12} \equiv 1 \pmod 3$,

$$70 = 12 \cdot 5 + 10,$$

па је

$$3^{70} \equiv (3^{12})^5 \cdot 3^{10} \pmod{13},$$

слиједи

$$3^{70} \equiv 3^{10} \pmod{13},$$
$$3^3 \equiv 1 \pmod{13}$$
$$3^{10} \equiv (3^3)^3 \cdot 3 \pmod{13},$$

тј.

$$3^{10} \equiv 3 \pmod{13},$$
$$2^{70} + 3^{70} \equiv 0 \pmod{13}.$$

Дакле, $13 \mid 2^{70} + 3^{70}$.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

135

Ојлеровом методом ријешити конгруенције:

(а) $5x \equiv 4 \pmod{12}$
(б) $3x \equiv 5 \pmod{10}$

Доказ. (а) Како је нзд$(5, 12) = 1$, а $1 \mid 4$, наша конгруенција има јединствено рјешење. Ако искористимо Ојлерову теорему добијамо

$$\begin{aligned} x &\equiv 5^{\varphi(12)-1} \cdot 4 \pmod{12} \\ &\equiv 5^{4-1} \cdot 4 \pmod{12} \\ &\equiv 5^3 \cdot 4 \pmod{12} \\ &\equiv 5 \cdot 4 \pmod{12} \\ &\equiv 20 \pmod{12} \\ &\equiv 8 \pmod{12} \end{aligned}$$

Дакле, рјешење почетне конгруенције је $x \equiv 8 \pmod{12}$.

(б) Како је нзд$(3, 10) = 1$, а 1 је дјелилац броја 5, па наша почетна конгруенција има јединствено рјешење. Као и под (а) искористимо Ојлерову теорему и добијамо

$$\begin{aligned} x &\equiv 3^{\varphi(10)-1} \cdot 5 \pmod{10} \\ &\equiv 3^{4-1} \cdot 5 \pmod{10} \\ &\equiv 3^3 \cdot 5 \pmod{10} \\ &\equiv 3 \cdot 5 \pmod{10} \\ &\equiv 15 \pmod{10} \\ &\equiv 5 \pmod{10} \end{aligned}$$

Дакле, рјешење почетне конгруенције је $x \equiv 5 \pmod{10}$.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

136 ●●●●

Ријешити систем линеарних конгруенција:

$$\begin{aligned} x &\equiv 4 \pmod{6} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 6 \pmod{11} \end{aligned}$$

Доказ. Како је $m_1 = 6, m_2 = 7, m_3 = 11$ они су у паровима узајамно прости, па можемо примијенити Кинеску теорему о остацима да бисмо добили рјешење овог система. Имамо да је $M = 6 \cdot 7 \cdot 11 = 462$.

$$\begin{aligned} M_1 &= \frac{M}{m_1} = \frac{462}{6} = 77 \\ M_2 &= \frac{M}{m_2} = \frac{462}{7} = 66 \\ M_3 &= \frac{M}{m_3} = \frac{462}{11} = 42 \end{aligned}$$

Да бисмо дошли до рјешења система, потребно је ријешити сљедеће три линеарне конгруенције:

$$\begin{aligned} 77y_1 &\equiv 1 \pmod 6 \\ 66y_2 &\equiv 1 \pmod 7 \\ 42y_2 &\equiv 1 \pmod{11} \end{aligned}$$

Њихова рјешења налазимо користећи обрат Еуклидовог алгоритма, у ствари тражимо рјешења Диофантових једначина:

$$\begin{aligned} 77y_1 - 6k &= 1 \\ 66y_2 - 7m &= 1 \\ 42y_3 - 11n &= 1 \end{aligned}$$

Сада, како је:

$$\begin{aligned} 77 &= 6 \cdot 12 + 5 \\ 6 &= 5 \cdot 1 + 1 \end{aligned}$$

слиједи да је $1 = 6 - 5 = 6 - (77 - 6 \cdot 12) = 13 \cdot 6 + 77 \cdot (-1)$. Дакле, $y_1 = -1$.

Како је:

$$\begin{aligned} 66 &= 7 \cdot 9 + 3 \\ 7 &= 3 \cdot 2 + 1 \end{aligned}$$

слиједи да је $1 = 7 - 3 \cdot 2 = 7 - (66 - 7 \cdot 9) \cdot 2 = -2 \cdot 66 + 19 \cdot 7$. Дакле, $y_2 = -2$.

Како је:

$$\begin{aligned} 42 &= 11 \cdot 3 + 9 \\ 11 &= 1 \cdot 9 + 2 \\ 9 &= 4 \cdot 2 + 1 \end{aligned}$$

добијамо да

$$\begin{aligned} 1 &= 9 - 4 \cdot 2 = \\ &= 9 - 4 \cdot (11 - 9) = \\ &= 9 - 4 \cdot (11 - (42 - 11 \cdot 3)) = \\ &= 9 - 4 \cdot (11 - 42 + 11 \cdot 3) = \\ &= 9 - 4 \cdot (4 \cdot 11 - 42) = \\ &= 9 - 16 \cdot 11 + 4 \cdot 42 = \\ &= 42 - 33 - 16 \cdot 11 + 4 \cdot 42 = \\ &= 5 \cdot 42 - 19 \cdot 11 \end{aligned}$$

Дакле, $y_3 = 5$.

Добијамо:

$$x = 4 \cdot 77 \cdot (-1) + 5 \cdot 66 \cdot (-2) + 6 \cdot 42 \cdot 5 = 292.$$

Дакле, рјешење датог система је $x = 292$.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

137 ●●●●

(а) (Математичка олимпијада у Мађарској, 1990.) Показати да постоји $n \in \mathbf{N}$, тако да

$$2^{1990} \mid (1989^n - 1).$$

Наћи најмање такво n.

(б) (Математичка олимпијада у Румунији, 1989.) Нека је $m \geq 3$ непаран природан број. Одредити најмање n за које важи

$$2^{1989} \mid (m^n - 1).$$

Доказ. (а) Треба одредити минимално n за које је $2^k \mid (m^n - 1)$, гдје је k дати природни број.

Нека је $n = 2^t q$, гдје је q непаран број. Тада имамо факторизацију:

$$m^n - 1 = (m^{2^t})^q - 1 = (m^{2t} - 1)[(m^{2^t})^{q-1} + \ldots + (m^{2^t}) + 1].$$

Број у угластој загради је непаран, зато што је ријеч о q непарних бројева, па $2^k \mid (m^n - 1)$ акко $2^k \mid (m^{2^t} - 1)$. Отуда слиједи да је $q = 1$, за тражено минимално n. С друге стране, имамо да важи:

$$(m^{2^t} - 1) = (m^2 - 1)(m^2 + 1) \cdot \ldots \cdot (m^{2^{t-1}} + 1).$$

Будући да је овдје m непаран број, m^2 даје остатак 1 при дијељењу са 4, а исто важи и за број облика $m^{2^r}, r \geq 1$. Због тога су у горњем производу са десне стране сви чиниоци сем првог дјељиви са 2, али не и са 4, што значи да је $t - 1$ највећи степен којим двојка дијели овај производ.

Према томе, преостаје да се размотри степен двојке у фактору $m^2 - 1 = (m - 1)(m + 1)$. Како m може давати остатак 1 или 3 при дијељењу са 4, посебно ћемо размотрити ова два случаја:

$$1)\ m \equiv 1 \pmod 4$$
$$2)\ m \equiv 3 \pmod 4.$$

Ако је $m \equiv 1 \pmod 4$, уочимо највећи број $s \geq 2$, са особином да $2^s \mid (m - 1)$. Тада је $m + 1$ дјељив са 2, али не и са 4, па је највиши степен којим 2 дијели $m^2 - 1$ дјељив са 2^{s+1}, али не и са једнак $s + 1$.

С друге стране, ако је $m \equiv 3 \pmod 4$, посматрамо највећи број $s \geq 2$ за који важи $2^s \mid (m + 1)$. Слично као малоприје, слиједи да је број $m^2 - 1$ дјељив са 2^{s+1}, али не и са 2^{s+2}.

Дакле, ако је број s одређен као што је то описано у претходном пасосу, тада је највиши степен којим 2 дијели $m^{2^t} - 1$ једнак $(t-1)+(s+1) = t+s$. Тражено минимално рјешење је $n = 2^{k-s}$ у случају $s \leq k$, у супротном је $n = 1$.
У задатку (а) је $m = 1989 = 4 \cdot 494 + 3$, па је у том случају $s = 2$, док је $k = 1990$, што значи да је рјешење задатка $n = 2^{1988}$.

(б) Овдје треба примијенити горње рјешење, за $k = 1989$.

$\square$

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

138 ●●●●

Дат је низ 1, 2, 4, 8, 16, 23, ... у кјем је сваки следећи број једнак збиру пртходног броја и збира његових цифара, тј. $a_1 = 1$ и $a_n = a_{n\text{-}1} + S(a_n)$ за $n > 1$, гдје је $S(x)$- збир цифара броја x. Да ли се у том низу појављује број 2 004?

Доказ. Бројеви x и $S(x)$ дају једнаке остатке при дијељењу са 3, тј.

$$x \equiv S(x) \pmod 3$$

Отуда је $a_n \equiv 2a_{n\text{-}1} \pmod 3$ за све $n > 1$,тј.
$a_1 \equiv 1 \pmod 3$, $a_2 \equiv 2 \pmod 3$, $a_3 \equiv 1 \pmod 3$, $a_4 \equiv 2 \pmod 3$, итд.
Одавде индуктивно слиједи $a_{2k\text{-}1} \equiv 1 \pmod 3$ и $a_{2k} \equiv 2 \pmod 3$ за свако $k \leqslant 1$. Како је $2004 \equiv 0 \pmod 3$, број 2004 није члан датог низа. $\square$

(**Сања Лончар 7/19 Б**) задатак преузет са
Збирка ријешених задатака из теорије бројева - Небојша Икодиновић, Марија Станић

139 ●●●●

Доказати да $641 \mid 2^{32} + 1$.

Доказ. Јасно је да:

$$641 = 2^7 \cdot 5 + 1 = 2^4 + 5^4$$

$$2^7 \cdot 5 \equiv -1 \pmod{641}$$

$$5^4 \equiv -2^4 \pmod{641}$$

$$5^4 \cdot 2^{25} \equiv (5 \cdot 2^7)^4 \equiv (-1)^4 \equiv 1 \pmod{641}$$

Посљедња конгруенција и $5^4 \equiv -2^4 \pmod{641}$ нам указују:

$$-2^4 \cdot 2^{28} \equiv 1 \pmod{641}$$

$$641 \mid (2^{32}+1)$$

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

140

●●●●

Наћи $5^{158} \pmod{11}$.

Доказ. Како је $158 = 15 \cdot 10 + 8$ имамо:

$$5^{158} = (5^{15})^{10}(5^8) \equiv 5^8 \pmod{11}$$

на основу Фермаове мале теореме.

Сада,

$$5^8 = (5^2)^4$$
$$= 25^4 \equiv 3^4 \pmod{11}$$
$$81 \equiv 4 \pmod{11}$$

Као крајњи резултат добијамо да:

$$5^{158} \pmod{11} = 4$$

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://www.math.fsu.edu/~pkirby/mad2104/SlideShow/s5_3.pdf`

141

●●●●

Ријешити: $146! \pmod{149}$.

Доказ. Број 149 је прост.

На основу Вилсонове теореме имамо да $148! \equiv -1(\pmod{149})$.

$$x = 146! \pmod{149}$$

$$147 \cdot 148 \cdot x = 148! \pmod{149}$$

$$(-2)\cdot(-1)x = (-1) \pmod{149}$$

$$-2 \cdot x = (-1) \pmod{149}$$

Сада како је $-2^{-1} \equiv 74 \pmod{149}$.

$$74 \cdot (-2 \cdot x) \equiv 74 \cdot 1 \pmod{1)49}$$

$$x = 74 \pmod{149}$$

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`http://sites.millersville.edu/bikenaga/number-theory/wilson-fermat/wilson-fermat.html`

142

Последња цифра броја $x^2 + xy + y^2$ је 0. Доказати да су онда последње двије цифре овог броја нуле.

Доказ. Да бисмо доказали да су последње двије цифре неког броја нуле можемо да користимо конгруентност по модулу 100. Уколико је $x^2 + xy + y^2 \equiv 0 \pmod{100}$ онда се овај број завршава са двије нуле.
Кренимо од тога да знамо да је последња цифра била нула, тј. да је број је дјељив са 10. Уколико је број дјељив са 10, значи да је дјељив и са 2 и са 5. Дакле:

$$\begin{gathered} 2 \mid x^2 + xy + y^2, \\ 5 \mid x^2 + xy + y^2. \end{gathered}$$

Да би било испуњено да $2 \mid x^2 + xy + y^2$ морају и x и y бити дјељиви са 2. Ако су оба непарна или један паран, а други непаран $x^2 + xy + y^2$ неће бити дјељив са 2. Што се тиче дјељивости са 5 имамо:

$$\begin{gathered} 5 \mid x^2 + xy + y^2, \\ \Rightarrow 5 \mid 2(x^2 + 2xy + y^2) \\ \Rightarrow 5 \mid x^2 + 2xy + y^2 + x^2 + y^2 \\ \Rightarrow 5 \mid (x+y)^2 + x^2 + y^2 \end{gathered}$$

Могући остаци квадрата при дијељењу са 5 су 0, 1 и 4. Дакле могућности су да $5 \mid x$, $5 \mid y$ и $5 \mid x + y$ или да је један од ова три броја дјељив са 5, а од друга два један облика $5k \pm 1$, а други облика $5l \pm 2$, а како је овај други случај немогућ, остаје да је тачан први и да су и x и y дјељиви са 5. Како су оба броја дјељива и са 2 и са 5, слиједи да су оба дјељива са 10. Одатле закључујемо да израз $x^2 + xy + y^2$ мора бити дјељив са 100, па се овај број завршава са двије нуле.

□

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

143

Наћи посљедње двије цифре броја $7^{7^{1000}}$.

Доказ. Посматрајмо:

$$\phi(100) = \phi(2^2) \cdot \phi(5^2) = (2^2 - 2)(5^2 - 5) = 40,$$

при чему је $\phi(n)$ Ојлерова функција.

На основу Ојлерове теореме знамо да

$$7^{40} \equiv 1 \pmod{100}.$$

Сада,

$$\phi(40) = \phi(2^3) \cdot \phi(5) = 4 \cdot 4 = 16$$

.

$$7^{16} \equiv 1 \pmod{40}.$$

Како је $1000 = 16 \cdot 62 + 8$, онда:

$$7^{1000} = (7^{16})^{62} \cdot 7^8 \equiv 1^{62} \cdot 7^8 \equiv (7^4)^2 \equiv 1^2 \equiv 1 \pmod{40},$$

што нам указује да број 7^{1000} можемо записати на сљедећи начин:

$$7^{1000} = 40t + 1.$$

То ћемо искористити:

$$7^{7^{1000}} \equiv 7^{40t+1} \equiv 7 \cdot (7^{40})^t \equiv 7 \pmod{100}$$

На крају закључујемо да ће посљедње двије цифре нашег броја бити 07.

☐

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

144

Нека су a и b прости бројеви. Доказати да природни бројеви c и d такви да важи $a^2 + b^2 + c^2 = d^2$ постоје ако и само ако је бар један од бројева a и b паран.

Доказ. Једнакост $a^2 + b^2 + c^2 = d^2$ еквивалентна је са $a^2 + b^2 = d^2 - c^2$, тј. са $a^2 + b^2 = (d - c)(d + c)$. Прво претпоставимо да је један од бројева a и b паран. Уколико је други број непаран, тада је израз $a^2 + b^2$ непаран. У том случају одговарајуће бројеве c и d можемо наћи рјешавајући систем

$$\begin{aligned} d-c&=1\\ d+c&=a^2+b^2 \end{aligned}$$

(добијају се рјешења $c=\frac{a^2+b^2-1}{2}$ и $d=\frac{a^2+b^2+1}{2}$, што јесу природни бројеви). Уколико је и други број паран, тада је израз a^2+b^2 дјељив са 4, па и том случају одговарајуће бројеве c и d можемо наћи рјешавајући систем

$$\begin{aligned} d-c&=2\\ d+c&=\tfrac{a^2+b^2}{2} \end{aligned}$$

(добијају се рјешења $c=\frac{a^2+b^2}{4}-1$ и $d=\frac{a^2+b^2}{4}+1$, што јесу природни бројеви).
Узмимо сада да важи $a^2+b^2=(d-c)(d+c)$, и докажимо да је бар један од бројева a и b паран. Претпоставимо супротно: нека су и a и b непарни бројеви. Тада важи $a^2\equiv 1 \pmod 4$ и $b^2\equiv 1 \pmod 4$, па слиједи $a^2+b^2\equiv 2 \pmod 4$. С друге стране, ако су c и d исте парности, тада су оба израза $d-c$ и $d+c$ парна, па је њихов производ (што је a^2+b^2) дјељив са 4, а то је контрадикција. Ако су c и d различите парности, тада је њихов производ непаран, и поново имамо контрадикцију. □

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

145

Помоћу математичке индукције доказати да $11^n\equiv 1+10n \pmod{100}$ за све природне бројеве n.

Доказ. $(n=1)$

$$11^1\equiv 1+10\cdot 1 \pmod{100}$$

$$11\equiv 11\cdot 1 \pmod{100}$$

Индуктивна претпоставка:

$$11^k\equiv 1+10k \pmod{100}$$

Показујемо да:

$$11^{k+1}\equiv 1+10(k+1) \pmod{100}$$

$$\begin{gathered} 11^{k+1}=11\cdot 11^k\equiv 11\cdot(1+10k) \pmod{100} =\\ =11+110k \pmod{100}\equiv 11+10k \pmod{100} =\\ =1+10(k+1) \pmod{100} \end{gathered}$$

На основу математичке индукције смо успјели да покажемо да за сваки природан број n важи $11^n\equiv 1+10n \pmod{100}$.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://www.math.ksu.edu/~pinner/math506/Spring2020/506S20Ex1Sols.pdf`

146

Одредити највећи заједнички дјелилац свих бројева из скупа

$$\{(n+2014)^{n+2014}+n^n \mid n>2014^{2014}\}$$

за природан број n.

Доказ. Означимо са d тражени број. Доказаћемо да је $d=4$. Нека је, за природан број n

$$x_n=(n+2014)^{n+2014}+n^n.$$

Нека је p прост број који не дијели 2014 и $n>2014^{2014}$ такво да $p \mid n$. Тада $p \nmid n+2014$ па $p \nmid x_n$. Одавде закључујемо да број d може бити дјељив једино простим бројевима из скупа $\{2,19,53\}$.
За $n>2014^{2014}$ такво да $19\cdot 53 \mid n-1$ имамо $x_n \equiv 1+1 \pmod{19}$ и $x_n \equiv 1+1 \pmod{53}$ односно $19 \nmid d$ и $53 \nmid d$. Дакле, $d=2^k$ за неко $k \geq 0$.
Ако је n паран број, онда су бројеви $(n+2014)^{n+2014}$ и n^n дјељиви са 4, па $4 \mid x_n$.
Ако је $n \equiv 1 \pmod 4$, онда је $x_n \equiv 1^{n+2014}+1^n \equiv 0 \pmod 4$.
Слично, за $n \equiv -1 \pmod 4$, добијамо $x_n \equiv 1^{n+2014}+(-1)^n \equiv 0 \pmod 4$. Из свега наведеног закључујемо да је $k \geq 2$. Даље, за $n>2014^{2014}$ такво да је $n \equiv 3 \pmod 8$ имамо

$$x_n \equiv 1^{n+2014}+3^n \equiv 1+3\cdot(3^2)^{\frac{n-1}{2}} \equiv 1+3 \equiv 4 \pmod 8,$$

па $8 \nmid d$, односно $d=4$.

□

(**Александар Вујовић 4/19 Б**) задатак преузет са :
`https://imomath.com/srb`

147

а) Које су посљедње двије цифре броја 3^{25}?
б) Одредити посљедњу цифру у декадном запису броја 3^{400}.
в) Којом цифром се завршава број 7^{2006}?

Доказ. а) Посљедње двије цифре можемо добити тако да подијелимо број са 100 и видимо који је остатак, тј. занима нас $3^{25} \pmod{100}$. Имамо да важи $3^4 \equiv 81 \pmod{100}$ те када квадрирамо обије стране добијемо $3^8 \equiv 81^2 \pmod{100} \equiv 6561 \pmod{100} \equiv 226981 \pmod{100} \equiv 81 \pmod{100}$. Сада помножимо обије стране с 3 како бисмо добили $3^{25} \equiv 243 \pmod{100} \equiv 43 \pmod{100}$.
Дакле, посљедње двије цифре 3^{25} су 43. Калкулатор не би могао израчунати овај број јер је једноставно превелик. Калкулатор ће заокружити одговор и неке цифре ће се изгубити.

б) Треба да одредимо остатак при дијељењу броја 3^{400} са 10 јер дијељењем неког броја са 10 остатак представља посљедњу цифру тог броја. Дакле, $3^{400} \equiv ? \pmod{10}$. Имамо:

$$\begin{gathered}3 \equiv 3 \pmod{10}\\ 3^2 \equiv -1 \pmod{10}\\ (3^2)^{200} \equiv (-1)^{200} \pmod{10}\\ 3^{400} \equiv 1 \pmod{10}\end{gathered}$$

Дакле, посљедња цифра броја 3^{400} је 1.

в) Посљедња цифра неког броја је у ствари остатак при дијељењу тог броја бројем 10.

$$\begin{gathered}7^2 = 49 \equiv -1 \pmod{10}\\ 7^{2006} = (7^2)^{1003} \equiv (-1)^{1003} = -1 \pmod{10}\end{gathered}$$

Како је $9 \equiv -1 \pmod{10}$, а $0 \leq 9 < 10$, значи да је посљедња цифра броја 7^{2006} цифра 9.

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са

`https://zir.nsk.hr/islandora/object/mathos%3A121/datastream/PDF/view`

`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf`

`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

148

Доказати да је број $2^{702} \cdot 19^{826} - 11^{347} \cdot 17^{195}$ дјељив са 3.

Доказ. Могући остаци при дијељењу са 3 су 0, 1 или 2. Знамо да је $2 \equiv 2 \pmod 3$, такође можемо рећи и да је $2 \equiv -1 \pmod 3$, јер броју 2 фали 1 да би био дјељив са 3 (по дефиницији важи да $3 \mid 2-(-1)$).

Па је:

$$2^{702} \equiv (-1)^{702} \quad \pmod 3,$$

тј.

$$2^{702} \equiv 1 \quad \pmod 3.$$

На исти начин ћемо наћи преостале остатке:

$$\begin{gathered}19 \equiv 1 \quad \pmod 3 \implies 19^{826} \equiv 1^{826} \quad \pmod 3\\ \implies 19^{826} \equiv 1 \quad \pmod 3\end{gathered}$$

$$\begin{gathered}11 \equiv 2 \quad \pmod 3 \iff 11 \equiv -1 \quad \pmod 3\\ \implies 11^{347} \equiv (-1)^{347} \quad \pmod 3\\ \implies 11^{347} \equiv -1 \quad \pmod 3\end{gathered}$$

$$\begin{gathered}11 \equiv 2 \quad \pmod 3 \iff 17 \equiv -1 \quad \pmod 3\\ \implies 17^{195} \equiv (-1)^{195} \quad \pmod 3\\ \implies 17^{195} \equiv -1 \quad \pmod 3\end{gathered}$$

На крају добијамо:

$$2^{702} \cdot 19^{826} - 11^{347} \cdot 17^{195} \equiv 1 \cdot 1 - (-1) \cdot (-1) \pmod 3 \equiv 0 \pmod 3.$$

Дакле, $3 \mid 2^{702} \cdot 19^{826} - 11^{347} \cdot 17^{195}$.

$\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14559/mod_resource/content/1/Kongruencije-peti`
`20termin.pdf`

149

●●●●

а) Које остатке при дијељењу са 9 дају квадрати природних бројева?

б) Доказати да не постоје природни бројеви m и n такви да је

$$m^2 + n^2 = 6\underbrace{0\ldots0}_{13}$$

Доказ. а) Остаци при дијељењу са 9 су $0, 1, 2, 3, 4, 5, 6, 7, 8$, односно $0, 1, 2, 3, 4, -1, -2, -3, -4$.

- Ако је $x \equiv 0 \pmod 9$, тада је $x^2 \equiv 0 \pmod 9$.
- Ако је $x \equiv \pm 1 \pmod 9$, тада је $x^2 \equiv 1 \pmod 9$.
- Ако је $x \equiv \pm 2 \pmod 9$, тада је $x^2 \equiv 4 \pmod 9$.
- Ако је $x \equiv \pm 3 \pmod 9$, тада је $x^2 \equiv 0 \pmod 9$.
- Ако је $x \equiv \pm 4 \pmod 9$, тада је $x^2 \equiv 7 \pmod 9$.

Дакле, остаци које могу дати квадрати природних бројева при дијељењу са 9 су 0, 1, 4 и 7.

б) Број $6\underbrace{0\ldots0}_{13}$ можемо записати као $6 \cdot 10^{13}$. Како је $10 \equiv 1 \pmod 9$, слиједи да је $10^{13} \equiv 1 \pmod{19}$, па је $6 \cdot 10^{13} \equiv 6 \pmod 9$. На основу дијела под (а) слиједи да при дијељењу броја $m^2 + n^2$ са 9 можемо добити остатке 0, 1, 2, 4, 5, 7 и 8 (нпр. ако је $m^2 \equiv 7 \pmod 9$ и $n^2 \equiv 4 \pmod 9$, тада је $m^2 + n^2 = 7 + 4 \pmod 9$, односно $m^2 + n^2 \equiv 2 \pmod 9$).

Како $m^2 + n^2$ и $6 \cdot 10^{13}$ дају различите остатке при дијељењу са 9, слиједи $m^2 + n^2 \neq 6\underbrace{0\ldots0}_{13}$.

$\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%`
`20%28drugi%20deo%29.pdf`

150

12 хлебова подијелило је 12 људи, сваки мушкарац добио је по 2 хлеба, жена по пола хлеба, а свако дијете по четвртину хлеба. Колико је било мушкараца, колико жена а колико дјеце?

Доказ. Са m означимо број мушкараца, са z број жена и са d број дјеце.

Знамо да имамо 12 људи, па би прва једначина била $m + z + d = 12$, како имамо и 12 хлебова друга једначина је $2m + \frac{1}{2}z + \frac{1}{4}d = 12$, тј. $8m + 2z + d = 48$. Како $2 \mid 8m$, $2 \mid 2z$ и $2 \mid 48$ тада $2 \mid d$. С обзиром да је d број дјеце, а знамо да је укупан број људи 12, то нам говори да је $0 \leq d \leq 12$.

Ако претпоставимо да је $d = 12$, тада из једначине $2m + \frac{1}{2}z + \frac{1}{4}d = 12$ добијамо да $\frac{1}{4} \cdot 12 = 12$, tj. $3 = 12$ што је немогуће. Дакле, $d \neq 12$.
Имамо да $2 \equiv d$ и $0 \leq d \leq 12$, одакле знамо да је d паран односно облика $d = 2k$, $k \in \mathbb{N}$. Ако је $0 \equiv d < 12$, то је $0 \equiv k < 6$.
Замјеном $d = 2k$ у једначинама $m + z + d = 12$ и $8m + 2z + d = 48$, добијамо једначине $m + z + 2k = 12$ и $4m + z + k = 24$. Рјешавањем ових једначина добијамо да је $k = 3m - 12$. Како $3 \mid 12$ и $3 \mid 3m$ то важи да $3 \mid k$. Како знамо да је $0 \leq k < 0$ закључујемо да је $k = 0$ или $k = 3$.

- $k = 0$
  $12 - 3m = 0 \implies m = 4$
  $d = 2k = 0$
  $z = 12 - m - 2k = 12 - 4 - 0 = 8$

  Прво рјешење је: 4 мушкарца, 8 жена и нема дјеце.

- $k = 3$
  $m - 12 = 3 \implies m = 5$
  $d = 2k = 6$
  $z = 12 - m - 2k = 12 - 5 - 6 = 1$

  Друго рјешење је: 5 мушкараца, 6 дјеце и 1 жена.

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14714/mod_resource/content/1/Kongruencije%20%28drugi%20deo%29.pdf`

151

Наћи остатак који се добија при дијељењу броја:
а) $3^{105}+4^{105}$ са 11.
б) 1978^{20} са 125.
в) $9\cdot 99\cdot 999\cdots \underbrace{99\ldots 9}_{9999}$ са бројем 1000?

Доказ. а) Прво ћемо наћи остатак при дијељењу броја 3^{105} са 11.

$$3\equiv 3 \pmod{11}$$
$$3^2\equiv -1 \pmod{11} \text{ (Броју } 3^2=9 \text{ фали 2 да би био дјељив са 11.)}$$
$$3^3\equiv -6 \pmod{11}$$

До претходног закључка можемо доћи на два начина, прво, знамо да броју $3^3=27$ фали још 7 до броја 33 који је дјељив са 11. Друго, већ смо показали да је $3\equiv 3 \pmod{11}$ и $3^2\equiv -2 \pmod{11}$, одакле је $3^3=3\cdot 3^2\equiv 3\cdot(-2) \pmod{11}$.

Такође можемо рећи и да је

$$3^3\equiv 5 \pmod{11}.$$

На исти начин закључујемо

$$\begin{aligned}3^4&\equiv 4 \pmod{11}\\ 3^5&\equiv 12 \pmod{11}\\ 3^5&\equiv 1 \pmod{11}\\ (3^5)^{21}&\equiv 1^{21} \pmod{11}\\ 3^{105}&\equiv 1 \pmod{11}.\end{aligned}$$

Сада ћемо наћи остатак при дијељењу броја 4^{105} са 11.

$$\begin{aligned}4&\equiv 4 \pmod{11}\\ 4^2&\equiv 5 \pmod{11}\\ 4^3&\equiv -2 \pmod{11}\end{aligned}$$

Јер $4^3=4\cdot 4^2\equiv 4\cdot 5 \pmod{11}$, знамо да броју 20 фали 2 до броја 22 који је дјељив са 11, па је $4^3\equiv -2 \pmod{11}$.

Сада имамо

$$\begin{aligned} 4^4 &\equiv -8 \pmod{11} \\ 4^4 &\equiv 3 \pmod{11} \\ 4^5 &\equiv 12 \pmod{11} \\ 4^5 &\equiv 1 \pmod{11} \\ (4^5)^{21} &\equiv 1^{21} \pmod{11} \\ 4^{105} &\equiv 1 \pmod{11}. \end{aligned}$$

На крају добијамо

$$3^{105} + 4^{105} \equiv 1 + 1 \pmod{11} \equiv 2 \pmod{11}.$$

б) Како је $1978 = 2000 - 22$ и број 2000 дјељив са 125, то је:

$$\begin{gathered} 2000 \equiv 0 \pmod{125} \\ 1978 \equiv -22 \pmod{125} \\ \text{Тада је } 1978^{20} \equiv (-22)^{20} \pmod{125}. \end{gathered}$$

Даље је:

$$(-22)^{20} = 484^{10} = 256^5 \equiv 6^5 \pmod{125} \equiv 26 \pmod{125}.$$

Дакле, остатак при дијељењу броја 1978^{20} са 125 је 26.

в) Уочимо да је

$$999 \equiv 9999 \equiv \ldots \equiv \underbrace{99\ldots9}_{9999} \equiv -1 \pmod{1000}.$$

То је укупно $999-3+1 = 997$ бројева и њихов производ је конгруентан са $-1 \pmod{1000}$. Стога, цијели израз је конгруентан са $(-1) \cdot 9 \cdot 99 = -891 \equiv 109 \pmod{1000}$. Дакле, остатак при дијељењу броја $9 \cdot 99 \cdot 999 \cdots \underbrace{99\ldots9}_{9999}$ са бројем 1000 једнак је 109.

$\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/14559/mod_resource/content/1/Kongruencije-peti`
`20termin.pdf`
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?`
`sequence=1`
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

152
●●●●

Нека је n природан број. Доказати да је највећи заједнички дјелилац бројева n^2+1 и $(n+1)^2+1$ или 1 или 5, те доказати да је једнак 5 ако и само ако је $n \equiv 2 \pmod{5}$.

Доказ. Нека је $d = \text{нзд}(n^2+1, (n+1)^2+1)$. Тада d дијели број

$$((n+1)^2+1) - (n^2+1) = 2n+1,$$

те број

$$n(2n+1) - 2(n^2+1) = n-2.$$

Према томе, d дијели

$$(2n+1) - 2(n-2) = 5,$$

па је $d \in \{1, 5\}$.

Ако број n даје остатке $0, 1, 2, 3, 4$ при дијељењу са 5, онда број n^2+1 даје остатке редом $1, 2, 0, 0, 2$ а $(n+1)^2+1$ остатке редом $2, 0, 0, 2, 1$. Према томе, бројеви n^2+1 и $(n+1)^2+1$ истовремено су дјељиви са 5 ако и само ако је $n \equiv 2 \pmod 5$.

☐

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

153

(Математичка олимпијада, 1999.) Нека је $n \in \mathbb{N}, n > 10$ такав да свака од његових цифара припада скупу $S = \{1, 3, 7, 9\}$. Доказати да n има неки прост дјелилац који је ≥ 11.

Доказ. Примијетимо да производ свака два броја из скупа $\{1, 3, 7, 9\}$, по модулу 20, је такође број из тог скупа. Дакле, то важи и за сваки коначни производ тих бројева. Специјално, било који број облика $3^j 7^k \equiv 1, 3, 7$ или $9 \pmod{20}$.

Сада, ако су све цифре броја n из скупа S, онда је његова цифра десетице непарна и не можемо имати $n \equiv 1, 3, 7$ или $9 \pmod{20}$. Тако да, n не може бити облика $3^j 7^k$. Не може ни бити дјељив са 2 или 5 (у супротном његова посљедња цифра не би била $1, 2, 3$ или 9). Стога n мора бити дјељив неким простим бројем који је ≥ 11, као што је требало доказати. ☐

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

154

Нека је d било који позитиван број различит од 2, 5 и 13. Доказати да постоје различити бројеви a и b из скупа $\{$ 2,5,13,$d\}$ такви да $ab - 1$ није потпун квадрат.

Доказ. Прво ћемо провјерити шта се дешава када су $a, b \neq d$.
$2 \cdot 5 - 1 = 10 - 1 = 9(a = 2, b = 5$ или обрнуто)
$2 \cdot 13 - 1 = 26 - 1 = 25(a = 2, b = 13$ или обрнуто)
$13 \cdot 5 - 1 = 65 - 1 = 64(a = 13, b = 5$ или обрнуто)
Директном провјером смо утврдили да у свим случајевима када су оба $a, b \neq d$, $ab - 1$ јесте потпун квадрат. Претпоставимо сада да је$a = d$, b ће тада бити из скупа $\{$ 2,5,13$\}$. Дакле, провјеравамо да ли може неки од $2d$ -1, $5d$ -1 і $13d$ -1 да не буде потпун квадрат. Да бисмо то доказали претпоставимо супротно. Нека су сва три потпуни квадрати. Посматрајмо остатке при дијељењу са 4.

$$13d \ - 1 = k^2 \qquad\qquad (1)$$

$$5d \ - 1 = l^2 \qquad\qquad (2)$$

$$2d \ - 1 = m^2 \qquad\qquad (3)$$

$$(1) \Rightarrow 13d \equiv 1, 2 \pmod 4 \Rightarrow d \equiv 1, 2 \pmod 4$$

1.случај: $d \equiv 1 \pmod 4 \Rightarrow d = 4k + 1$,за неко $k \in \mathbb{Z}$

$$(2) \Rightarrow 20k + 4 = 4(5k + 2) = l^2$$

$$\Rightarrow (\frac{l}{2})^2 = 5k + 2 \equiv 2 \pmod 5,$$

што је немогуће, јер имамо контрадикцију са тим да остаци потпуних квадрата при дијељењу са 5 само 0,1 или 4, али не и 2. Дакле, преостаје случај када је $d \equiv 2 \pmod 4$. 2.случај: $d \equiv 2 \pmod 4 \Rightarrow d = 4k + 2$,за неко $k \in \mathbb{Z}$

$$(2) \Rightarrow m^2 \equiv 3 \pmod 8)$$

И овдје имамо контрадикцију, јер могући остаци потпуних квадрата при дијељењу са 8 могу бити само 0,1 или 4, али не и 3.
Закључујемо да $2d$ -1, $5d$ -1 і $13d$ -1 не могу сва три да буду потпуни квадрати, што значи да постоји бар један од њих који није потпун квадрат.
Напомена: У задатку смо користили остатке по модулу 4,5 и 8 квадрата природних бројева. Сви парни бројеви су облика $2k$, дакле парни број на квадрат ће бити облика $4k^2$, а то је $\equiv 0 \pmod 4$. Што се тиче непарних бројева, они су облика $2k + 1$, па је сваки непаран број на квадрат облика $4k^2 + 4k + 1$, а то је $\equiv 1 \pmod 4$. Дакле, квадрати свих природних бројева дају остатке 0 или 1 при дијељењу са 4.
Остаци при дијељењу са 5 за природне бројеве су 0, 1, 2, 3, или 4 па су остаци по модулу 5 за квадрате ових бројева 0, 1 или 4. Слично за 8, остаци за природне бројеве су 0, 1, 2, 3, 4, 5, 6 или 7, па су могућности за остатке 0, 1 или 4.

□

(**Сања Лончар 7/19 Б**) задатак преузет са
`elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

155

Пронађите све могућности за позитивне цијеле бројеве x, y, z такве да је $x \leq y \leq z$ и

$$x^3(y^3 + z^3) = 2012(xyz + 2)$$

Доказ. Примијетимо да је $2012 = 2 \cdot 2 \cdot 503$, па је десна страна дјељива са овим бројевима, дакле да би једнакост била испуњена и лијева страна мора да буде дјељива са 503 и 2^2. То ћемо искористити да испитамо могућности за x, y и z.
Ако $503 \mid x$ тада 503^3 дијели лијеву страну једнакости, док највише 503^1 дијели десну страну. Одавде закључујемо да $503 \nmid x$. Како x дијели лијеву страну једнакости, јасно је да мора да дијели и $2012 \cdot (xyz + 2)$. Ако $x \nmid 2012$, тада $x \mid xyz + 2$, па $x \mid 2$ (јер $x \mid xyz$), што је супротно претпоставци да $x \nmid 2012$. Када $x \mid 2012$ мора бити $x = 2^\alpha$, гдје $\alpha \in \{0, 1, 2\}$. Ако је $x = 2^2$, тада 2^6 дијели лијеву страну , док највише 2^3 дијели десну страну, дакле $x \in \{1, 2\}$.
Како је 503 прост број, на основу Мале Фермаове теореме имамо:

$$y^{502} \equiv z^{502} \pmod{503}$$

Из тога да $503 \mid x(y^3 + z^3)$ и $503 \mid x$ имамо да $503 \mid (y^3 + z^3)$, односно:

$$y^3 + z^3 \equiv 0 \pmod{503}$$

$$y^3 \equiv -z^3 \pmod{503}$$

Даље, имамо:

$$y^{3 \cdot 167} \equiv -z^{3 \cdot 167} \pmod{503}$$

$$\Rightarrow y \equiv -z \pmod{503}$$

Тако да $503 \mid (y + z)$, па је $(y + z) = 503k$.
1. случај:$x = 1$
Тада једначина постаје:

$$y^3 + z^3 = 2012(yz + 2)$$

$$503k(y^2 - yz + z^2) = 2012(yz + 2)$$

$$k(y^2 - yz + z^2) = 4yz + 8$$

$$k(y - z)^2 + yz(k - 4) = 8$$

Како је $yz(k - 4) \leq 8$, мопа бити $k \leq 4$, јер је $yz + 1 \geq y + z = 503k \geq 503 \Rightarrow yz \geq 502$.
Пошто је $y^3 + z^3 = 2012(yz + 2)$, закључујемо да $y^3 + z^3$ мора бити паран број, што значи да ће y и z бити исте парности, па ће самим тим и број $y + z$ бити паран. Даље, како имамо да је $y + z = 503k$ закључујемо да је k паран. Дакле, $k \in \{2, 4\}$.
Ако је $k = 4$ тада$(y - z)^2 = 2$ што је немогуће. Ако је $k = 2$ тада:
$2(y - z)^2 - 2yz = 8$
$\Rightarrow (y + z)^2 - 5yz = 4 \Rightarrow 2^2 \cdot 503^2 - 4 = 5yz$, али лијева страна није дјељива са 5, тако да нема рјешења кад је $x = 1$.
2. случај: $x = 2$
Једначина тада постаје:

$$2^3(y^3 + z^3) = 2 \cdot 2012(yz + 1)$$

$$k(y^2 - yz + z^2) = yz + 1$$

Ако је $|y - z| > 1$, тада $k(y^2 - yz + z^2) \geq y^2 - yz + z^2 > yz + 1$, што није тачно, дакле $y = z$ или $|y - z| = 1$. Одавде имамо:
$2y^3 = 503y^2 + 503$,
дакле 503 дијели десну страну, па сигурно нијели и лијеву. Одавде имамо $503 \mid y$, па $503^3 \mid 2y^3$, али како 503^3 не дијели десну страну, то је контрадикција. Значи $k = 1$ и онда је рјешење $(x, y, z) = (2, 251, 252)$. ☐

(**Сања Лончар 7/19 Б**) задатак преузет са
`elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

156
●●●●

Одредити све природне бројеве x и y за које је

$$2014^x + 11^x = y^2.$$

Доказ. За $x = 1$ једино рјешење је пар $(x, y) = (1, 45)$. Претпоставимо да је $x \geq 2$. Како је $2014^x + 11^x$ непаран број, закључујемо да је и y непаран. Са друге стране, $4 \mid 2014^x$, па је $y^2 = 2014^x + 11^x \equiv 11^x \pmod 4$, а како квадрат непарног броја даје остатак 1 при дијељењу са 4, закључујемо да је $11^x \equiv 1 \pmod 4$. Међутим, $11^x \equiv 3^x \pmod 4$, па 11^x даје остатак 1 при дијељењу са 4 акко је x паран број. Тада $11^x \equiv 2^x \equiv 1 \pmod 3$, па $y^2 = 2014^x + 11^x \equiv 1 + 1 = 2 \pmod 3$, што није могуће, јер квадрат природног броја даје остатак 0 или 1 при дијељењу са 3. Једино рјешење је пар $(x, y) = (1, 45)$. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

157
●●●●

Доказати да важи

$$27|49^{95} + 113^{41}.$$

Доказ. Означимо $49^95 + 113^41 = A$. Треба провјерити да ли важи

$$A \equiv 0 \pmod{27}?$$

Лако види да је $49 \equiv 22 \pmod{27}$. Тада из леме која каже да је $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ за прост број p и $\alpha \geqslant 1$, имамо да важи

$$\varphi(27) = \varphi(3^3) = 3^3 - 3^2 = 18$$

Примјеном Еуклидове теореме слиједи

$$49^{18} \equiv 1 \pmod{27}$$

Даље, из Пропозиције $\langle$ Ако је $a \equiv b \pmod{m}$, онда $a^n \equiv b^n \pmod{m}, \forall n \in \mathbb{N}$ $\rangle$, имамо да важи

$$\begin{aligned} 49^{95} &\equiv (49^{18})^5 \cdot 49^5 \pmod{27} \\ &\equiv 1^5 \cdot 49^5 \pmod{27} \\ &\equiv 22^5 \pmod{27} \\ &\equiv 7 \pmod{27}. \end{aligned}$$

Сада имамо

$$113 \equiv 5 \pmod{49},$$

па примјеном Еуклидове теореме слиједи

$$113^{18} \equiv 1 \pmod{49}.$$

Аналогно закључујемо

$$\begin{aligned} 113^{41} &\equiv (113^{18})^2 \cdot 5^5 \pmod{49} \\ &\equiv 1^2 \cdot 5^5 \pmod{27} \\ &\equiv 20 \pmod{27} \end{aligned}$$

Стога је $49^{95} + 113^{41} \equiv 7 + 20 \equiv 0 \pmod{27}$. ☐

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://repozitorij.mathos.hr/islandora/object/mathos%3A260/datastream/PDF/view`

158
●●●●

Наћи остатак при дијељењу $(1! + 2! + 3! + 4! + \ldots)$ са 9.

Доказ. Прије свега, уочимо да је $n! \equiv 0 \pmod{9}$ за $\forall n \geq 6$, јер у израчунавању факторијела сваког броја већег од 5, имамо чиниоце 3 и 6, па је број дјељив са 9. Стога, остаје да нађемо $(1! + 2! + 3! + 4! + 5!) \pmod{9}$.

$$1! \equiv 1 \pmod{9}$$

$$2! \equiv 2 \pmod{9}$$

$$3! \equiv 6 \pmod{9}$$

$$4! \equiv 24 \equiv 6 \pmod{9}$$

$$5! \equiv 120 \equiv 3 \pmod{9}$$

$$(1! + 2! + 3! + 4! + 5!) \equiv 1 + 2 + 6 + 6 + 3 \equiv 18 \equiv 0 \pmod{9}$$

Дакле, остатак при дијељењу је 0. ☐

(**Сања Лончар 7/19 Б**) задатак преузет са
`http://math.cmu.edu/~/acarguerml/archive/15-16/number-theory-09-13-15-solutions.pdf`

159

Нека је $P(x)$ полином са цјелобројним коефицијентима, такав да за сваки природан број n број $P(P(n))$ при дијељењу са n даје остатак $n-1$. Доказати да полином $P(x)$ нема цјелобројну нулу.

Доказ. Како за сваки природан број n важи $n \equiv 0 \pmod{n}$, а самим тим и $P(P(n)) \equiv P(P(0)) \pmod{n}$. Одакле, по услову задатка имамо $P(P(0)) \equiv -1 \pmod{n}$, односно $n \mid P(P(0)) + 1$, за сваки природан број n, па је $P(P(0)) = -1$. Претпоставимо да постоји цијели број a, такав да је $P(a) = 0$. Тада је $P(x) = (x-a)Q(x)$, за неки полином $Q(x)$ са цјелобројним коефицијентима, па важи

$$P(0) = -aQ(0) \text{ и } -1 = P(P(0)) = (-a \cdot Q(0) - a) \cdot (Q(P(0))) = -a \cdot (Q(0)+1) \cdot Q(P(0)).\ (*)$$

Одавде је број $Q(0)$ паран (јер је $Q(0)+1 \in \{-1,1\}$), па је због $P(0) = -a \cdot Q(0)$ и $P(0)$ паран број. Нека је $P(0) = b$. Из $(*)$ је $Q(b) \in \{-1,1\}$, те је $Q(b)$ непаран. Међутим, како је $b \equiv 0 \pmod{2}$, то је $1 \equiv Q(b) \equiv Q(0) \equiv 0 \pmod{2}$, што је контрадикција. Овим смо доказали да полином $P(x)$ нема цјелобројну нулу, што је и требало доказати. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

160

Нека је n природан број. Показати да ако су a и b природни бројеви већи од 1, такви да $2^n - 1 = ab$, онда $ab - (a-b) - 1$ можемо записати у облику $k \cdot 2^{2m}$ за неки непаран број k и природан број m.

Доказ. Примијетимо сљедеће:

$$ab - (a-b) - 1 = (a+1)(b-1)$$

Требали бисмо показати да су највећи степени двојке који дијеле $(a+1)$ и $(b-1)$ заправо један исти број.

Нека су 2^s и 2^t највећи степени двојке који дијеле $(a+1)$ и $(b-1)$, редом. Како је:

$$a+1, b+1 \leq ab+1 = 2^n$$

онда знамо да су $s, t \leq n$.

Примјећујемо да $2^s \mid 2^n = ab+1$ и $2^s \mid a+1$, тако да

$$ab \equiv a \equiv -1 \mod 2^s$$

Стога,

$$b \equiv 1 \mod 2^s$$

тј.

$$2^s \mid b-1$$

па закључујемо да $s \leq t$.

Слично,

$$ab \equiv -1 \equiv -1 \mod 2^t$$

, тако да $a \equiv -1 \mod 2^t$ и $2^t \mid a+1$.

Онда $t \leq s$.

На основу претходног закључујемо да $t = s$, па је највећи степен двојке који дијели $(a+1)(b-1)$ заправо $2s$.

Па на крају имамо:

$ab - (a-b) - 1 = k \cdot 2^{2s}$ за непарно k.

☐

(**Андрија Бошковић 14/19 Б**) задатак преузет са `https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

161

Нека су $p_1, p_2, p_3, ..., p_n$ различити прости бројеви, доказати да $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + ... + \frac{1}{p_n}$ није реалан број.

Доказ. Број

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + ... + \frac{1}{p_n} = \frac{p_2 \cdot p_3 \cdots p_n + ... + p_1 \cdot p_2 \cdots p_{n-1}}{p_1 \cdot p_2 \cdots p_n}$$

није цио број јер бројилац датог разломка није дјељив са p_1 (због тога што фигуришу искључиво прости бројеви имамо да први сабирак бројиоца није дјељив са p_1 док остали јесу), именилац је истовремено дјељив са p_1 што указује да $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + ... + \frac{1}{p_n}$ није цио број.

☐

(**Андрија Бошковић 14/19 Б**)

162

Нека је (x, y, z) рјешење једначине $x^2 + y^2 = z^2$. Показати да је један од ова три броја дјељив са 3.

Доказ. Претпоставимо да ниједан од бројева x, y, z није дјељив са 3. То значи да се они могу записати у облику

$$x = 3q + 2(\text{или} \quad x = 3q + 2)$$

$$y = 3q + 2(\text{или} \quad y = 3q + 2)$$

$$z = 3q + 2(\text{или} \quad z = 3q + 2)$$

па је $x^2 = 9q^2 + 6q + 1$(односно $x^2 = 9q^2 + 12q + 3 + 1$) и слично и за y, z.

То значи да је $x^2 \equiv y^2 \equiv z^2 \equiv 1 \pmod 3$.

Из полазне једначине добијамо да је $1+1 \equiv 1 \pmod 3$,што није тачно. Дакле,претпоставка не важи,па је бар један од бројева x, y, z дјељив са 3. □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

163

Доказати да је број $20^{15} - 1$ дјељив са $11 \cdot 31 \cdot 61$.

Доказ. Показаћемо посебно дјељивост овог броја са сваким од простих фактора.
Имамо

$$20 \equiv 9 \pmod{11},$$
$$20^2 \equiv 81 \equiv 4 \pmod{11},$$
$$20^4 \equiv 6561 \equiv 5 \pmod{11},$$
$$20^8 \equiv 25 \equiv 3 \pmod{11},$$

Множењем ових конгруенција добијамо

$$20^{15} \equiv 9 \cdot 4 \cdot 5 \cdot 3 \equiv 1 \pmod{11}$$

па је

$$20^{15} - 1 \equiv 0 \pmod{11}.$$

Слично добијамо за преостала два фактора

$$20 \equiv -11 \pmod{31},$$
$$20^2 \equiv 121 \equiv -3 \pmod{31},$$
$$20^4 \equiv 9 \pmod{31},$$
$$20^8 \equiv 81 \equiv -12 \pmod{31},$$

$$20^{15} \equiv (-11) \cdot (-3) \cdot 9 \cdot (-12) \equiv -3564 \equiv 1 \pmod{31},$$

па је

$$20^{15} - 1 \equiv 0 \pmod{31}.$$

$$20 \equiv 20 \pmod{61}.$$
$$20^2 \equiv 400 \equiv 34 \pmod{61}.$$
$$20^4 \equiv 1156 \equiv -3 \pmod{61},$$
$$20^8 \equiv 9 \pmod{61}.$$

$$20^{15} \equiv (20) \cdot 34 \cdot (-3) \cdot 9 \equiv -18360 \equiv 1 \pmod{61},$$

па је

$$20^{15} - 1 \equiv 0 \pmod{61}.$$

□

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`https://www.fer.unizg.hr/_download/repository/diskont1-11.pdf`

164

●●●●

Наћи остатак при дијељењу броја 66^{15} са 7.

Доказ. $66 = 7 \cdot 9 + 3 \implies 66 - 3 = 7 \cdot 9 \implies 7|66 - 3 \implies 66 \equiv 3 \pmod 7 \implies 66^{15} \equiv 3^{15} \pmod 7$.
Бројеви 66^{15} и 3^{15} имају исти остатак при дијељењу са 7.
Сада тражимо остатак при дијељењу броја 3^{15} са 7.
Како је $3^{15} = (3^3)^5 = 27^5$ имамо:
$27 = 7 \cdot 3 + 6 \implies 27 \equiv 6 \pmod 7 \implies 27^5 \equiv 6^5 \pmod 7$
Видимо да бројеви 27^5 и 6^5 имају исти остатак при дијељењу са 7,па тражимо остатак при дијељењу 6^5 са 7.
Како је $6 \equiv -1 \pmod 7 \implies 6^5 \equiv (-1)^5 \pmod 7 \implies 6^5 \equiv -1 \pmod 7$
Дакле, тражени остатак је једнак остатку при дијељењу -1 са 7.
Пошто је $-1 = 7 \cdot (-1) + 6$ закључујемо да је остатак при дијељењу 66^{15} са 7 једнак 6. □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.ss-ilok.skole.hr/dokumenti?dm_document_id=104&dm_dnl=1`

165

●●●●

За $n \geqslant 0$, показати да је

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

Доказ. Доказ изводимо математичком индукцијом.

Примијетимо да је за $n = 1$

$$(-13)^2 = 169 \equiv -12 \pmod{181}$$

Са друге стране је

$$(-13)^1 + (-13)^0 = -13 + 1 = -12 \pmod{181}$$

Претпоставимо да дата конгруеција важи за $n \in N$, тј.

$$(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$$

Сада, за $n+1$

$$(-13)^{n+1}+1 \equiv (-13)[(-13)^{k+1}] \pmod{181} \equiv (-13)[(-13)^{k}+(-13)^{k-1}]$$
$$\pmod{181} \equiv (-13)^{k+1}+(-13)^{k} \pmod{181}$$

а то је управо оно што је и требало доказати. □

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.math.ust.hk/excalibur/v20_n2.pdf`

166 ●●●●

Доказати да постоји бесконачно много простих бројева конгруентних са $3 \pmod 4$

Доказ. Претпоставимо супротно, дакле да постоји коначно много бројева $p_1, p_2, \ldots, p_r$ који су $\equiv 3 \pmod 4$, при чему је један од њих, рецимо $p_1 = 3$. Сви они задовољавају услов: $p_j \equiv 3 \pmod 4$, и на основу наше претпоставке, то су једини прости бројеви са тим својством.

Конструишимо сада број A облика $A = 4p1\cdots pr - 1$. Видимо да је $A \equiv -1 \equiv 3 \pmod 4$

Примијетимо да никоје p_j не дијели A. У супротном, да постоји неко $p_j \in p_1, \ldots, p_r$ такво да $p_j \mid A$, а очигледно је да $p_j \mid A+1$, то би значило да $p_j \mid (A+1-A) = 1$, дакле, да је $p_j = 1$, што није прост број.

Посматрајмо број A. Разликујемо 2 случаја:

1. A - прост број. У том случају, дошли смо до контрадикције показавши да постоји још један прост број са својством да је $\equiv 3 \pmod 4$, и тиме је доказ завршен. У супротном,
2. A - сложен број. Посматрајмо његове просте факторе q_i. Постоји макар једно q_i, $q_i \equiv 3 \pmod 4$. Ово мора важити јер су фактори броја A прости, дакле непарни (јер је и A непаран), стога ниједан фактор q_i не може бити конгруентан са 0 или $2 \pmod 4$. То би онда значило да су сви фактори броја A, па и он сам конгруентни са $1 \pmod 4$ чиме бисмо опет дошли у контрадикцију са почетном претпоставком.

□

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.docsity.com/en/congruence-number-theory-exam/256385/`

167 ●●●●

Које цифре треба уписати умјесто x и y у броју $30x0y03$ да би резултат био дјељив са 13?

као збир

Доказ. Број $n = 30x0y03$ можемо записати као $3 \cdot 10^6 + x \cdot 10^4 + y \cdot 10^2 + 3$.

Знамо да важи следеће:

$$10^2 \equiv 9 \pmod{13}$$

Из овога даље можемо закључити:

$$10^2 \cdot 10 \equiv 9 \cdot 10 \pmod{13} \Rightarrow 10^3 \equiv 90 \pmod{13} \Rightarrow 10^3 \equiv 12 \pmod{13}$$

Сличним резоновањем добијамо:

$$10^4 \equiv 3 \pmod{13}$$

$$10^5 \equiv 4 \pmod{13}$$

$$10^6 \equiv 1 \pmod{13}$$

Сада за број n важи:

$n \equiv 3 + 3x + 9y + 3 \equiv 0 \pmod{13}$

$\Rightarrow 3x + 9y + 6 \equiv 0 \pmod{13}$

$\Rightarrow 3x + 9y + 6 \equiv -6 \equiv 7 \equiv 20 \equiv 30 \pmod{13}$

$\Rightarrow 3(x + y) \equiv 33 \pmod{13}$

Дијелимо ову конгруенцију са 3, што значи да модуо морамо подијелити са нзд$(3, 13) = 1$. Дакле,

$$x + 3y \equiv 11 \pmod{13}$$

Замјеном једне промјенљиве, рецимо y цифрама од 0 до 9 добијамо могуће вриједности парова (x, y), а то су:

$(8, 1), (5, 2), (2, 3), (9, 5), (6, 6), (3, 7)$ и $(9, 8)$. □

(**Маријана Велетић 19/19 Ц**)задатак преузет са `https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

168

Природни бројеви N и N^2 у декадном запису се завршавају истим низом од 4 цифре $abcd, a > 0$. Наћи број abc.

Доказ. $N^2 - N = N(N-1) \equiv 0 \pmod{10000}$.

$10000 = 2^4 \cdot 5^4$, дакле $N(N-1)$ мора бити дјељиво и са 5^4 и 2^4. Међутим, примијетимо да ако N или $N-1$ имају и 2 и 5 у својој факторизацији, други се мора завршити са 9 или 1 (респективно), што би значило да он није дјељив ни са 2 ни са 5. Из овога закључујемо да је један дјељив са $5^4 = 625$, а други са $2^4 = 16$.

Један овакав кандидат је $N = 625$ јер је, наравно, $625 \equiv 0 \pmod{365}$, а такође је и $625 \equiv 1 \pmod{16}$, па је $N-1$ дјељиво са 16. Међутим, $625^2 = 390625$, што не одговара услову да је $a > 0$.

Друга опција је да N буде дјељиво са 16, а $N-1$ са 625. То значи да $N-1$ мора бити $\equiv -1 \pmod{16}$. Већ смо навели да је $625 \equiv 1 \pmod{16}$. На основу тога је $625 \cdot 15 \equiv 15 \equiv -1 \pmod{16}$.

Дакле, $N - 1 = 625 \cdot 15 = 9375 \Rightarrow N = 9376$. Тражени број abc је 937. □

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://artofproblemsolving.com/downloads/printable_post_collections/4911`

169

Која је величина највећег подскупа S скупа $\{1, 2, \ldots, 50\}$ таквог да у њему не постоји пар различитих елемената који у збиру даје 7?

Доказ. Прво, примијетимо да постоји 8 бројева који су $1 \leqslant a \leqslant 50$ који су $\equiv 1 \pmod 7$ $(1, 8, 15, 22, 29, 36, 43, 50)$ и по 7 бројева који су конгруентни са сваким од бројева $2 - 6 \pmod 7$.

Даље, примијетимо да не може постојати пар бројева (a, b) такав да је $a \equiv -b \pmod 7$ јер би то значило да $(a + b) \mid 7$. Ово су парови $(1, 6)$, $(2, 5)$ и $(3, 4)$. У скупу S се смије појавити само један број $\equiv 0 \pmod 7$.

Да бисмо оформили скуп са највећим могућим бројем елемената, узећемо 1 број $\equiv 0 \pmod 7$, 8 бројева $\equiv 1 \pmod 7$ (они ће у збиру убијек дати број $\equiv 1 \pmod 7$) и 14 бројева који су $\equiv 2 - 5 \pmod 7$. Бројеве $\equiv 6 \pmod 7$ не можемо уврстити у скуп јер би они дали број дјељив са 7 у комбинацији са бројевима који су $\equiv 1 \pmod 7$ које смо већ додали. Од преосталих 28 могућих бројева бирамо двије групе, и то тако да то нису истовремено група која даје остатак 3 и она која даје остатак 4 при дијељењу са 7, или двије које дају остатке 5 и 2.

На основу наведеног, одговор је да је скуп S скуп од највише $1 + 8 + 14 = 23$ елемента. □

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

3 Прости бројеви

170 ●●●●

Нека су a и b природни бројеви и нека за свако $n \in \mathbb{N}$, a^n+n дијели b^n+n. Доказати да је $a = b$.

Доказ. Претпоставимо супротно, $a \neq b$. Видимо да ће морати да буде $a < b$. Нека је p прост број већи од b. Посматрајмо $n = (a+1)(p-1)+1$. Имамо $n \equiv 1 \pmod{p-1}$ и $n \equiv -a \pmod{p}$. За свако $r \in \mathbb{N}$ важи по Малој Ферамаовој теореми

$$r^n = r(r^{a+1})^{p-1} \equiv r \pmod{p}$$

Одакле имамо да

$$a^n \equiv a \pmod{p}$$

Заједно са $n \equiv -a \pmod{p}$

$$a^n + n \equiv 0 \pmod{p}$$

Како је $b^n + n$ дјељив са $a^n + n$ видимо да је $b^n + n$ дјељив са p. Имамо $b^n + n \equiv b - a \pmod{p}$, што је немогуће јер би било $b - a > 0$, $b - a < p$ и $p | b - a$. Контрадикција је настала јер смо претпоставили да $a \neq b$. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из
104 Number Theory Problems From the Training of the USA IMO Team

171 ●●●●

Нека је дат прост број p, $p > 3$. Доказати да ако једначина $p^k+p^l+p^m = n^2$ има цјелобројних рјешења, тада $8|p+1$.

Доказ. Нека једначина $p^k+p^l+p^m = n^2$ има цјелобројних рјешења. Без губљења општости претпоставимо да $k \geq l \geq m$. Тада једначину можемо записати у облику

$$p^m(p^{k-m} + p^{k-m} + 1) = n^2$$

Ако је $l > m$, имамо да $p \mid (p^{k-m} + p^{k-m})$, па је $p \nmid (p^{k-m} + p^{k-m} + 1)$
Ако је $l = m, k > m$, имамо да $p \mid p^{k-m}$,па је $p \nmid (p^{k-m} + 1 + 1)$
Ако је $k = l = m$, имамо да $p \nmid (1 + 1 + 1)$, jer је $p > 3$
Како p не може да дијели $(p^{k-m} + p^{l-m} + 1)$. Можемо да закључимо да је m паран број. Па је и $(p^{k-m} + p^{k-m} + 1)$ квадрат неког природног борја i. $(p^{k-m} + p^{k-m} + 1)$ је непаран број, па је и i непаран број. i можемо записати у облику

$$i = 8 \cdot k + 1$$

$$i = 8 \cdot k - 1$$

$$i = 8 \cdot k + 3$$

$$i = 8 \cdot k - 3$$

У сваком случају добијамо да је $i^2 \pmod{8} = 1$.
Како је p прост број већи од три, то се и он може записати у облику

$$p = 8 \cdot k + 1$$

$$p = 8 \cdot k + 3$$

$$p = 8 \cdot k + 5$$

$$p = 8 \cdot k + 7$$

Провјером закључујемо да је немогуће да $i \pmod{8} = 1$ за прва три случаја, па је једино могуће $p = 8 \cdot k + 7$ односно $8 \mid (p + 1)$. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет са
`http://refkol.ro/matek/mathbooks/Olympiad%20Stuff/1220NT.pdf`

172

Нека су p и q прости бројеви, $p - 1$ дјељив са q, $q^3 - 1$ дјељив са p, онда је $p = 1 + q + q^2$. Доказати.

Доказ.

$$q|(p-1)$$

$$p|(q-1) \cdot (q^2 + q + 1)$$

Како је p прост, то p дијели $q + 1$ или $q^2 + q + 1$. Претпоставимо да $p|(q - 1)$, тада

$$p \cdot k_1 = q - 1, \ k_1 \geqslant 1$$

$$q \cdot k_2 = p - 1, \ k_2 \geqslant 1$$

Па је

$$(q \cdot k_2 + 1)k_1 = q - 1$$

$$(q \cdot k_2 + 1)k_1 + 1 = q$$

Што је немогуће јер $(q \cdot k_2 + 1) \cdot k_1 \geqslant q$. Закључујемо да $p|(q^2 + q + 1)$.

$$q(q+1) = k \cdot p - 1, \;\; k \geqslant 1$$

Имамо да је $q|(p-1)$, па је $q \leqslant p-1$, односно $q+1 \leqslant p$. Како је $q(q+1) = k \cdot p - 1 > (k-1) \cdot p$ закључујемо да је $q > k - 1$.

$$q(q+1) = k \cdot (p-1) + k - 1, \;\; k \geqslant 1$$

$$q(q+1) - k \cdot (p-1) = k - 1, \;\; k \geqslant 1$$

Из посљедње једнакости видимо да $q|(k-1)$. Пошто је $q > k - 1$ добијамо да је $k - 1 = 0$, односно $k = 1$. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

173

Могу ли природни бројеви $n-2012$, n, $n+2012$ бити истовремено прости?

Доказ. Не. Претпоставимо супротно. Како је $n - 2012$ прост, то је n>3. Па се n може записати у облику $3k+1$ или $3k-1$. Нека је $n = 3k+1$, тада је $n+2012 = 3k+2013$ дјељив са 3. Нека је $n = 3k-1$, тада је $n - 2012 = 3k - 2013$ дјељив са 3. Закључујемо да не могу сва три броја истовремено бити прости. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

174

Ако је p прост број, доказати да је $N = \frac{(2p)!}{(p!)^2} - 2$ дјељив са p^2.

Доказ.

$$\frac{(2p)!}{(p!)^2} = \binom{2p}{p} = \sum_{i=0}^{p} \binom{p}{i}^2 = \binom{p}{0}^2 + \binom{p}{p}^2 + \sum_{i=1}^{p-1} \binom{p}{i}^2 = 2 + \sum_{i=1}^{p-1} \binom{p}{i}^2$$

Па је

$$\frac{(2p)!}{(p!)^2} - 2 = \sum_{i=1}^{p-1} \binom{p}{i}^2$$

Како је p прост, то је сваки од чланова суме дјељив са p^2 јер је $\binom{p}{i}$ дјељив са p кад је p прост. Закључујемо да је N дјељиво са p. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

175

Одредити са колико се нула завршава број 1000! .

Доказ. Познато нам је сљедеће тврђење (доказано је на часу) :
Ако су $n, p \in \mathbb{N}$ такви да је p прост и $p \leq n$, онда је степен броја p у факторизацији $n!$ једнак

$$\sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$$

Претходна сума је коначна јер за довољно велико k члан $\left\lfloor \frac{n}{p^k} \right\rfloor = 0.$
Примјетимо да број 0 на крају неког природног броја зависи од броја 10-ки , прецизније од броја 2-ки и 5-ица које се јављају у канонској факторизацији тог природног броја. Дакле , потребно је наћи број понављања простих фактора 5 и 2 тј. њихов експонент у факторизацији броја $n!$.
На основу наведеног тврђења добијамо да је број понављања фактора 5 односно фактора 2 једнак

$$\sum_{k=1}^{\infty} \left\lfloor \frac{1000}{5^k} \right\rfloor = 200 + 40 + 8 + 1 + 0 + \cdots = 249$$
$$\sum_{k=1}^{\infty} \left\lfloor \frac{1000}{2^k} \right\rfloor = 500 + 250 + 125 + 62 + 31 + 15 + 7 + 3 + 1 + 0 + \cdots = 994$$

Даље закључујемо да је $n! = 5^{249} \cdot 2^{994} \cdot \ldots = 10^{249} \cdot 2^{745} \cdot \ldots \implies$ број $n!$ се завршава са 249 нула. ☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`http://www.its.caltech.edu/~kpilch/olympiad/NumberTheory-Complete.pdf`

176

Нека је број $2^k + 1$ прост. Доказати да је тада $k = 0$ или $k = 2^n$ за неки $n \geq 0$.

Доказ. Претпоставимо да k има неки непаран прости фактор p. Тада из $k = p \cdot m$ слиједи да је број

$$2^k + 1 \;=\; (2^m)^p + 1^p = (2^m + 1)(2^{m(p-1)} - 2^{m(p-2)} + ... + 1)$$

дјељив са $2^m + 1$, па није прост.

Бројеви $f_n = 2^{2^n} + 1$ називају се Фермаови бројеви. Сматрао је да су сви они прости. Када уврстимо n добијамо $f_0 = 3$, $f_1 = 5$, $f_2 = 17$, $f_3 = 257$ и $f_4 = 65537$ и они су заиста прости. Међутим, $f_5 = 2^{32} + 1$ је сложен. То видимо из следећег:

$$\begin{aligned}2^{32}+1 &= 2^4\cdot 2^{28}+1=(641-5^4)\cdot 2^{28}+1=641\cdot 2^{28}-(5\cdot 2^7)^4+1\\ &= 641\cdot 2^{28}-(641-1)^4+1\\ &= 641\cdot(2^{28}-641^3+4\cdot 641^2-6\cdot 641+4).\end{aligned}$$

Према томе, $641|f_5$.
Хипотеза је да је само коначно много Фермаових бројева просто. □

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

177 ●●●●

Доказати:

1. Ако је p прост број, тада је $p^{2011}+p^{2013}$ сложен
2. Да број $2^{10}+3^{12}$ није прост
3. Да је $p=2$ једини прост број за који важи да је 3^p+p^3 прост.

Доказ.

1. Ако је $p=2$ тада је $2^{2011}+2^{2013}$ збир два парна броја, који је паран број, па самим тим и сложен. Нека је p прост број тако да је $p\geq 3$. Он је онда и непаран. Али, и непаран степен непарног броја ће бити непаран број, па је збир $p^{2011}+p^{2013}$ збир два непарна броја, а то је паран број. Па пошто је паран он је и сложен, што је и требало показати.

2. Можемо извршити следећу трансформацију у запису:

$$2^{10}+3^{12}=(2^5)^2+(3^6)^2$$

и пробати да направимо квадрат бинома у коме ће нам 2^5 и 3^6 бити чланови. То ћемо постићи додавњем и одузимањем члана $2\cdot 2^5\cdot 3^6$. Па ћемо имати

$$\begin{aligned}2^{10}+3^{12} &= (2^5)^2+(3^6)^2\\ &= (2^5)^2+2\cdot 2^5\cdot 3^6+(3^6)^2-2\cdot 2^5\cdot 3^6\\ &= (2^5+3^6)^2-2^63^6\\ &= (2^5+3^6)^2-6^6\\ &= (2^5+3^6)^2-(6^3)^2\\ &= (2^5+3^6+6^3)(2^5+3^6-6^3)\end{aligned}$$

Последњи израз нам потврђује да је број $2^{10}+3^{12}$ сложен.

3. За $p = 2$ је и $3^2 + 2^3 = 17$ прост, а за друге прост бројеве p, који су уз то и непарни, збир $3^p + p^3$ је збир два непарна броја, па је он паран, а самим тим и сложен. Дакле, број $3^p + p^3$ је прост једино за $p = 2$.

$\square$

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

178

●●●○

Да ли постоји прост број p који се може представити у облику збира кубова два природна броја? Доказати.

Доказ. Ако такав прост број p постоји, он би се могао представити као:

$$p = a^3 + b^3$$

гдје су a и b природни бројеви. Сада нам је неопходно познавање формуле за растављање збира кубова: $a^3 + b^3 = (a + b) \cdot (a^2 - ab + b^2)$, па кад њу искористимо имамо да је

$$p = (a + b) \cdot (a^2 - ab + b^2).$$

Пошто прост број нема других дјелилаца, осим самог себе и јединице, и због чињенице да је $a + b > 1$, имаћемо да је:

$$a^2 - ab + b^2 = 1.$$

Ријешимо ову једначину у скупу природних бројева.
Она је еквивалентна са: $2a^2 - 2ab + 2b^2 = 2$. Односно, сређивањем претходног израза имамо да је $a^2 + b^2 + (a - b)^2 = 2$. Одавде добијамо да је једино рјешење, за нас интересантно, $a = 1$ и $b = 1$, јер је услов да буду природни бројеви. Из овога добијамо да постоји прост број $p = 2$ за природне бројеве $a = 1$ и $b = 1$, такав да је $p = 2 = 1^3 + 1^3$. Друге могућности не постоје. $\square$

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

179

●●○○

Одредити, ако постоји, прост број p такав да $p^2 \mid 5^{p^2} + 1$.

Доказ. Ако претпоставимо да постоји прост бриј p који задовољава тражени услов, тада према Малој Фермаовој теореми имамо $5^p \equiv 5 \pmod{p}$, а одатле и $5^{p^2} \equiv 5^p \pmod{p}$, па је

$$5^{p^2} \equiv 5^p \equiv 5 \pmod{p}$$

и

$$5^{p^2} + 1 \equiv 6 \pmod{p}.$$

С друге стране, из услова $p^2 \mid 5^{p^2}+1$, слиједи да је

$$5^{p^2}+1 \equiv 0 \pmod{p}.$$

Дакле, $6 \equiv 0 \pmod{p}$, па $p \in \{2,3\}$.

- За $p=2$ имамо да је $5^4+1=626 \equiv 2 \pmod{4}$, па 2 не задовољава услов задатка.
- За $p=3$ имамо $5^9+1=1953126=9\cdot 217014 \equiv 0 \pmod{9}$, па је 3 једини прост број који задовољава услов задатка.

□

(**Радоман Гледовић 6/19 Ц**) задатак преузет из
Збирка ријешених задатака из теорије бројева - Небојша Икодиновић

180

Одредити све парове простих природних бројева p и q за које постоји цијели број a такав да вриједи $a^4 = pa^3 + q$.

Доказ. Ако су p и q прости и a цијели број за који вриједи $a^4 = pa^3+q$, онда је $a^3(a-p)=q$, те закључујемо да a^3 дијели прост број q. Према томе, a може бити само 1 или -1. Ако је $a=1$, онда је $1-p=q$. Пошто такви прости бројеви не постоје, слиједи да је $a=-1$, па имамо да је $1+p=q$, а то је једино могуће за $p=2$ и $q=3$. □

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

181

Нека је $n \geq 2$ природан број и p прост број. Ако је број $p-1$ дјељив бројем n, а број n^3-1 дјељив бројем p, доказати да је $4p-3$ квадрат неког природног броја.

Доказ. По услову задатка дато је да n дијели $p-1$, па слиједи да постоји природан број a такав да је

$$(1) \qquad p-1 = an.$$

Закључујемо да је $p-1 \geq n$. Из услова да је $n^3-1=(n-1)(n^2+n+1)$ дјељив простим бројем p, слиједи да је n^2+n+1 дјељив са p.
(***Напомена:*** У изразу $(n-1)(n^2+n+1)$, $n-1$ не може бити дјељив са p јер је $p > n-1$)
Сада слиједи, да постоји природан број b такав да је

$$(2) \qquad n^2+n+1 = bp.$$

Комбиновањем једнакости (1) и (2) добијамо:

$$n^2+n+1 = b(an+1),$$

односно

$$n(n+1-ab) = b-1.$$

Означимо са $c = n+1-ab$. Како је $b-1 \in \mathbb{N}_0$ слиједи да је и $c \in \mathbb{N}_0$, па је

$$b = cn+1.$$

Сада имамо

$$n^2+n+1 = bp = (cn+1)(an+1) = acn^2+(a+c)n+1,$$

па одузимањем јединице и дијељењем са n добијамо

$$(3) \qquad n+1 = acn+a+c.$$

Како знамо да су $a, n \in \mathbb{N}$, претходна једнакост може бити испуњена једино ако је $c = 0$. Дакле, слиједи да је $b = 1$ и $p = n^2+n+1$ што повлачи да је $4p-3 = 4n^2+4n+1 = (2n+1)^2$. ***Напомена:*** У изразу (3) ако бисмо за c узели било који позитиван број већи од нуле једнакост не би била задовољена. Најједноставнији случај јесте ако узмемо да је $a = 1$ и $c = 1$. Тада добијамо да је $n+1 = n+2$ што није тачно. Важи и за остале бројеве веће од један. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

182

Нека је p прост број и a цио број узајамно прост са p . Дефинишимо

$$\operatorname{ord}(a) = \min\{k \in \mathbb{N} \mid a^k \equiv 1 \pmod{p}\}$$

Доказати да $\operatorname{ord}(a) \mid p-1$.

Доказ. Користећи алгоритам дијељења добијамо

$$p-1 = \operatorname{ord}(a)\cdot k + s \ , \ k \in \mathbb{Z} \ , \ 0 \le s < \operatorname{ord}(a)$$

Потребно је доказати да је $s = 0$. Како је нзд$(a, p) = 1$ из Фермаове мале теореме слиједи да је:

$$a^{p-1} \equiv 1 \pmod{p}$$

Из тога даље добијамо

$$1 \equiv a^{p-1} \equiv a^{\operatorname{ord}(a)\cdot k+s} \equiv \text{(po definiciji ord)} \equiv$$
$$1^k \cdot a^s \equiv a^s \pmod{p}$$

Дакле , $a^s \equiv 1 \pmod{p}$ и $0 \le s < \operatorname{ord}(a)$, одакле слиједи да је $s = 0$. ☐

(**Велимир Ћоровић 5/19 Б**) задатак преузет са
`http://www.math.ubc.ca/~bennett/Math312/312psol2.pdf`

183

Нека је $p > 3$ прост број . Доказати да се број $4p^2 + 1$ може представити као збир квадрата три различита природна броја .

Доказ. Нека је $p > 3$ прост број . Тада p може бити само облика $p = 6k \pm 1$, јер остали облици не могу бити прости , што закључујемо на основу сљедећег

$$\begin{aligned} 6k &= 6 \cdot k \\ 6k + 2 &= 2(3k + 1) \\ 6k + 3 &= 3(2k + 1) \\ 6k + 4 &= 2(3k + 2) \end{aligned}$$

Дакле за $p = 6k \pm 1$ посматрамо број $4p^2 + 1$.

$$4p^2 + 1 = 4(6k \pm 1)^2 + 1 = 144k^2 \pm 48k + 5$$

Циљ нам је да $4p^2 + 1$ запишемо као збир 3 квадрата . Како је $5 = 2^2 + 1^2$ покушаћемо да формирамо 2 квадрата бинома и један 'слободан' квадрат

$$\begin{aligned} 4p^2 + 1 = (ak + 1)^2 + (bk + 2)^2 + (ck)^2 &= (a^2 + b^2 + c^2)k^2 + (2a + 4b)k + 5 = \\ &= 144k^2 \pm 48k + 5 \end{aligned}$$

гдје су a, b и c непознате које задовољавају сљедећи систем једначина

$$\begin{aligned} &a^2 + b^2 + c^2 = 144 \\ &a + 2b = \pm 24 \end{aligned}$$

Наравно тражимо да $a, b, c \neq 0$. Морамо ријешити систем за $+$ и $-$.

Посматрајући конкретно $p = 7 = 6 \cdot 1 + 1$ можемо олакшати рјешавање система

$$4 \cdot 7^2 + 1 = 10^2 + 9^2 + 4^2$$

На основу претходног можемо 'погодити' рјешење $(a, b, c) = (8, 8, 4)$. Након провјере закључујемо у случају $p = 6k + 1$ рјешење је $(a, b, c) = (8, 8, 4)$.

Сада ставимо $p = 5 = 6 \cdot 1 - 1$ онда је

$$4 \cdot 5^2 + 1 = 7^2 + 6^2 + 4^2$$

На основу претходног опет можемо 'погодити' рјешење $(a, b, c) = (-8, -8, 4)$.Након провјере закључујемо у случају $p = 6k - 1$ рјешење је $(a, b, c) = (-8, -8, 4)$.

Коначно ,

$$4p^2 + 1 = \begin{cases} (8k + 1)^2 + (8k + 2)^2 + (4k)^2 & , \ p = 6k + 1 \\ (8k - 1)^2 + (8k - 2)^2 + (4k)^2 & , \ p = 6k - 1 \end{cases}$$

□

(**Велимир Ћоровић 5/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/TBr_JBMO_vb.pdf`

184

Доказати:
а) Ако је p прост број, онда $\binom{p}{k}$ је дјељиво са p за свако $0 < k < p$.
б) Доказати да ако је p прост број, онда $p \mid 2^p - 2$.

Доказ. а)

$$\binom{p}{k} = \frac{p(p-1)\cdot\ldots\cdot(p-k+1)}{k!}$$
$$\implies \quad k!\binom{p}{k} = p(p-1)\cdot\ldots\cdot(p-k+1)$$

Из чега видимо да $p \mid k!\binom{p}{k}$. Како $k < p$ і $p \nmid k!$, слиједи да $p \mid \binom{p}{k}$.
б) Користећи Биномну теорему:

$$2^p - 2 = (1+1)^p - 2 = \binom{p}{0} + \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{p-1} + \binom{p}{p} - 2 =$$
$$= \binom{p}{1} + \binom{p}{2} + \ldots + \binom{p}{p-1}$$

Користећи задатак под а), видимо да p дијели све сабирке. Слиједи да $p \mid 2^p - 2$.

□

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

185

(а) Сваки природан број већи од 1 садржи прости фактор.
(б) Природан број n је сложен акко садржи прост фактор p такав да $p \le \sqrt{n}$.

Доказ. (а) Нека је n природан број већи од 1. Тврђење доказујемо (трансфинитном) индукцијом по n. За $n = 2$, јасно. Нека тврђење важи за све природне бројеве мање од n. Докажимо да важи за n.
Разматрамо случајеве:
1. Нека је n прост број. Тада је управо n тај прости фактор.
2. Нека је n сложен број. Тада постоји природан број t, $t \mid n$. Како је $1 < t < n$ то онда по индуктивној претпоставци постоји прост број p такав да $p \mid t$. Како $p \mid t \ \wedge \ t \mid n \Rightarrow p \mid n$.
Дакле, тврђење важи за сваки природан број већи од 1.

(б) Нека је n природан број који садржи прост фактор p такав да $p \le \sqrt{n}$. Тада постоји природан број k, $n = p \cdot k$. Из $p \le \sqrt{n} \ \Rightarrow \ k \ge p$.
Обрнуто, нека је n сложен број. Тада постоји природан број t, $t \mid n$. За дато t, постоји s, $n = t \cdot s$. Како је $s \ne 1 \wedge s \ne n$, то онда $1 < s < n$. Без смањења општости, нека је $1 < t \le s$. Тада, на основу (а), постоји прост број p такав да $p \mid t$.

$$\Rightarrow p\ \leq t\ \wedge p\ \leq s\ \Rightarrow\ p^2 \leq t \cdot s = n\ \Rightarrow\ p \leq \sqrt{n}.$$

☐

(**Сандра Вујичић 2/19 Б**) задатак преузет са `http://nasport.pmf.ni.ac.rs/materijali/175/TBP%20predavanja%20nv%202018-2019.pdf`

186

Доказати да је n^4+4 сложен број за свако $n>1$.

Доказ. Израз n^4+4 ћемо написати као производ 2 природна броја различита од 1.

$$\begin{aligned} &n^4+4 = \text{ (додајемо и одузимамо } 4n^2 \text{)}\\ =&n^4+4n^2+4-4n^2=\\ =&(n^2+2)^2-(2n)^2 = \text{(разлика квадрата)}\\ =&(n^2+2n+2)(n^2-2n+2)\end{aligned}$$

Израз $n^2+2n+1>1$ за $n>1$. Функција $f(x)=x^2-2x+2$ је строго растућа на интервалу $(1,+\infty)$ и $f(1)=1$, па одатле закључујемо да је $(n^2-2n+2)>1$ за $n>1$.

Дакле , написали смо број n^4+4 као производ 2 природна броја различита од 1 , закључујемо да је n^4+4 сложен за $n>1$.

Напомена Разлагање коришћено у задатку је специјалан случај идентитета Софије Жермејн (Sophie Germain) . Више можете погледати на `https://www.cut-the-knot.org/blue/SophieGermainIdentity.shtml` . ☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет са `https://dms.rs/wp-content/uploads/2017/03/TeorijeBrojeva_MarijaC.pdf`

187

Наћи све позитивне цијеле бројеве a,b за које је a^4+4b^4 прост број.

Доказ.

$$\begin{aligned} a^4+4b^4 &= a^4+4b^4+4a^2b^2-4a^2b^2=\\ &=(a^2+2b^2)^2-4a^2b^2=\\ &=(a^2+2b^2+2ab)(a^2+2b^2-2ab)=\\ &=[(a+b)^2+b^2][(a-b)^2+b^2]\end{aligned}$$

Како је $(a+b)^2+b^2>1$, то a^4+4b^4 може бити прост број само ако је $(a-b)^2+b^2=1$ што важи само за $a=b=1$.

☐

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

188

Нека је n позитивни цијели број. Конструисати скуп од n узастопних позитивних цијелих бројева који нису прости.

Доказ. Нека је n позитивни цијели број.
Конструишимо на следећи начин: $(n+1)!+2,\ (n+1)!+3, \dots, (n+1)!+(n+1)$ n узастопних позитивних цијелих бројева.

$$\forall i = 2, \dots, n-1 \quad i \mid (n+1)! + i$$
$$\frac{(n+1)!}{i} > 0 \implies \frac{(n+1)!+i}{i} = \frac{(n+1)!}{i} + 1 > 1$$

Па можемо да закључимо да је $(n+1)!+i$ је производ 2 цијела броја различита од 1. Дакле, $(n+1)!+i$ је сложен број. ☐

(**Милена Јововић 1/19 Б**) задатак преузет са
`http://math.cmu.edu/~cargue/arml/archive/16-17/number-theory-09-11-16-solutions.pdf`

189

(1999 Математичка олимпијада у Румунији) Нека су a, b, c цијели бројеви различити од 0, $a \neq c$ такви да $\frac{a}{c} = \frac{a^2+b^2}{c^2+b^2}$ Доказати да $a^2+b^2+c^2$ не може бити прост број.

Доказ.

$$\frac{a}{c} = \frac{a^2+b^2}{c^2+b^2}$$
$$a(c^2+b^2) = c(a^2+b^2)$$
$$ac^2+ab^2-ca^2-cb^2 = 0$$
$$ac(c-a) - b^2(c-a) = 0$$
$$(ac-b^2)(c-a) = 0$$

Како $a \neq c$, закључујемо да мора $ac = b^2$. Па,

$$a^2+b^2+c^2 = a^2+ac+c^2 = a^2+2ac-b^2+c^2 =$$
$$= (a+c)^2 - b^2 = (a+c-b)(a+c+b)$$

Kako $a^2+b^2+c^2>3$, онда ако је то заиста прост број, могућа су следећа 4 случаја:
(1) $a+c-b=1$ i $a+c+b=a^2+b^2+c^2$
(2) $a+c-b=-1$ i $a+c+b=-(a^2+b^2+c^2)$
(3) $a+c+b=1$ i $a+c-b=a^2+b^2+c^2$
(4) $a+c+b=-1$ i $a+c-b=-(a^2+b^2+c^2)$
Ријешавамо први случај

$$a+c-b=1 \implies a+c=b+1$$

Посматрамо

$$\begin{aligned}&a^2+b^2+c^2-2(a+c)+1=\\&=a+c+b-2a-2c+1=\\&=-a-c+b+1=\\&=-(a+c)+b+1=\\&=-(b+1)+b+1=0\end{aligned}$$

Дакле

$$a^2+b^2+c^2-2(a+c)+1=0$$

тј.

$$(a-1)^2+b^2+(c-1)^2=1$$

одакле слиједи

$$\begin{aligned}&a-1=0 \implies a=1\\&c-1=0 \implies c=1\\&\implies a=c\end{aligned}$$

што је контрадикција са претпоставком.
Прелазимо на други случај

$$a+c-b=1 \implies a+c=b-1$$

Посматрамо

$$\begin{aligned}&a^2+b^2+c^2+2(a+c)+1=\\&=-a-c-b+2a+2c+1=\\&=a+c-b+1=\\&=b-1+b+1=0\end{aligned}$$

Дакле

$$a^2+b^2+c^2+2(a+c)+1=0$$

тј.

$$(a+1)^2 + b^2 + (c+1)^2 = 1$$

одакле слиједи $a = c$ што је контрадикција са претпоставком.
Слично ријешавамо трећи случај $a + c + b = 1 \implies a + c = 1 - b$. Пролазећи кроз сличан поступак, добијамо $(a-1)^2+b^2+(c-1)^2 = 1$ одакле опет слиједи $a = c$ што је контрадикција са претпоставком.
И четврти случај, аналогно ријешавајући, добијамо $(a+1)^2 + b^2 + (c+1)^2 = 1$ одакле опет слиједи $a = c$. Контрадикција.

Други начин: Из $b^2 = ac$ можемо да закључимо да a и c морају бити истог знака. Отуда, замјенимо их са њиховим негативним вриједностима ако је потребно. Претпоставимо $a, c > 0$. Слично, можемо претпоставити $b > 0$.
Сада посматрајмо израз $a^2 + b^2 + c^2 = (a + c - b)(a + c + b)$. Ако је ово прост број, онда мањи фактор тог броја $a + c - b$ мора бити једнак 1.
Kako je $a \neq c$, мора важити $a+c > 2\sqrt{ac}$ па $a+c-b > 2b-b = b \geq 1$ што је контрадикција са претпоставком $a + c - b = 1$.
Дакле, $a^2 + b^2 + c^2$ не може бити прост број.

□

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

190 ● ● ● ●

(2002 Математичка олимпијада у Румунији) Нека су p и q два различита проста броја. Доказати да постоје цијели бројеви a и b такви да аритметичка средина свих дјелиоца броја $n = p^a q^b$ је такође цијели број.

Доказ. Сума свих дјелиоца броја n је дата формулом

$$(1 + p + p^2 + \ldots + p^a)(1 + q + q^2 + \ldots + q^b)$$

што се може лако видјети када се ослободимо заграда.
Број n има укупно $(a+1)(b+1)$ позитивних дјелиоца па слиједи да је аритметичка средина свих дјелиоца броја n

$$M = \frac{(1 + p + p^2 + \ldots + p^a)(1 + q + q^2 + \ldots + q^b)}{(a+1)(b+1)}$$

Ако су и p и q непарни бројеви, можемо узети да је $a = p$ и $b = q$ па се види да је M цијели број.
Ако је $p = 2$ и q непаран, узмимо $b = q$ и посматрајмо $a+1 = (1+q+q^2+\ldots+q^{q-1})$. Онда, $M = 1 + 2 + 2^2 + \ldots + 2^a$ је цијели број.
За p непарно и $q = 2$ узмимо $a = p$ и $b = p + p^2 + \ldots + p^{p-1}$, па слиједи да је M цијели број. □

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

191

Одредити све природне бројеве n и просте бројеве p такве да је $5p+1=n^2$.

Доказ. Траже се парови облика (n,p) такви да је

$$5p+1=n^2 \iff p=\frac{(n-1)(n+1)}{5}.$$

За $n=1$ и $n=2$ та једначина није задовољена јер добијамо да је $p=0$ односно $p=\frac{3}{5}$, па није задовољен услов да је p прост број .

Посматрајмо сада случај $n \geq 3$. Нагласимо да је $n-1 \neq 1$ и $n+1 \neq 1$. Пошто је p прост број онда је $\frac{(n-1)(n+1)}{5}$ такође прост . Тачно један од фактора $n-1$ и $n+1$ је дјељив са 5 , и тај фактор мора бити једнак 5 , у супртоном би онда при дјељењу са 5 дао неки природан број који кад се помножи оним другим фактором који је различит од 1 даје резултат који није прост .

Имамо 2 случаја

(I) Случај $n-1=5$

$$\implies n=6 \implies p=\frac{(n-1)(n+1)}{5} \implies p=7$$

(II) Случај $n+1=5$

$$\implies n=4 \implies p=\frac{(n-1)(n+1)}{5} \implies p=3$$

Пошто су 3 и 7 прости бројеви , парови $(6,7)$ и $(4,3)$ су рјешења задатка . ☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`https://dms.rs/wp-content/uploads/2017/03/TeorijeBrojeva_MarijaC.pdf`

192

За које природне бројеве n је број $3^{2n+1}-2^{2n+1}-6^n$ сложен?

Доказ. Дати израз можемо записати у облику

$$3\cdot(3^n)^2-2\cdot(2^n)^2-3^n\cdot 2^n.$$

Након смјене $x = 3^n$, $y = 2^n$, добијамо $3x^2 - 2y^2 - xy$, што се може раставити на следећи начин:

$$3x^2 - 2y^2 - xy = 3x^2 - 3xy + 2xy - 2y^2 = (x - y)(3x + 2y).$$

Уврштавајући вриједности за x, y имамо

$$3^{2n+1} - 2^{2n+1} - 6^n = (3^n - 2^n)(3^{n+1} + 2^{n+1}).$$

Како за $n \geq 2$ важи $3^n - 2^n > 1$, то је дати број сложен за све природне бројеве $n \neq 1$. За $n = 1$, он је једнак простом броју 13. Потпуно аналогним поступком, могуће је показати да је за $a \geq 2$ и $n \geq 2$ број $(a+1)^{2n+1} - a^{2n+1} - (a(a+1))^n$ сложен.

☐

(**Невена Гиговић 1/19 Ц**)

193

a) За природне бројеве a, b, c, d важи $a^2 + b^2 = c^2 + d^2$. Да ли је $a+b+c+d$ сложен број?
b) Одредити све просте бројеве p за које је и број $3^p + p^3$ прост.

Доказ. Решавамо на следећи начин:

a)

$$\begin{aligned}(a+b+c+d)^2 &= a^2 + b^2 + c^2 + d^2 + 2ab + 2ac + 2ad + 2bc + 2bd + 2cd \\ &= 2(a^2 + b^2 + ab + ac + ad + bc + bd + cd).\end{aligned}$$

Значи, $(a+b+c+d)^2$ је паран број, па је и $a+b+c+d$ паран, дакле сложен.

b) За $p = 2$ је и $3^2 + 2^3 = 17$ прост, а за друге просте бројеве p, који су уз то и непарни, збир $3^p + p^3$ је збир два непарна броја, па је он паран, а тиме и сложен. Дакле, број $3^p + p^3$ је прост једино за $p = 2$.

☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

194

Наћи све парове (a, b) природних бројева који задовољавају једначину $a^{b^2} = b^a$.

Доказ. Нека је (a, b) решење ове једначине. Примијетимо да је (1,1) једно решење, па посматрајмо $a, b > 1$.

Нека су $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n}$ и $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot \ldots \cdot p_n^{\beta_n}$ факторизације бројева a и b. Јасно је, због једначине коју задовољавају, α_i, $\beta_i > 0$ $\forall i = 1, \ldots, n$. (сваки фактор који учествује у факторизацији a мора се наћи и у факторизацији броја b). Када уврстимо у једначину:

$$p_1^{\alpha_1 b^2} \cdot p_2^{\alpha_2 b^2} \cdot \ldots \cdot p_n^{\alpha_n b^2} = p_1^{\beta_1 a} \cdot p_2^{\beta_2 a} \cdot \ldots \cdot p_n^{\beta_n a}$$

$\Rightarrow \alpha_i \cdot b^2 = \beta_i \cdot a, \forall i = 1, \ldots, n \Rightarrow \frac{\alpha_i}{\beta_i} = \frac{a}{b^2} = r$ за неки рационалан број r.

Одавде је $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_n^{\alpha_n} = p_1^{\beta_1 r} \cdot p_2^{\beta_2 r} \cdot \ldots \cdot p_n^{\beta_n r} = b^r$ тј. $a = b^r$.

па када опет уврстимо у једначину: $b^{rb^2} = b^{b^r} \Rightarrow r \cdot b^2 = b^r$ тј. $r = b^{r-2}$.

Како рационалан степен природног броја b може бити једнак рационалном броју r само ако је r природан број, то онда остаје да r мора бити природан број.

Индукцијом докажимо да за $r \geq 5$, $r < 2^{r-2} \leq b^{r-2}$.

За $r = 5 \Rightarrow 5 < 2^3 \leq b^3$, па како посматрамо $b > 1$, важи база индукције.

Претпоставимо да неједнакост важи за $r - 1$.

Покажимо да важи за r.

Како је $r - 1 < 2^{r-3} \Rightarrow r < 2^{r-3} + 1 < 2 \cdot 2^{r-3} = 2^{r-2}$. Овај дио неједнакости важи. Остаје још да видимо да је $2^{r-2} \leq b^{r-2}$, а ово је јасно јер $b > 1$.

Дакле, остају нам случајеви $r \in (1, 2, 3, 4)$. Уврштавањем у $r = b^{r-2}$ и $a = b^r$ добијамо да су решења дате једначине (1,1), (27,3) и (16, 2).

☐

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

195

Природан број n има два проста дјелиоца, а број n^2 укупно 15 позитивних дјелилаца. Колико позитивних дјелилаца има број n^3?

Доказ. Како природан број n има два проста дјелиоца, то је $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, а како n^2 има 15 позитивних дјелиоца, то је $\tau(n^2) = 15$.

Ако знамо да је $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2}$, онда је $n^2 = (p_1^{\alpha_1} \cdot p_2^{\alpha_2})^2 = p_1^{2\alpha_1} \cdot p_2^{2\alpha_2}$, takoђе $n^3 = (p_1^{\alpha_1} \cdot p_2^{\alpha_2})^3 = p_1^{3\alpha_1} \cdot p_2^{3\alpha_2}$.

Одакле важи да је $\tau(n^2) = (2\alpha_1 + 1)(2\alpha_2 + 1) = 15 = 3 \cdot 5$, односно, $2\alpha_1 + 1 = 5$ и $2\alpha_2 + 1 = 3$ (изједначавамо на овај начин јер нам је циљ да добијемо најмањи природан број који задовољава услове задатка) тј. $\alpha_1 = 2$ и $\alpha_2 = 1$.

Како се у задатку тражи $\tau(n^3)$ то је

$$\tau(n^3) = (3\alpha_1 + 1)(3\alpha_2 + 1) = (3 \cdot 2 + 1)(3 \cdot 1 + 1) = 28.$$

☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/13890/mod_resource/content/1/Prosti%20brojevi%20%28%C4%8Detvrti%20termin%29%2021.3.2020..pdf`

196

●●●●

Наћи све природне бројеве n за које су сви бројеви који имају у декадном $n-1$ запису цифру 1 и једну цифру 7 прости.

Доказ. Број N који се састоји од $n-1$ цифара 1 и једне цифре 7 може се записати у облику

$$N = A_n + 6 \cdot 10^k,$$

гдје је A_n број који је написан са n јединица, а $0 \leq k < n$.

Ако $3 \mid n$ тада је збир цифара броја N дјељив са 3, па стога $3 \mid n$, због чега N није прост.

Сада посматрајмо случај $n \geq 6$. Како бројеви A_s редом за $s = 1, 2, 3, 4, 5, 6$ дају остатке 1, 4, 6, 5, 2, 0 при дијељењу са 7, и како је:

$$A_{m+6} = A_m 10^6 + A_6 \equiv A_m + A_6 \equiv A_m \pmod 7,$$

слиједи да $7 \mid A_l$ акко $6 \mid l$. Дакле, за $k = 0, 1, 2, 3, 4, 5$ број 10^k даје редом остатке 1, 3, 2, 6, 4, 5, па $6 \cdot 10^k$ за исте вриједности k редом даје остатке 6, 4, 5, 1, 3, 2. Одавде слиједи закључак: ако за неко $n \geq 6$ важи $A_n \equiv r \pmod 7$ и $3 \nmid n$, тада можемо наћи такво $k \leq 5$ да је $6 \cdot 10^k \equiv -r \pmod 7$, па онда

$$7 \mid \underbrace{(A_n + 6 \cdot 10^k)}_{N},$$

тј. N није прост.

Значи довољно је да провјеримо вриједности $n = 2, 4, 5$. За $n = 5$ имамо $11711 = 7 \cdot 1673$, а за $n = 4$ је $1711 = 29 \cdot 59$. С друге стране, за $n = 2$, бројеви 17 и 71 су прости. Према томе, решење задатка је $n \in \{1, 2\}$.

□

(**Невена Гиговић 1/19 Ц**) задатак преузет из
Елементарна теорија бројева Игор Долинка

197

●●●●

Наћи све тројке (p, q, r) простих бројева за које важи $p^2 - q \cdot r = 2500$.

Доказ. Како је p прост број онда је $p \equiv 1 \pmod 3$ или $p \equiv -1 \pmod 3$, односно $p^2 \equiv 1 \pmod 3$. Такође је и $2500 \equiv 1 \pmod 3$ па ако почетну једначину трансформишемо у облику:

$$p^2 - 2500 = q \cdot r \Leftrightarrow (p-50)(p+50) = q \cdot r$$

закључујемо да је лијева страна дјељива са 3, па мора бити и десна. Како су q и r прости један од њих мора бити 3. Без смањења општости нека је то q. Тада је:

$$(p-50)(p+50) = 3 \cdot r$$

Како је r прост број, могући су следећи случајеви:

(1) $p-50=3 \wedge p+50=r \Rightarrow p=53 \wedge r=103$

(2) $p-50=1 \wedge p+50=3\cdot r \Rightarrow p=51$, а то није прост број па овај случај није могућ.

Како q и r могу замијенити улоге, (53, 3, 103) и (53, 103,3) су двије тројке које задовољавају дату једначину.

$\square$

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb`

198

Одредити све просте бројеве p и q за које важи $p \mid 30q-1$ и $q \mid 30p-1$.

Доказ. Примијетимо да је нзд$(pq, 30) = 1$, односно $p, q \neq 2, 3, 5$. Из услова $p \mid 30q-1$ и $q \mid 30p-1$ добијамо да $pq \mid (30q-1)(30p-1) = 900pq-30p-30q+1$ па

$$pq \mid 30(p+q)-1.$$

Одавде закључујемо да постоји природан број n такав да нзд$(n, 30) = 1$ (јер нзд$(pq, 30) = 1$) за који важи:

$$pqn = 30(p+q)-1$$

Посматрајмо следеће случајеве:
1) $n=1$
Једначина постаје $pq = 30(p+q)-1$ која је еквивалентна са $(p-30)(q-30) = 899 = 29\cdot 31$.
Одавде добијамо решења $(p, q) \in \{(59, 61), (61, 59), (31, 929), (929, 31)\}$
2) $n>1$
Одавде слиједи $n \geq 7$ (јер је (нзд$(n, 30) = 1$ тј. $n \neq 2, 3, 5$).
Сада имамо

$$7pq \leq pqn = 30(p+q)-1 < 30(p+q).$$

Због симетрије можемо узети да је $p \leq q$. Дијељењем последње неједнакости са $30pq$ добијамо

$$\frac{7}{30} < \frac{1}{p} + \frac{1}{q} \leq \frac{2}{p}$$

Одавде је $p \leq \frac{60}{7} < 9$, а како је $p \geq 7$, то мора бити $p = 7$. Сада

$$7 \mid 30q-1 \text{ и } q \mid 30\cdot 7-1 = 209 = 11\cdot 19$$

Одавде је $q = 11$ или $q = 19$. Други случај отпада јер број $30\cdot 19-1 = 569$ није дјељив са 7. Дакле, у овом случају једина решења су $(p, q) \in \{(7, 11), (11, 7)\}$.

Коначно, сва решења дата су са $(p, q) \in \{(7, 11), (11, 7), (59, 61), (61, 59), (31, 929), (929, 31)\}$.

$\square$

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb`

199 ●●●●

Да ли постоји природан број n за који важи $361 \mid n^2 + 4n - 15$?

Доказ. Важи да је $n^2 + 4n - 15 = (n+2)^2 - 19$. Претпоставимо да постоји n тако да:

$$361 \mid (n+2)^2 - 19$$

Како је $361 = 19 \cdot 19$ онда:

$$19 \mid (n+2)^2 - 19 \Rightarrow 19 \mid (n+2)^2$$

па како је 19 прост број:

$$19^2 \mid (n+2)^2 \Leftrightarrow 361 \mid (n+2)^2 \Rightarrow 361 \mid 19$$

Контрадикција. Дакле, не постоји такав број.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb`

200 ●●●●

Показати да постоји бесконачно много простих бројева.

Доказ. Претпоставимо да постоји коначно много простих бројева и поређајмо их у низ:

$$p_1, p_2, p_3, ..., p_n$$

На основу овога знамо да су остали бројеви сложени, па је и број

$$p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$$

сложен број. Али како је дати број сложен он мора бити дјељив са барем једним простим бројем. Како су претходно сви сложени бројеви поређани у низ, уочавамо да ће наш број, подијељен са било којим бројем из низа простих бројева дати остатак 1. Конструисали смо још један прост број и дати поступак можемо понављати до бесконачности. Закључујемо да је скуп простих бројева бесконачан.

□

(**Андрија Бошковић 14/19 Б**)
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

201 ●●●●

Ако су p и $7p-1$ прости бројеви онда је $7p+1$ сложен.

Доказ. Нека је $p=2$, тада је $7p-1=7\cdot 2-1=13$, што је прост број. А број $7p+1=7\cdot 2+1=15$, је сложен, што смо хтјели показати.

Нека је сада p прост број већи од 2. Сви прости бројеви већи од 2 су непарни. Како је $7p$ непаран у том случају, онда имамо и да је број $7p+1$ паран. Овим смо покрили све могуће случајеве.

□

(**Андрија Бошковић 14/19 Б**)
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

202 ●●●●

Ако су бројеви p и $2p^2+1$ прости, доказати да је и број $3p^2+2$ такође прост.

Доказ. Ако је p прост број већи од 3, тада је p облика $6k+1$ или $6k+5$ за неко k.

Нека је $p=6k+1$, онда имамо:
$2p^2+1=2(6k+1)^2+1=2(36k^2+12k+1)+1=3(24k^2+8k+1)$
Закључујемо да је дати број сложен.
Такође за $p=6k+5$ имамо:
$2p^2+1=2(6k+5)^2+1=2(36k^2+60k+25)+1=3(24k^2+40k+17)$
И овај број је сложен.
Закључујемо да не можемо пронаћи прост број p већи од 3 такав да је $2p^2+1$ прост.
Позабавимо се сада простим бројевима 2 и 3.
За $p=2$ имамо да је број $2p^2+1=9$ такође сложен, па и њега искључујемо.
За $p=3$ имамо да је број $2p^2+1=19$ прост. Ово нам омогућава даљу провјеру.

$$3p^2+2=29$$

Заиста, за све бројеве за које важи да су p и $2p^2+1$ прости имамо да је и број $3p^2+2$ такође прост.

□

(**Андрија Бошковић 14/19 Б**)
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

203 ●●●●

Одредити најмањи природан број чија је половина потпун квадрат, трећина потпун куб, а петина потпун пети степен.

Доказ. Тражени број n мора бити дјељив са 2, 3 и 5. Због минималности, нема других простих фактора.

Нека је $n = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma}$.

Из услова задатка имамо:

$$\frac{n}{2} = 2^{\alpha-1} \cdot 3^{\beta} \cdot 5^{\gamma} = a^2$$

$$\frac{n}{3} = 2^{\alpha} \cdot 3^{\beta-1} \cdot 5^{\gamma} = b^3$$

$$\frac{n}{5} = 2^{\alpha} \cdot 3^{\beta} \cdot 5^{\gamma-1} = c^5$$

при чему су ,b и c природни бројеви.

Тада је α најмањи непаран природан број дјељив са 3 и 5, β најмањи природан број дјељив са 2 и 5 који при дијељењу са 3 даје остатак 1 и γ најмањи природан број дјељив са 2 и 3 који при дијељењу са 5 даје остатак 1.

Према томе закључујемо да:

$$\alpha = 15$$

$$\beta = 10$$

$$\gamma = 6$$

Тада је:

$$n = 2^{15} \cdot 3^{10} \cdot 5^{6} = 30233088000000$$

□

(**Андрија Бошковић 14/19 Б**)
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

204

Нека су $p_1, p_2, p_3, ..., p_n$ различити прости бројеви, доказати да $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + ... + \frac{1}{p_n}$ није реалан број.

Доказ. Број

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + ... + \frac{1}{p_n} = \frac{p_2 \cdot p_3 \cdots p_n + ... + p_1 \cdot p_2 \cdots p_{n-1}}{p_1 \cdot p_2 \cdots p_n}$$

није цио број јер бројилац датог разломка није дјељив са p_1 (због тога што фигуришу искључиво прости бројеви имамо да први сабирак бројиоца није дјељив са p_1 док остали јесу), именилац је истовремено дјељив са p_1 што указује да $\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + ... + \frac{1}{p_n}$ није цио број.

□

(**Андрија Бошковић 14/19 Б**)
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

205

Постоји ли прост број p тако да и бројеви $3p+1$ и $5p+1$ буду прости?

Доказ. Постоји. То је број $p=2$,јер су тада $3\cdot 2+1=7$ и $5\cdot 2+1=11$ прости. Више од овог не би било могуће јер би за било који други прост број $p \geq 3$,због његове непарности,бројеви $3p+1$ и $5p+1$ били парни па тиме и сложени. □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`https://zadaci.files.wordpress.com/2012/11/prostibrojevi1.pdf`

206

Наћи све природне бројеве $n<1979$ који задовољавају следећи услов: ако је m природан број,$1<m<n$, $(m,n)=1$, онда је m прост број.

Доказ. Нека је S скуп свих природних бројева за које ва‘е наведени услови.Ако је $n \in S$ и $p^2<n$,гдје је p прост број онда n и p^2 нису узајамно прости бројеви јер p^2 није прост број. Према томе $p \mid n$.Ако је $n>49$ и $n \in S$ онда је сваки од бројева 2,3,5,7 делилац броја n.Зато је $n \geq 2\cdot 3\cdot 5\cdot 7=210>11^2, pai11 \mid n$.
Даље слиједи $n \geq 210\cdot 11=2310>1979$,што је контрадикција. Зато је $S \subset \{1,2,\ldots,49\}$.
(а) Нека је $n>25$. Тада $n \in S$ ако и само ако је број n дјељив са $2\cdot 3\cdot 5=30$.
Такав број је само 30.
(б) Нека је $9<n\leq 25$. Тада $n \in S$ ако и само ако је n дјељиво са $2\cdot 3=6$.То важи за бројеве 12,18,24.
(в) Нека је $4<n\leq 9$. Тада $n\in S$ ако и само ако је n паран број.Дакле $6\in S$,$8\in S$.
(г) Лако се провјерава да сваки од бројева 2,3,4 припада скупу S.
Према томе $S=\{2,3,4,6,8,12,18,24,30\}$. □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

207

Одредити све просте бројеве p,q,r,s такве да је:

$$p\cdot q\cdot(r+s)=2013$$

Доказ. Како се тражи да број 2013 запишемо као производ нека три броја, то уствари значи да га морамо раставити на чиниоце да бисмо видјели који све бројеви долазе у обзир за избор ова три броја.Растављањем броја 2013 на просте чиниоце добијамо да је $2013=3\cdot 11\cdot 61$. Сва три броја су проста, па сада разматрамо који од њих могу бити p и q,а који може бити збир простих бројева $(r+s)$. Најбитније је прво размотрити $(r+s)$ јер видимо да збир два проста броја никако не може бити ни 3 ни 11, дакле преостаје нам само да $r+s=61$. Значи да ће p и q бити из скупа $\{3,11\}$.Сада још треба одредити тачне вриједности за r и s. Како

је 61 непаран број добијамо га као збир једног парног и једног непарног броја(када би и r и s били оба непарни,њихов збир би био паран, што нам у овом случају не одговара).Дакле како је једини прост паран број 2 закључујемо да један од бројева r и s мора бити 2,а за други онда преостаје да буде 59, да би у збиру дали 61.
Дакле за $(p, q, r, s) = \{3, 11, 2, 59\}$

$$p \cdot q \cdot (r + s) = 3 \cdot 11 \cdot (2 + 59) = 3 \cdot 11 \cdot 61 = 2013$$

За $(p, q, r, s) = \{3, 11, 59, 2\}$

$$p \cdot q \cdot (r + s) = 3 \cdot 11 \cdot (59 + 2) = 3 \cdot 11 \cdot 61 = 2013$$

За $(p, q, r, s) = \{11, 3, 2, 59\}$

$$p \cdot q \cdot (r + s) = 11 \cdot 3 \cdot (2 + 59) = 3 \cdot 11 \cdot 61 = 2013$$

За $(p, q, r, s) = \{11, 3, 59, 2\}$

$$p \cdot q \cdot (r + s) = 11 \cdot 3 \cdot (59 + 2) = 3 \cdot 11 \cdot 61 = 2013$$

Скуп рјешења је, дакле:

$S(p, q, r, s) = \{(3, 11, 2, 59), (3, 11, 59, 2), (11, 3, 2, 59), (11, 3, 59, 2)\}$

□

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

208

Природан број n је **савршен број** ако је једнак збиру свих својих позитивних дјелилаца (искључујући сам број n), тј. ако је $\sigma(n) = 2n$.
Ако је $2^p - 1$ прост број онда је $2^{p-1}(2^p - 1)$ савршен број и сваки паран савршен број је тог облика.

Доказ. Нека је $k = 2^p - 1$ прост број и $n = 2^{p-1}(2^p - 1)$. Да бисмо показали да је број n савршен треба показати да је $\sigma(n) = 2n$. Пошто је функција σ мултипликативна и $\sigma(k) = k + 1 = 2^p$, то је

$$\sigma(n) = \sigma(2^{p-1}) \cdot \sigma(k)$$

$$= (1 + 2 + 2^2 + \cdots + 2^{p-1}) \cdot 2^p$$

$$= (2^p - 1) \cdot 2 \cdot 2^{p-1} = 2n,$$

одакле слиједи да је број n савршен.
Обрнуто, нека је n произвољан паран савршен број. Запишимо га у облику $n = 2^{p-1}m$, гдје је m непаран број и $p \geq 2$. Из мултипликативности функције σ слиједи:

$$\sigma(2^{p-1}m) = \sigma(2^{p-1})\sigma(m) = (2^p - 1)\sigma(m).$$

Пошто је n савршен број то је

$$\sigma(n) = 2n = 2^p m.$$

Из претходне двије једнакости слиједи

$$2^p m = (2^p - 1) \cdot \sigma(m),$$

па закључујемо да $2^p - 1 \mid 2^p m$, тј. да $2^p - 1 \mid m$. Према томе, $m = (2^p - 1)M$. Замјењујући то у претходну једнакост добијамо

$$2^p(2^p - 1)M = (2^p - 1) \cdot \sigma(m),$$

тј. $2^p M = \sigma(m)$. Како су m и M дјелиоци од m то је

$$2^p M = \sigma(m) \geq m + M = 2^p M,$$

па је $\sigma(m) = m + M$. То значи да је број m прост и једина његова два дјелиоца су m и $1 = M$. Према томе, $m = 2^p - 1$ је прост број, што је и требало доказати. ☐

(**Лазар Шћекић 6/19 Б**) задатак из збирке задатака
"Теорија бројева-Марија Станић, Небојша Икодиновић

209

Одредити све просте бројеве p, q који задовољавају једначину $p^q + q^p = r, r \in R$. (r-прост)

Доказ. Уочимо да, ако нађемо рјешење (p, q), тада ће важити симетричност, па ће и (q, p) такође представљати рјешење.
Пошто су p и q прости бројеви, мора важити $p \geq 2$ и $q \geq 2$, па зато $p^q + q^p$, односно r не може бити једнако 2. Како је 2 једини паран прост број, а r је прост који није 2, слиједи да r мора бити непаран.
Било који непаран број дигнут на било који степен као резултат даје опет непаран број. Такође, било који паран број дигнут на било који степен као резултат даје паран број. Одавде слиједи да p и q не могу истовремено да буду парни или истовремено непарни, јер би тада и p^q и q^p били истовремено парни, односно истовремено непарни, па би њихов збир био паран број, што нас доводи до контрадикције, јер смо већ констатовали да је r непаран.
Закључујемо, један од бројева p и q мора бити непаран, а други паран. Оба броја су проста, па је јасно да онај паран мора да буде 2. Важи симетричност, па ћемо узети да је $p = 2$:

$$2^q + q^2 = r$$

Пошто је q непаран прост број, а најмањи непаран прост број је 3, закључујемо да је $q \geq 3$. Разматраћемо случајеве:

I случај ($q = 3$):

$$2^3 + 3^2 = r$$

$$8 + 9 = 17 = r$$

Број 17 јесте прост, па су рјешења за овај случај (2,3) и (3,2).

II случај (q>3):

Пошто је q прост број и већи је од 3, он не може бити дјељив са 3, тј. не може бити облика $q = 3k$, већ само може бити облика $q = 3k + 1$ или $q = 3k + 2, k \in N$.Због тога имамо два подслучаја:

IIа: $(q = 3k + 1) \implies$ пошто је q непарно, онда k мора бити парно.

IIб: $(q = 3k + 2) \implies$ пошто је q непарно, онда k мора бити непарно.

Рјешаваћемо случајеве редом:

IIа: ($q = 3k + 1$), k парно:

$$2^{3k+1} + (3k + 1)^2 = r$$

$$8^k \cdot 2 + 9k^2 + 6k + 1 = r$$

$$(9 - 1)^k \cdot (3 - 1) + 9k^2 + 6k + 1 = r$$

$$3(9 - 1)k - (9 - 1)^k + 9k^2 + 6k + 1 = r$$

$$3[(9 - 1)^k + 3k^2 + 2k] - (9 - 1)^k + 1 = r$$

$$3[(9-1)^k+3k^2+2k]-[\binom{k}{0}9^k(-1)^0+\binom{k}{1}9^{k-1}(-1)^1+...+\binom{k}{k-1}9(-1)^{k-1}+\binom{k}{k}(-1)^k]+1 = r$$

$$3[(9-1)^k+3k^2+2k]-9[\binom{k}{0}9^{k-1}(-1)^0+\binom{k}{1}9^{k-2}(-1)^1+...+\binom{k}{k-1}(-1)^{k-1}]-\binom{k}{k}(-1)^k+1 = r$$

Пошто је у овом случају k парно, то је $(-1)^k = 1$:

$$3[(9 - 1)^k + 3k^2 + 2k] - 9[\binom{k}{0}9^{k-1}(-1)^0 + \binom{k}{1}9^{k-2}(-1)^1 + ... + \binom{k}{k-1}(-1)^{k-1}] - 1 + 1 = r$$

$$3[(9 - 1)^k + 3k^2 + 2k] - 9[\binom{k}{0}9^{k-1}(-1)^0 + \binom{k}{1}9^{k-2}(-1)^1 + ... + \binom{k}{k-1}(-1)^{k-1}] = r$$

Из посљедње једнакости се види да је r дјељиво са 3. Како је $r > 3$ (јер $p = 2, q > 3$), то значи да r није прост број, па овај случај отпада.

IIб: ($q = 3k + 2$), k непарно:

$$2^{3k+2} + (3k + 2)^2 = r$$

$$8^k \cdot 2^2 + 9k^2 + 12k + 4 = r$$

$$(9 - 1)^k \cdot (3 + 1) + 9k^2 + 12k + 3 + 1 = r$$

$$3(9 - 1)^k + (9 - 1)^k + 9k^2 + 12k + 3 + 1 = r$$

$$3[(9 - 1)^k + 3k^2 + 4k + 1] + (9 - 1)^k + 1 = r$$

$$3[(9-1)^k+3k^2+4k+1]+[\binom{k}{0}9^k(-1)^0+\binom{k}{1}9^{k-1}(-1)^1+...+\binom{k}{k-1}9(-1)^{k-1}+\binom{k}{k}(-1)^k]+1 = r$$

$$3[(9-1)^k+3k^2+4k+1]+9[\binom{k}{0}9^{k-1}(-1)^0+\binom{k}{1}9^{k-2}(-1)^1+...+\binom{k}{k-1}(-1)^{k-1}]+\binom{k}{k}(-1)^k+1=r$$

Пошто је у овом случају k непарно, тада је $(-1)^k$=-1:

$$3[(9-1)^k+3k^2+4k+1]+9[\binom{k}{0}9^{k-1}(-1)^0+\binom{k}{1}9^{k-2}(-1)^1+...+\binom{k}{k-1}(-1)^{k-1}]-1+1=r$$

$$3[(9-1)^k+3k^2+4k+1]+9[\binom{k}{0}9^{k-1}(-1)^0+\binom{k}{1}9^{k-2}(-1)^1+...+\binom{k}{k-1}(-1)^{k-1}]=r$$

Одавде се види да је r дјељиво са 3. Како је $r > 3$ $(p = 2, q > 3)$, то значи да r није прост број, тако да и овај случај отпада.
Дакле, једина два пара рјешења су:

$$(p, q) = (2, 3)$$

и

$$(q, p) = (2, 3).$$

□

(**Лазар Шћекић 6/19 Б**) задатак са интернета
Такмичење из математике, Србија 1991

210
●●●●

Ако је $x^2 + 2y^2$ прост непаран број, онда је он облика $8n + 1$ или $8n + 3$. Доказати.

Доказ. Како је x^2+2y^2 непаран, онда x мора бити непаран па је $x^2 \equiv 1 \pmod 8$. Доказаћемо то:
x је непаран, па се може записати у облику $x = 2q + 1$. Даље је

$$x^2 = 4q^2 + 4q + 1 = 4q(q + 1) + 1$$

Пошто је тачно један од бројева q и $q + 1$ дјељив са 2, то значи да је

$$x^2 = 8r + 1.$$

Одатле је квадрат било ког непарног броја конгруентан са 1 по модулу 8.
Уколико је y паран, слиједи да је $y = 2q$, па је $2(2q)^2 = 8q^2$, тј. $2y^2 \equiv 0 \pmod 8$. Дакле, $x^2 + 2y^2 \equiv 1 \pmod 8$. Слично, ако је y непаран, $2y^2 \equiv 2 \pmod 8$, па је онда $x^2 + 2y^2 \equiv 3 \pmod 8$.

□

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://forum.matemanija.com/`

211

Ако су $2n+1$ и $3n+1$ потпуни квадрати, $n \in N$, онда $5n+3$ није прост број. Доказати.

Доказ. Нека је $2n+1 = a^2$, $3n+1 = b^2$, за неке $a, b \in N$. Тада $5n+3 = 4(2n+1)-(3n+1) = 4a^2 - b^2 = (2a-b)(2a+b)$. Претпоставимо да је $2a - b = 1$. Тада се претходна једнакост своди на $5n+3 = 2a+b$. Затим, $2b = 2a+b-(2a-b) = 5n+3-1 = 5n+2$. И коначно, $(b-1)^2 = b^2 - 2b + 1 = (3n+1) - (5n+2) + 1 = -2n$. Добија се $(b-1)^2 = -2n < 0$, што је контрадикција, па мора бити $2a - b \neq 1$. Из једнакости $5n+3 = (2a+b)(2a-b)$ видимо да је $2a - b$ природан број већи од 1, зато што су $5n+3$, $2a+b \in N$. Према томе, $5n+3$ није прост јер је дјељив са $2a-b$. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://forum.matemanija.com/`

212

Два играча играју следећу игру: први играч записује једну цифру; затим други играч дописује са лијеве или десне стране неку цифру; затим први дописује са лијеве или десне стране неку цифру; затим други поново дописује са лијеве или десне стране неку цифру итд. Показати да први играч може играти тако да после сваког потеза другог играча записани број није потпуни квадрат.

Доказ. Прва цифра коју први играч треба да запише мора бити 7 јер је то једина цифра таква да не постоји двоцифрен квадрат који почиње или завршава се са 7. Затим претпоставимо да је у неком тренутку, након потеза другог играча, записан број $c_1c_2c_3\ldots c_{2k-1}c_{2k}$. Први играч сада треба да допише 7 или 8 са десне стране. У том случају, уколико други играч допише било коју цифру са лијеве стране,добијени број неће бити потпун квадрат јер се ниједан потпун квадрат не завршава цифрама 7 или 8.Уколико други играч допише било коју цифру са десне стране, добиће се један од следећих бројева:
$c_1c_2c_3\ldots c_{2k-1}c_{2k}70, c_1c_2c_3\ldots c_{2k-1}c_{2k}71, \ldots, c_1c_2c_3\ldots c_{2k-1}c_{2k}89$.
Ради се о 20 узастопних бројева већих од 1000 па међу њима не могу бити два која су потпуни квадрати. У случају да међу њима нема ниједан потпун квадрат, први играч може да допише било коју од цифара 7 или 8.Ако је један од уочених бројева потпун квадрат и ако је његова претпоследња цифра 7,први играч треба да допише 8 а у супротном случају цифру 7. У било ком од претпостављених случајева други играч не може формирати потпун квадрат дописивањем било које од цифара. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

213

Доказати да је број $512^3 + 675^3 + 720^3$ сложен.

Доказ. Директно израчунавање вриједности датог израза свакако не обећава много:

$512^3 = 134217728$, $675^3 = 307546875$, $720^3 = 373248000$,

$512^3 + 675^3 + 720^3 = 815012603$. Да ли је број 815012603 сложен? Покушаћемо да откријемо неке правилности које ће нас довести до одговора.

Сама поставка задатка указује на идентитет

$$x^3 + y^3 + z^3 - 3xyz = (x + y + z)(x^2 + y^2 + z^2 - xy - yz - zx).$$

Овај идентитет не раставља збир кубова на чиниоце, па се не може директно употријебити. Покушаћемо да откријемо неку везу између бројева 512, 675 и 729 која би могла бити од користи. Растављањем датих бројева на чиниоце имамо:

$$512 = 2^9,\ 675 = 3^3 \cdot 5^2,\ 720 = 2^4 \cdot 3^2 \cdot 5$$

Уочимо да је $2 \cdot 720^2 = 3 \cdot 512 \cdot 675$.

Дакле, за $x = 512$, $y = 675$, $z = 720$ имамо да је $2z^2 = 3xy$, одакле слиједи да је $2z^3 = 3xyz$, па је

$$x^3 + y^3 + z^3 = x^3 + y^3 - z^3 + 2z^3 = x^3 + y^3 + (-z)^3 - 3xy(-z).$$

Користећи везу између бројева x, y, z, уколико добијени израз разложимо на чиниоце строго веће од 1 закључујемо да је $x^3 + y^3 + z^3$ сложен број. Овај резон важи и за ма које друге бројеве за које поменута веза важи.
Раставићемо израз са десне стране једнакости на следећи начин:

$$\begin{aligned} &x^3 + y^3 + (-z)^3 - 3xy(-z) = x^3 + y^3 - z^3 + 3xyz = \\ &= x^2(x + y - z) - xy(x + y - z) + y^2(x + y - z) + xz(x + y - z) + yz(x + y - z) + z^2(x + y - z) = \\ &= (x + y - z)(x^2 - xy + y^2 + xz + yz + z^2) \end{aligned}$$

Из добијеног идентитета, везе коју смо користили у његовом добијању и која за поменуте бројеве важи, као и чињенице да су $x + y - z > 1$ и $x^2 - xy + y^2 + xz + yz + z^2 > 1$ за дате бројеве, слиједи да је број сложен. □

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
мастер рад под називом "ЧЕТИРИ ЕТАПЕ РЕШАВАЊА ЗАДАТАКА ИЗ ЕЛЕМЕНТАРНЕ ТЕОРИЈЕ БРОЈЕВА", Тијана Спасић, Београд, 2017. година

214

За природне бројеве a, b, c, d важи $a^2+b^2 = c^2+d^2$. Да ли је број $a+b+c+d$ сложен?

Доказ.

$$(a+b+c+d)^2 = a^2+b^2+c^2+d^2+2ab+2ac+2ad+2bc+2bd+2cd$$
$$= 2(a^2+b^2+ab+ac+ad+bc+bd+cd).$$

Значи, $(a+b+c+d)^2$ је паран број, па је $a+b+c+d$ и паран, односно сложен.

$\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

215

●●●●

Наћи све просте бројеве p такви да су и бројеви $8p^2+1$ прости.

Доказ. Ако је $p=2$, тада $8p^2+1=33$ није прост број.
Ако је $p=3$, тада $8p^2+1=73$ јесте прост број.
За $p=5$ број $8p^2+1=201$ није прост.

Нека је сада p прост број већи од 5. Тада је p облика $6k+1$ или $6k+5$ $(k\in\mathbb{N})$.

Ако је $p=6k+1$, тада је
$8(6k+1)^2+1=8(36k^2+12k+1)+1=3(96k^2+32k+3)$ сложен број.

Ако је $p=6k+5$, тада је
$8(6k+5)^2+1=8(36k^2+60k+25)+1=3(96k^2+160k+67)$ сложен број.

Дакле, једино рјешење је $p=3$. $\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

216

●●●●

Наћи све просте бројеве p такви да су и бројеви $p+10$ и $p+14$ прости.

Доказ. Ако је $p=2$, тада $p+10=12$ није прост број.
Ако је $p=3$, тада $p+10=13$ и $p+14=17$ јесу прости бројеви.
За $p=5$ број $p+10=15$ није прост.

Значи, сваки природан број је облика $3k$, $3k+1$, $3k+2$. Међу бројевима облика $3k$ једино је $p=3$ прост број. У том случају су и бројеви $p+10=13$ и $p+14=17$ такође прости, па $p=3$ јесте рјешење.

За $p=3k+1$ број $p+14=3(k+5)$ је сложен, а за $p=3k+2$ број $p+10=3(k+4)$ је сложен.
Дакле, једини прост број са траженом особином је број 3. $\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

217

Наћи све просте бројеве p такви да су и бројеви $p^2 + 4$ и $p^2 + 6$ прости.

Доказ. Ако је $p = 2$, тада је $p^2 + 4 = 8$ сложен број.
Ако је $p = 3$, тада је $p^2 + 6 = 15$ сложен број.
За $p = 5$ бројеви $p^2 + 4 = 29$ и $p^2 + 6 = 31$ су прости.

Ако је p прост број већи од 5, тада разликујемо следеће случајеве:

1. $p = 5k + 1$ за неко $k : p^2 + 4 = (5k + 1)^2 + 4 = 5(5k^2 + 2k + 1)$ је сложен број;

2. $p = 5k + 2$ за неко $k : p^2 + 6 = (5k + 2)^2 + 6 = 5(5k^2 + 4k + 2)$ је сложен број;

3. $p = 5k + 3$ за неко $k : p^2 + 6 = (5k + 3)^2 + 6 = 5(5k^2 + 6k + 3)$ је сложен број;

4. $p = 5k + 4$ за неко $k : p^2 + 4 = (5k + 4)^2 + 4 = 5(5k^2 + 8k + 4)$ је сложен број.

Дакле, једино рјешење је $p = 5$. □

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

218

Наћи све природне бројеве n за које је израз $n^4 + 4^n$ прост број.

Доказ. Нека је $n = 1$.

$$n^4 + 4^n = 5$$

Дати број је прост.

Јасно је да избором парног броја n као рјешење нашег израза добијамо паран број, што искључује парне бројеве као могућа рјешења.

Сада претпоставимо да је $n > 1$ непаран.

$$n^4+4^n = n^4+2n^2 2^n+4^n-2n^2 2^n = (n^2+2^n)^2-(n\cdot 2^{\frac{n+1}{2}})^2 = (n^2+2^n+n\cdot 2^{\frac{n+1}{2}})(n^2+2^n-n\cdot 2^{\frac{n+1}{2}})$$

Избором било којег $n > 1$ јасно је да дати израз за оба чиниоца има бројеве веће од 1. Ово указује да је дати израз прост искључиво за $n = 1$.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

219

Показати да $f(n) = n^5 + n^4 + 1$ није прост, за n>1.

Доказ. Показаћемо да се полином $f(n)$ може представити као производ фактора нижег степена који такође имају цјелобројне коефицијенте. С обзиром на то да је слободан члан једнак 1, уколико би постојао линеаран фактор, он би морао бити облика $n+1$ или $n-1$. Стандардно провјеравамо да ли постоје линеарни фактори (рачунамо $f(1)$ и $f(-1)$).
$f(1) \neq 0$ и $f(-1) \neq 0$, одакле закључујемо да не постоји линеарни фактор.
Тражимо квадратне и кубне факторе. Постоје двије могућности:

$$n^5 + n^4 + 1 = (n^2 + an + 1)(n^3 + bn^2 + cn + 1)$$

и

$$n^5 + n^4 + 1 = (n^2 + an - 1)(n^3 + bn^2 + cn - 1).$$

Посматрајмо први случај. Када измножимо десну страну, добија се

$$n^5 + n^4 + 1 = n^5 + (a+b)n^4 + (ab + c + 1)n^3 + (ac + b + 1)n^2 + (a+c)n + 1$$

Упоређивањем коефицијената са лијеве и десне стране једнакости, добијамо систем:

$$a + b = 1$$

$$ab + c + 1 = 0$$

$$ac + b + 1 = 0$$

$$a + c = 0$$

Рјешење система је: $a = 1$, $b = 0$, $c = -1$. Добили смо факторизацију

$$n^5 + n^4 + 1 = (n^2 + n + 1)(n^3 - n + 1).$$

Полином се у првом случају може факторисати, па то значи да није прост. Пошто смо већ првим случајем показали да полином није прост, то други нема потребе ни да разматрамо. □

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://forum.matemanija.com/`

220

Нека су дати прости бројеви $p_1 < p_2 < \ldots < p_{31}$. Доказати да ако 30 дијели суму њихових четвртих степена, тада међу њима постоје три узастопна проста броја.

Доказ. Докажимо да се међу датим бројевима налазе бројеви $2, 3, 5$.

Наиме, како је четврти степен непарног броја непаран, то не може свих 31 бројева бити непарно тј. један од њих мора бити паран. Како је он и прост, то он мора бити једнак 2. Слично, како четврти степени природних бројева који нису дјељиви са 3 дају остатак 1 по модулу 3, то бар један од датих 31 бројева мора бити дјељив са 3. Како је он и прост, он мора бити једнак 3.

Докажимо даље да четврти степен било ког природног броја n који није дјељив са 5, даје остатак 1 по модулу 5. Уколико је $n \equiv \pm 2$ тада је $n^4 \equiv 2^4 \pmod 5$, тј. $n^4 \equiv 1 \pmod 5$.

Сада, уколико ниједан од датих 31 бројева није дјељив са 5, тада сума њихових четвртих степена даје остатак 1 по модулу 5, што је немогуће. Значи барем један од њих је дјељив са 5, па како је и прост, једнак је 5.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

221 ●●●●

(а) Одредити најмањи природан број који има тачно 4 дјелиоца.
(б) Одредити најмањи природан број који је дјељив са 30 и има тачно 12 дјелиоца.

Доказ. (а) Ако је $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја n, тада је $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$. Да бисмо одредили n треба одредити:

- k - број међусобно различитих простих дјелилаца од n
- $p_1, p_2, \ldots, p_k$ просте чиниоце броја n
- $\alpha_1, \alpha_2, \ldots, \alpha_k$,

тако да је $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ најмањи број са особином:

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1) = 4.$$

Пошто је $\alpha_i + 1 \geq 2, i = 1, 2, \ldots, k$ и $4 = 2 \cdot 2$ слиједи да је $k = 2$,тј. да n има само два проста фактора и при томе је

$$\alpha_1 + 1 = 2 \text{ и } \alpha_2 + 1 = 2 \text{ тј. } \alpha_1 = 1 \text{ и } \alpha_2 = 1.$$

Дакле, n је производ два проста броја ($n = p_1 \cdot p_2$), а најмањи међу њима је производ прва два проста броја ($p_1 = 2$ и $p_2 = 3$). Дакле, $n = 6$.
(б) Нека је n тражени број. Пошто $30 \mid n$, слиједи да $2 \mid n$, $3 \mid n$ и $5 \mid n$. Тада је

$$n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \ldots \qquad (\alpha, \beta, \gamma \geq 1),$$

па је

$$\tau(n) = (\alpha+1)(\beta+1)(\gamma+1)(\ldots) = 12 = 2 \cdot 2 \cdot 3,$$

одакле се види да број n нема других простих дјелилаца (осим 2, 3 и 5), тј. да је $n = 2^\alpha{\cdot}3^\beta{\cdot}5^\gamma$, као и да је, због услова минималности броја n,

$$\alpha+1 = 3,\ \beta+1 = 2,\ \gamma+1 = 2.$$

Дакле,тражени број је $n = 2^2 \cdot 3 \cdot 5 = 60$.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

222
●●●●

Доказати да за сваки прост број p важи $(p-2)! \equiv 1 \pmod p$.

Доказ. Према Вилсоновој теореми важи:

$$\begin{gathered}
(p-1)! + 1 \equiv 0 \pmod p \\
(p-2)! \cdot (p-1)! + 1 \equiv 0 \pmod p \\
(p-2)! \cdot p - (p-2)! + 1 \equiv 0 \pmod p \\
p \cdot (p-2)! - ((p-2)! - 1) \equiv 0 \pmod p \\
(p-2)! - 1 \equiv 0 \pmod p.
\end{gathered}$$

Одакле слиједи,

$$(p-2)! \equiv 1 \pmod p.$$

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

223
●●●●

Наћи све просте бројеве p, q, r који задовољавају једначину
$p(p+1) + q(q+1) = r(r+1)$.

Доказ. Желимо да нађемо сва рјешења једначине $p(p+1)+q(q+1) = n(n+1)$, тако да су p и q прости бројеви, а n природан број. Из дате једначине имамо:

$$p(p+1) = n(n+1) - q(q+1) = (n-q)(n+q+1)$$

и мора бити $n > q$.
Како је p прост број, имамо да $p \mid n - q$ или $p \mid n + q + 1$.
Ако $p \mid n - q$, онда је $p \leq n - q$ из чега слиједи да је $p(p + 1) \leq (n - q)(n + q + 1)$, па је $n + q + 1 \leq n - q + 1$. То је немогуће.
Дакле, $p \mid n + q + 1$, што значи да за неки природан број k важи:

$$n + q + 1 = kp \implies p + 1 = k(n - q) \tag{3.1}$$

Ако је $k = 1$, онда је $n+q+1 = p$ и $p+1 = n-q$, одакле слиједи $p-q = n+1$ и $p+q = n+1$. То је немогуће. Дакле, $k > 1$.

Из (3.1) лако добијамо:

$$2q = (n + q) - (n - q) = kp - 1 - (n - q) = \quad = k[k(n - q) - 1] - 1 - (n - q) = (k + 1)[(k - 1)(n - q) - 1].$$

Како је $k \geq 2$, имамо $k + 1 \geq 3$. Лијева страна посљедње једнакости има само $1, 2, q, 2q$ као своје дјелиоце (позитивне,цијеле бројеве). На основу тога је

$$k + 1 = q \text{ или } k + 1 = 2q.$$

Ако је $k + 1 = q$, онда је $(k - 1)(n - q) = 3$. Одатле слиједи $(q - 2)(n - q) = 3$. Добијамо:

$$q - 2 = 1, n - q = 3, k = q - 1 \implies q = 3, n = 6, k = 2 \text{ и на основу (3.1) } p = 5$$
$$\text{или}$$
$$q - 2 = 3, n - q = 1, k = q - 1 \implies q = 5, n = 6, k = 4 \text{ и на основу (3.1) } p = 3$$

С друге стране, ако је $k+1 = 2q$ онда је $(k-1)(n-k) = 2$. Одатле слиједи $2(q-1)(n-q) = 2$. Добијамо да је $q - 1 = 1, n - q = 1$ тј. $q = 2, n = 3$ и на основу (3.1) $p = 2$. Тако да, за све природне бројеве n и просте бројеве p, q долазимо до рјешења:

1) $p = q = 2, n = 3, p = 2$
2) $p = 5, q = 3, n = 6$ и
3) $p = 3, q = 5, n = 6$.

Примијетимо да је n прост број само у првом случају, па је то наше коначно рјешење.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

224 ●●●●

У скупу од било која три узастопна цијела броја већа од 7, постоји најмање један који има најмање два различита проста дјелиоца. Доказати.

Доказ. Претпоставимо да сваки од бројева $n, n+1, n+2$, гдје је $n > 7$ има само један прост дјелилац. Ниједан од ових бројева није дјељив са 6, што значи да n мора бити облика $6k + 1, 6k + 2, 6k + 3$, гдје је k природан број.

Ако је $n = 6k+1$, онда број $6k+2$, који је паран и који има само једног простог дјелиоца, мора бити облика 2^m. Сада, како је $n > 7$, што значи да је $6k+2 = n+1 > 8$, број m мора бити већи од 3. Број $n+2 = 6k+3$ је дјељив са 3 и ако има само један прост дјелилац онда је он облика 3^s. Како је $6k+3 = n+3 > 9$, број s мора бити већи од 2. Штавише, имамо и $3^s - 2^m = 1$. Ова једначина има два рјешења у скупу цијелих бројева и то су: $s = m = 1$ и $s = 2, m = 3$. То добијамо на следећи начин:

Ако је s непаран и $s > 1$, онда је $s = 2k+1$, гдје је k природан број и с обзиром на то да је $3^2 \equiv 1 \pmod 4$ имамо да је $3^{2k+1} \equiv 3 \pmod 4$, одакле слиједи $2^m = 3^s - 1 = 3^{2k+1} - 1 \equiv 2 \pmod 4$. Значи, за $m \leq 1$ или $m = 1$. Пошто је $3^s - 2^m = 1$ имамо $s = 1$. Ако је s паран, $s = 2k$, за неки природан број k, онда имамо $2^m = 3^{2k} - 1 = (3^k - 1)(3^k + 1)$. Два узастопна парна броја $3^k - 1, 3^k + 1$ су, дакле, степени броја 2. Одавде слиједи да су то бројеви 2 и 4, па добијамо да је $k = 1$, а затим и да је $s = 2$. Добили смо рјешење $s = 2, m = 3$.

Ако је $n = 6k+2$, онда је $n = 2^m$ и $n+1 = 6k+3 = 3^s$, гдје је $m > 2$ (како је $n > 6$). Добијамо $3^s - 2^m = 1$, што је немогуће за $m > 3$.

Коначно, ако је $n = 6k+3$, онда је $n = 3^s, n+1 = 2^m$ и с обзиром на то да је $n > 7$ добијамо $s \geq 2, m > 3$, док једначина $2^m - 3^s = 1$ има само једно рјешење у скупу цијелих бројева и то $m = 2, s = 1$. То добијамо на сљедећи начин:

Како је $3^2 \equiv 1 \pmod 8$, имамо да је $3^{2k} + 1 \equiv 2 \pmod 8$ и $3^{2k-1} + 1 \equiv 4 \pmod 8$, што показује да, за природан број s, број $3^s + 1$ није дјељив са 8. Дакле, није дјељив са 2^m за $m \geq 3$. Тако да, ако за природне бројеве m и s имамо $2^m - 3^s = 1$, онда мора бити $m \leq 2$. Добијамо да важи $2 - 3^n = 1$ или $2^2 - 3^n = 1$. Прва могућност је немогућа, па је коначно рјешење $m = 2, s = 1$.

Дакле, претпоставка да, за $n > 7$, ниједан од бројева $n, n+1, n+2$ нема више од једног простог дјелиоца, нас је довела до контрадикције.
С друге стране, за $n = 7$ имамо $n+1 = 2^3, n+2 = 3^2$ и сваки од бројева $n, n+1, n+2$ има само један прост дјелилац.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

225

Нека су a и b природни бројеви, узајамно прости са c и $b \neq 1$. Доказати да постоји природан број n, такав да $ab^n + c$ није прост број.

Доказ. Нека је $A_n = ab^n + c, n \in \mathbb{N}$, низ природних бројева. Очигледно је
$A_n = ab(b^{n-1} - 1) + ab + c$.

Ако је $|ab + c| > 1$, постоји прост број p такав да $p \mid ab + c$. Како је нзд$(a, c) = 1$ и нзд$(b, c) = 1$, имамо да је нзд$(ab, c) = 1$, тј. нзд$(p, b) = 1$. Према Малој Фермаовој теореми имамо да $p \mid b^{p-1} - 1$. Дакле, $p \mid A_p$.

Ако је $|ab + c| = 1$, тј. $ab + c = d, d \in \{-1, 1\}$, имамо

$$A_{n+2} = ab^3(b^{n-1} - 1) + ab(b^2 - 1) + d.$$

Тада је $ab(b^2 - 1) + d > 1$, па постоји прост број p такав да

$$p \mid ab(b^2 - 1) + d, \text{ тј. } p \mid ab^3 + c.$$

Како је нзд$(ab^3, c) = 1$, то $p \nmid b$, па према Малој Фермаовој теореми слиједи $p \mid b^{p-1} - 1$, тј. $p \mid A_{p+2}$.

☐

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

226

Наћи све просте бројеве p за које је $p^3 - p + 1$ потпуни квадрат.

Доказ. Нека је $p^3 - p + 1 = n^2$,тј. $p(p^2 - 1) = (n - 1)(n + 1)$.
Имамо два случаја:
1. $p|n - 1$. Тада је $n - 1 = kp$ за неко $k \in N$ па добијамо да је $p(p - k^2) = 2k + 1$. Одатле слиједи $p - k^2 \geq 1$ и $p \leq 2k + 1$,одакле је $k^2 + 1 \leq 2k + 1$,односно $k = 1$ или $k = 2$.
За $k = 2$ добијамо $p = 5$,а $k = 1$ не даје решење;

2. $p|n + 1$. Тада је $n + 1 = lp$ за неко $l \in N$ па добијамо $2l - 1 = p(l^2 - p)$. Пошто је $p \geq 3$ (директно провјеравамо) и $l^2 - p \geq 1$ слиједи $l \geq 2$ и $p \leq 2l - 1$ па имамо

$$2l - 1 = p(l^2 - p) \geq p(l^2 - 2l + 1) \geq 3(l - 1)^2 \geq 3(l - 1) \geq 2l - 1.$$

Значи,све те неједнакости морају бити једнакости,па је $l = 2$ и $p = 3$. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

227

а) Доказати да не постоје прости бројеви p и q такви да је број

$$p^2 + 2012pq + q^2$$

потпун квадрат.
б) Доказати да постоји бесконачно много парова узајамно простих природних бројева (m, n) тако да је

$$m^2 + 2012mn + n^2$$

потпун квадрат.

Доказ. (а) Уколико су p и q непарни бројеви важи

$$p^2 + 2012pq + q^2 \equiv 1 + 0 + 1 \equiv 2 \pmod 4.$$

па $p^2 + 2012pq + q^2$ није потпун квадрат. Дакле, барем један од p и q је паран, па је једнак 2. Нека је (без смањења општости) $p = 2$. Уколико је q непаран тада је

$$p^2 + 2012pq + q^2 \equiv 4 + 0 + 1 \equiv 5 \pmod 8),$$

па $p^2+2012pq+q^2$ опет није потпун квадрат. Уколико је $p = q = 2$, тада је $p^2+2012pq+q^2 = 4 \cdot 2014$, што није потпун квадрат.
б) Посматрајмо једначину

$$m^2 + 2012mn + n^2 - t^2 = 0.$$

Ова једначина има рјешења у скупу природних бројева ако и само ако је $(2012^2 - 4)n^2 + 4t^2$ потпун квадрат, тј. ако је

$$1005 \cdot 1007 \cdot n^2 = s^2 - t^2,$$

гдје је s природан број. Нека су зато s и t такви да је $s - t = 1005 \cdot 1007$ $s + t = n^2$. Тада је

$$m = \tfrac{(n-1005)(n-1007)}{2}.$$

Уколико је још n непаран, већи од 1007 и узајамно прост са 1005 и 1007, тада је нзд$(m, n) = 1$ тј. (m, n) је пар са траженим својством. Оваквих бројева n има бесконачно много, чиме је доказ завршен. □

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

228

Одредити све просте бројеве p такве да $p^{2010} \mid 2010^{p^{2010}} + 1$

Доказ. Нека је p решење задатка. Тада из $2010^{p^{2010}}+1\equiv 0 \pmod{p}$ и на основу мале Фермаове теореме ($a^p\equiv a \pmod{p}$) добијамо:

$$2010^{p^{2010}}+1\equiv \left(2010^{p^{2009}}\right)^p+1\equiv 2010^{p^{2009}}+1\equiv \ldots \equiv 2010^{p^1}+1\equiv 2010+1\equiv 2011 \pmod{p}$$

па је $2011\equiv 0 \pmod{p}$ тј. $p\mid 2011$. Како је 2011 прост број то онда $p=2011$ је једино p које може бити решење задатка. Докажимо то. Нека је $s=2011^{2010}$. Из биномне формуле слиједи

$$2010^s+1=(2011-1)^s+1=1+\sum_{i=0}^{s}\binom{s}{i}2011^i\cdot(-1)^{s-i}=\sum_{i=1}^{s}\binom{s}{i}2011^i\cdot(-1)^{s-i}(*)$$

За $i\geq 2011$ важи да $2011^{2010}\mid 2011^i$ па $s\mid \binom{s}{i}2011^i\cdot(-1)^{s-i}$. За $1\leq i<2010$ важи нзд$(i!,2011)=1$. Како је бројилац разломка $\binom{s}{i}=\frac{s(s-1)\cdot\ldots\cdot(s-i+1)}{i!}$ дјељив са 2011^{2010} (пошто је $s=2011^{2010}$) слиједи да (за $1\leq i<2010$) важи $s\mid\binom{s}{i}$, па и $s\mid\binom{s}{i}2011^i\cdot(-1)^{s-i}$. Дакле, сви сабирци у **(*)** дјељиви су са s тј. $p=2011$ је једино решење задатка.

□

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

229

Одредити све просте бројеве p и q, за које је

$$p^{q+1}+q^{p+1}$$

потпун квадрат.

Доказ. Једино рјешење је $p=q=2$. Претпоставимо да је p непарно и $p^{q+1}+q^{p+1}=x^2$. Тада је $p^{q+1}=(x-q^{\frac{p+1}{2}})(x+q^{\frac{p+1}{2}})$. Ако су оба чиниоца $x\pm q^{\frac{p+1}{2}}$ дјељиви са p, онда $p\mid 2q^{\frac{p+1}{2}}$, па мора бити $p=q$, али тада је $x^2=2p^{p+1}$, што је немогуће.
Једина преостала могућност је $x-q^{\frac{p+1}{2}}=12q^{\frac{p+1}{2}}+1=x+q^{\frac{p+1}{2}}=p^{q+1}$. И ово је немогуће за q непарно, јер је тада $p^{q+1}\equiv 1$ и $2q^{\frac{p+1}{2}}+1\equiv 3 \pmod{4}$. Слиједи да је $q=2$.
Тада добијамо

$$2^{\frac{p+3}{2}}=p^3-1=(p-1)(p^2+p+1)$$

Међутим, p^2+p+1 је увијек непарно и веће од 1, што је контрадикција, па важи да је $p=q=2$

□

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://imomath.com/srb/`

230

Нека су a и b узајамно прости непарни природни бројеви. Наћи све могуће вриједности броја нзд$(2^a+2^{\frac{a+1}{2}}+1, 2^b+2^{\frac{b+1}{2}}+1)$.

Доказ. Примијетимо да је $(2^a+2^{\frac{a+1}{2}}+1)(2^a-2^{\frac{a+1}{2}}+1)=(2^a+1)^2-2^{a+1}=2^2+1$.Слиједи да је $d=(2^a+2^{\frac{a+1}{2}}+1,2^b+2^{\frac{b+1}{2}}+1)\mid(2^2+1,2^{2b}+1)\mid(2^4-1,2^{4b}-1)=2^{(4,4b)}-1=15$. (a и b узајамно прости). Притом $3\nmid 2^2+1$, па имамо $d\mid 5$.
Могуће вриједности су 1 и 5. За $\ =b=1$ је $d=5$, док је sa $(,b)=(1,3)d=1$ ☐

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://imomath.com/srb/`

231
●●●●

Одредити све просте бројеве p за које постоји природан број n такав да су бројеви n^2+3 и $(n+1)^2+3$ дјељиви са p.

Доказ. Претпоставимо да $p\mid n^2+3$ и $p\mid n^2+2n+4$ за неко $n\in\mathbb{N}$. Стога p дијели и њихову разлику:

$$p\mid(n^2+2n+4)-(n^2+3)=2n+1$$

Даље, имамо да $p\mid(2n+1)^2$, а из услова $p\mid n^2+3$ слиједи да $p\mid 4(n^2+3)$. Отуда слиједи да:

$$p\mid(2n+1)^2-4(n^2+3)=4n-11.$$

Сада добијамо

$$p\mid 2(2n+1)-(4n-11)=13,$$

па је $p=13$ једини прост број који би могао задовољити услове задатка.

Одредимо још и неко n за које важи $13\mid n^2+3,\ (n+1)^2+3$. Како $13\mid 2n+1$, слиједи да би "кандидат" за n могао бити број 6. Како $13\mid 6^2+3,\ 7^2+3$ слиједи да је $p=13$ једини прост број за који важе услови задатка.

☐

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

232
●●●●

а) Наћи све просте бројеве p, q и r такве да је $p=q^3-r^3$.
б) Наћи све просте бројеве p и q такве да је број $p^2+2pq+q^2$ степен броја 5.

Доказ. а) Имамо да је $p=q^3-r^3=(q-r)(q^2+qr+r^2)$.
Како је број p прост знамо да он има само два дјелиоца, број 1 и сам број p, на основу тога разликоваћемо два случаја:

- Нека је $q - r = 1$ и $q^2 + qr + r^2 = p$
  Бројеви 2 и 3 су једина два узастопна проста броја па закључујемо да је $q = 3$ и $r = 2$.
  Одакле је, $p = 3^2 + 3 \cdot 2 + 2^2 = 19$.

- Нека је $q - r = p$ и $q^2 + qr + r^2 = 1$.
  Једначина $q^2 + qr + r^2 = 1$ је немогућа јер су q и r прости бројеви, па је $q^2 + qr + r^2 > 1$.
  Дакле, у овом случају немамо рјешење.

б) Нека је $p^2 + 3pq + q^2 = 5^n$. Како је $p \geq 2$ и $q \geq$, добијамо да је

$$p^2 + 3pq + q^2 \geq 20,$$

што значи да је $n \geq 2$. Значи да је $p^2 + 3pq + q^2$ дјељив са 25.

Имамо да је $p^2 + 3pq + q^2 = (p - q)^2 + 5pq$, одакле је $(p - q)^2 + 5pq$ дјељив са 5, па је тада $(p - q)^2$ дјељив са 5, тј. $5 \mid (p - q)$ одакле слиједи да $25 \mid (p - q)^2$.

Како $25 \mid (p - qq)^2 + 5pq$ и $25 \mid (p - q)^2$, слиједи да $25 \mid 5pq$, тј. $p = 5$ или $q = 5$.

Међутим, ако је $p = 5$, због услова да $5 \mid p - q$ слиједи да је $q = 5$.

Коначно, јединствено рјешење је $p = q = 5$ и тада је $p^2 + 3pq + q^2 = 5^3$.

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/13890/mod_resource/content/1/Prosti%20brojevi%20%28%C4%8Detvrti%20termin%29%2021.3.2020..pdf`

233

а) Наћи природан број n такав да $3 \mid n$, $4 \mid n$ и $\tau(n) = 14$?
б) Природан број n има непаран број позитивних дјелилаца ако и само ако је он потпун квадрат. Доказати.

Доказ. а) Како $3 \mid n$ и $4 \mid n$, то број n можемо записати као $n = 2^{\alpha_1} \cdot 3^{\alpha_2}$, при чему није тешко закључити да је $\alpha_1 \geq 2$ и $\alpha_2 \geq 1$, да би услови задатка били испоштовани.
Тада је $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) = 2 \cdot 7 = 14$.

Тражимо најмањи природан број па узмимо да је $\alpha_1 + 1 = 7$ и $\alpha_2 + 1 = 2$, тј. $\alpha_1 = 6$ и $\alpha_2 = 1$.
Сада је, $n = 2^6 \cdot 3^1 = 192$.

б) Нека је $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, гдје су $p_1, p_2, \ldots, p_k$ различити прости бројеви такви да је $p_1 < p_2 < \ldots < p_k$, а $\alpha_1, \alpha_2, \ldots, \alpha_k$ су јединствени природни бројеви.

$$\begin{aligned}\tau(n) \text{ - непаран број } &\iff \tau(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) \text{ - непаран број}\\ &\iff (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) \text{ - непаран број}\\ &\iff \alpha_1+1, \alpha_2+2, \dots, \alpha_k+1 \text{ - непарни бројеви}\\ &\iff \alpha_1, \alpha_2, \dots, \alpha_k \text{ - парни бројеви}\\ &\iff \alpha_1 = 2t_1, \alpha_2 = 2t_2, \dots, \alpha_k = 2t_k, \text{ гдје } t_1, t_2, \dots, t_k \in \mathbb{N}\\ &\iff n = p_1^{2t_1} \cdot \ p_2^{2t_2} \dots p_k^{2t_k} = (p_1^{t_1} \cdot p_2^{t_2} \dots p_k^{t_k})^2\\ &\iff n \text{ је потпун квадрат.}\end{aligned}$$

$\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://imi.pmf.kg.ac.rs/moodle/pluginfile.php/13890/mod_resource/content/1/Prosti%20brojevi%20%28%C4%8Detvrti%20termin%29%2021.3.2020..pdf`

234
●●●●

Нека је $n > 6$ и нека су $a_1 < a_2 < \dots a_k$ сви природни бројеви мањи од n и узајамно прости са n. Доказати: ако је низ a_i аритметичка прогресија, тада је n прост број или степен двојке.

Доказ. На почетку уочавамо да је $a_1 = 1$ и $a_2 = p$, гдје је p најмањи прост број који не дијели n. Зато је разлика посматране аритметичке прогресије једнака $p-1$. Такође, $a_k = n-1$.
Ако је n непаран број, тада је $a_2 = 2$, па је уочена прогресија заправо $1, 2, \dots, n-1$, одакле слиједи да је број n прост.
Уколико је n паран, тада је $p \geq 3$. разматрамо два случаја. Ако је $p = 3$, тада је ријеч о прогресији $1, 3, \dots, n-1$, што значи да је n узајамно прост са сваким непарним бројем мањим од n, што је могуће само ако је $n = 2^m$ за неки природан број m. Ако је $p > 3$, слиједи да $3 \mid n$. Тада због:

$$n-2 = (n-1)-1 = a_k - a_1 = (p-1)(k-1)$$

важи $(p-1) \mid (n-2)$, па ако је q прост број и $q \mid (p-1)$, тада $q \mid (n-2)$. Међутим, $q < p$, па $q \mid n$. Отуда је $q \mid n$. Отуда је $q \mid 2$, тј. $q = 2$ као и $p - 1 = 2^s$ за $s \geq 2$, односно $p = 2^s + 1$. Пошто је p прост број, то је $s = 2^t$, $p = 2^{2^t+1}$ за $t \geq 1$. Али, сада имамо:

$$a_3 = 1 + 2(p-1) = 2p - 1 = 2^{2^t+1} + 1,$$

па $3 \mid a_3$. Зато $3 \mid \text{нзд}(a_3, n) = 1$. Контрадикција. $\square$

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

235

●●●●

За које природне бројеве n постоји природан број m тако да ниједан од бројева $m+1$, $m+2,\ldots,m+n$ није степен простог броја?

Доказ. Број x није степен простог броја ако и само ако има бар два проста фактора, што је еквивалентно растављању $x = ab$ на два узајамно проста чиниоца $a, b > 1$. Према томе, ако желимо да обезбиједимо да број $m+k$ не буде степен простог броја, можемо покушати да посматрамо број m дјељив са k, јер тада из $m = km'$ слиједи $m+k = k(m'+1)$. Да би k и $m'+1$ били узајамно прости, довољно је да $k \mid m'$.

При свему томе, мора бити $k \geq 2$. Како бисмо обезбиједили да овај услов буде испуњен, уведимо смјену $m = m_0 + 1$ и посматрајмо низ бројева

$$m_0 + 2, m_0 + 3, \ldots, m_0 + n + 1.$$

Као што смо видјели, услов $k \mid m_0$ омогућава факторизацију $m_0 + k = k(m_0' + 1)$ за погодно $m_0' \in \mathbb{N}$. Због тога, нека m_0 има облик $m_0 = (n+1)!m_1$. Тада за све $2 \leq k \leq n+1$ важи

$$m_0 + k = k\left(\frac{(n+1)!}{k}m_1 + 1\right).$$

У складу са горњим разматрањима, услов $k \mid m_1$ повлачи да

$$\text{нзд}\left(k, \frac{(n+1)!}{k}m_1 + 1\right) = 1,$$

па тада $m_0 + k$ није степен простог броја. Дакле, ако одаберемо

$$m_1 = (n+1)!,$$

имаћемо да ниједан од бројева $m_0 + 2, \ldots, m_0 + n + 1$ није степен простог броја. Стога тражени број m постоји за све $n \in \mathbb{N}$, пошто смо управо показали да је довољно узети

$$m = [(n+1)!]^2 + 1.$$

☐

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

236

●●●●

Нека је $f : \mathbb{N} \to \mathbb{N} \cup \{0\}$ таква да:
1) $f(1) = 0$;
2) $f(p) = 1$ за сваки прост број p;
3) $f(ab) = af(b) + bf(a)$ за све природне бројеве a и b.
Одредити све n за које је $f(n) = n$.

Доказ. Из услова 3) задатка слиједи

$$\frac{f(ab)}{ab} = \frac{f(a)}{a} + \frac{f(b)}{b},$$

па ако је $g(x) = \frac{f(x)}{x}$, захтјев задатка постаје да се одреде сви $n \in \mathbb{N}$ такви да је $g(n) = 1$, $g : \mathbb{N} \to \mathbb{Q}^+ \cup \{0\}$ таква да:
1) $g(1) = 0$;
2) $g(p) = \frac{1}{p}$ за сваки прост број p;
3) $g(ab) = g(b) + g(a)$ за све природне бројеве a и b.
Из новог услова 3) слиједи да за $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$ (канонска факторизација броја n) важи $g(n) = \alpha_1 g(p_1) + \alpha_2 g(p_2) + \ldots + \alpha_k g(p_k)$, па треба одредити све n за које је

$$\frac{\alpha_1}{p_1} + \frac{\alpha_2}{p_2} + \ldots + \frac{\alpha_k}{p_k} = 1. \qquad (*)$$

Сви сабирци у претходној једнакости су позитивни, па је $(\forall i \in \{1, 2, \ldots, k\})\ \alpha_i \leq p_i$. Након множења исте једнакости са $p_1 \cdot p_2 \cdot \ldots \cdot p_k$, добија се једнакост у којој су сви сабирци сем једног дјељиви са p_i, па и тај сабирак $(p_1 \cdot p_2 \cdot \ldots \cdot p_k \cdot \frac{\alpha_i}{p_i})$ мора бити дјељив са p_i, па $p_i \mid \alpha_i$, одакле је $\alpha_i \geq p_i$ (за свако $\{1, 2, \ldots, k\}$).
Слиједи да су сви сабирци у $(*)$ једнаки 1, па се у тој једнакости појављује само један сабирак, односно тражени бројеви су бројеви облика p^p, гдје је p прост број. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

237
●●●●

(Wilson-ова теорема) Ако је p прост број, онда је $(p-1)! \equiv -1 \pmod{p}$.

Доказ. За $p = 2$ и $p = 3$ конгруенција је очигледна, па претпоставимо да је $p \geq 5$. Групишимо чланове скупа $2, 3, \ldots, p-2$ у парове (i, j) са својством $i \cdot j \equiv 1 \pmod{p}$. Очигледно је $i \neq j$ јер би у том случају $i^2 \equiv 1 \pmod{p}$, па би $(i-1)(i+1) = i^2 - 1 \equiv 0 \pmod{p}$, а то је немогуће јер је $0 < i-1 < i+1 < p$. Тако добијамо $\frac{p-3}{2}$ конгруенција, па имамо да важи

$$2 \cdot 3 \cdot \ldots \cdot (p-2) \equiv 1 \pmod{p},$$

слиједи

$$(p-1)! \equiv 1 \cdot 1 \cdot (p-1) \equiv -1 \pmod{p}.$$

Важи и обратно тврђење.
Нека важи $(p-1)! \equiv -1 \pmod{p}$ и нека p није прост. Тада p има дјелитељ d, $1 < d < p$ и d дијели $(p-1)!$. Међутим, тада d мора дијелити -1, што је контрадикција. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

238

Нека је p прост број. Докажимо да је $(p-1)!+1$ степен од p ако и само ако је $p = 2, 3$ или 5.

Доказ. Најприје имамо:

$$(2-1)!+1 = 2^1, \quad (3-1)!+1 = 3^1, \quad (5-1)!+1 = 5^2.$$

Ако је $p > 5$, онда се у $(p-1)!$ појављују чиниоци $2, p-1$ и $\frac{p-1}{2}$, па $(p-1)^2 \mid (p-1)!$. Ако би било
$(p-1)!+1 = p^k = [(p-1)+1]^k = (p-1)^k + k(p-1)^{k-1} + \ldots + \binom{k}{2}(p-1)^2 + k(p-1)+1$,
онда би имали да $(p-1) \mid k$. То би повлачило да је $k \geq p-1$, те $(p-1)!+1 < (p-1)^{p-1}+1 < p^{p-1} \leq p^k$, што је контрадикција. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

239

Одредити све просте бројеве p тако да је $2p$ седми степен неког природног броја.

Доказ. Нека је тражени природни број n. Према условима задатка је $2p+1 = n^7$, тј. $n^7 - 1 = (n-1)(n^6+n^5+n^4+n^3+n^2n+1) = 2p$. Како су 1, 2, p и $2p$ једини чиниоци броја $2p$, то су могући следећи случајеви:
1) Ако је $n-1 = 1$, онда је $n = 2$, па је $(n^6+n^5+n^4+n^3+n^2+n+1) = 2p = 127$, што није могуће, јер је $2p$ паран, а 127 непаран број ;
2) Ако је $n-1 = 2$, онда је $n = 3$, па је $(n^6+n^5+n^4+n^3+n^2+n+1) = 1093 = p$, Како је 1093 прост број, то је уређени пар (3, 1093) једно рјешење проблема.
3) Ако је $n-1 = p$, онда је $n = p+1 \geq 3$, па је $(n^6+n^5+n^4+n^3+n^2+n+1) \geq n+1 \geq 3$ што значи да у овом случају нема рјешења.
4) Ако је $n-1 = 2p$, онда је $(n^6+n^5+n^4+n^3+n^2+n+1) = 1$,па је $(n^6+n^5+n^4+n^3+n^2+n) = 0$. Претходна једначина има једина реална рјешења $n = 0$ или $n = -1$, па проблем опет нема рјешења, јер 0 и -1 нису природни бројеви.

☐

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

240

Природни бројеви $a > b > 1$ су такви да $b^2+a-1 \mid a^2+b-1$. Доказати да b^2+a-1 није степен простог броја.

Доказ. Претпоставимо да $p^n = b^2 + a - 1 \mid a^2 + b - 1$, гдје је p прост број. Како $b^2 + a - 1 \mid (b-1)^2 - a^2$, сабирањем добијамо $p^n \mid (b^2-1)^2 + (b-1) = b(b-1)(b^2+b-1)$. Како су чиниоци $b-1$, b и b^2+b-1 узајамно прости по паровима, нпр. $(b-1, b^2+b-1\ ) {=} (b-1, b) {=} 1$ и $p^n < b(b-1)$, слиједи да $p^n \mid b^2+b-1$ и одатле $p^n \mid a-b$, што је немогуће јер $0 < a-b < p^n$. ☐

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://imomath.com/srb/`

241

Колико има природних бројева n таквих да важи једнакост $5p{+}13q = 65n$, ако су p и q прости бројеви?

Доказ. Ако је $5p + 13q = 65n$, онда је $5p = 13(5n - q)$, па $5p$ мора бити дјељиво са 13, што значи да је $p = 13$.
Слично је и $13q = 5(13n\breve{}p)$, па је $13q$ дјељиво са 5, односно $q = 5$.
Дакле $5 \cdot 13 + 13 \cdot 5 = 65n$, па је $n = 2$, једини број који испуњава горњи услов.

☐

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

242

Нека је $n \in Z_n, n > 4$. Показати да $n \mid (n-1)!$ акко је n сложен број.

Доказ. $(\Rightarrow)$

$n \mid (n-1)!$. Треба показати да је n сложен. Претпоставимо супротно, $n = p$ је прост број. Највећи могући прости дјелилац броја $(p-1)!$ је $p-1$, па онда не може важити да $p \mid (p-1)!$ чиме долазимо до контрадикције.

$(\Leftarrow)$

Важи да је $n = ab, 1 < a, b < n$ сложен број. Покажимо да $n \mid (n-1)!$.

- Ако је $a \neq b$, из $a, b < n$ закључујемо да се и a и b појављују у производу $(n-1)! = (n-1)(n-2)\cdots 21$, па мора важити да $n \mid (n-1)!$.
- Ако је $a = b > 2$, онда пошто је $2a < ab = n$ и a и b појављују у производу $(n-1)!$ па $a^2 = n \mid (n-1)!$. Да је $a = b = 2$ $(n = 4)$, почетна претпоставка не би важила: $4 \nmid 3! = 6$.

☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://math.dartmouth.edu/~jvoight/Sp2009-255/255-EX01.pdf`

243

Наћи све просте бројеве који се могу представити и као збир и као разлика 2 проста броја.

Доказ. Означимо такав прост број са r. r не може бити 2 јер не постоје два проста броја која у збиру дају 2, што значи да је $r > 2$, тј. да је r непаран прост број. Да би био непаран, пошто је збир два броја, један од њих мора бити паран а други непаран. То значи да је један од њих 2.

Дакле, знамо да је $r = p + 2 = q - 2$, гдје су p и q прости бројеви. Међутим, у том случају су p, r и q, тј. $p, p + 2$ и $r + 2 = p + 4$ три узастопна непарна проста броја, а постоји само једна таква тројка: 3, 5 и 7. Да бисмо показали да је то једина могућа тројка овог облика примијетимо да је једини прост број који је $\equiv 0 \pmod 3$, сам број 3. Преостала 2 могућа остатка при дијељењу са 3 су 1 и 2.

- Ако је $p \equiv 1 \pmod 3 \Rightarrow p + 2 \equiv 0 \pmod 3$, па би то значило да је $p + 2 = 3$, тј. $p = 1$, а 1 није прост број. Дакле, оваквих тројки, гдје је $p \equiv 1 \pmod 3$ нема.
- Ако је $p \equiv 2 \pmod 3 \Rightarrow p + 4 \equiv 6 \equiv 0 \pmod 3$, што би значило да да би $p + 4$ био прост број морао би бити једнак броју 3, а то је немогуће.

Из овога слиједи да постоји само један прост број који задовољава дати услов, а то је број 5. И заиста, $r = 5 = 3 + 2 = 7 - 2$ □

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

244

Нека је n природан број и нека важи да $p^2 \mid n$, за сваки прости фактор p броја n. Показати да се такво n може записати у облику a^2b^3, гдје су a и b такође природни бројеви.

Доказ. Представимо n у облику $n = p_1{}^{k_1} \cdots p_r{}^{k_r}$. Из услова да $p^2 \mid n$ је $k_i \geqslant 2$.

Запишимо $p_1{}^{k_1} \cdots p_r{}^{k_r}$ као $q_{m_1}^{k_{m_1}} \cdots q_{m_s}^{k_{m_s}} q_{n_1}^{k_{n_1}} \cdots q_{n_t}^{k_{n_t}}$, при чему су k_{m_i} непарни, значи $k_{m_i} \geqslant 3$, а k_{n_i} парни, значи облика $k_{n_i} = 2v_i$

$$
\begin{aligned}
n &= q_{m_1}^{k_{m_1}} \cdots q_{m_s}^{k_{m_s}} (q_{n_1}^{2v_1} \cdots q_{n_t}^{2v_t}) \\
&= q_{m_1}^{k_{m_1}} \cdots q_{m_s}^{k_{m_s}} (q_{n_1}^{v_1} \cdots q_{n_t}^{v_t})^2 \\
&= q_{m_1}^{k_{m_1}} \cdots q_{m_s}^{k_{m_s}} (x)^2, \text{ гдје је } x = q_{n_1}^{v_1} \cdots q_{n_t}^{v_t}.
\end{aligned}
$$

Како је000 k_{m_i} непарно и $\geqslant 3$, $k_{m_i} - 3$ је парно.

$n = q_{m_1}^3 \cdots q_{m_s}^3 (q_{m_1}^{m_1-3} \cdots q_{m_s}^{m_s-3})(x^2)$

Нека је $m_i - 3 = 2w_i$, а $q_{m_1} \cdots q_{m_s} = b$.

$n = b^3 (q_{m_1}^{2w_1} \cdots q_{m_s}^{2w_s})(x^2)$

Нека је $y = q_{m_1}^{w_1} \cdots q_{m_s}^{w_s}$. Онда је $n = b^3 y^2 x^2$.

Једноставном замјеном $a = yx$ долазимо до траженог: $n = a^2 b^3$. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-mo`
`pdf`

245

Ако је p прост број, а $n > 0$ цио број, онда су једини дјелиоци броја p^n бројеви $1, p, p^2, \ldots, p^{n-1}, p^n$. Доказати.

Доказ. Прво докажимо да сваки елемент из скупа $1, p, p^2, \ldots, p^{n-1}, p^n$ заиста дијели p^n.

За било које $j \in \{1, 2, \ldots, n\}$ важи да је $p^n = p^j p^{n-j}$. Одатле је очигледно да су $1, p, p^2, \ldots, p^{n-1}, p^n$ дјелиоци броја p^n. Сада покажимо да су они и једини.

Узмимо неко $a \in Z_{>0} : a \notin \{1, p, p^2, \ldots, p^{n-1}, p^n\}$.

Нека је $a = p^j, j \in Z : j > n$. Онда је $p^j = p^n p^{j-n}$ па $p^n \mid p^j \Rightarrow p^j \nmid p^n$.

Сада узмимо a које није степен простог броја, тј. $a \notin \{p^k : k > 0\}$. Онда $\exists q, q$ - прост и q дијели a. Ако претпоставимо да a дијели p^n на основу својства транзитивности релације "дијели"слиједи да q дијели p^n. На основу Еуклидове леме о простим дјелиоцима (ако p дијели $a_1 a_2 \cdots a_n$ онда p мора дијелити макар један од бројева $a_1, a_2 \ldots, a_n$) слиједи да q дијели p. Пошто је p прост, његови једини дјелиоци су 1 и p, што је контрадикторно чињеници да q дијели p^n. Дакле, $a \nmid p^n$.

Овим је доказано почетно тврђење, да не постоји број ван скупа $1, p, p^2, \ldots, p^{n-1}, p^n$ који дијели p^n. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://proofwiki.org/wiki/Divisors_of_Power_of_Prime`

246

Наћи све просте бројеве p такве да је сума свих позитивних дјелилаца броја p^4 једнака коријену неког природног броја.

Доказ. На основу претходног задатка јасно је да је сума свих позитивних дјелиоца броја p^4 једнака $1+p+p^2+p^3+p^4$. Ако је $1+p+p^2+p^3+p^4=n^2$, гдје је n неки природан број, тада:

$$(2p^2+p)^2 < (2n)^2 < (2p^2+p+2)^2$$

јер је:

$(2p^2+p)^2 = 4p^4+4p^3+p^2$

$(2n)^2 = 4n^2 = 4(1+p+p^2+p^3+p^4) = 4p^4+4p^3+4p^2+4p+4 \qquad$ **(*)**

$(2p^2+p+2)^2 = 4p^2+4p^3+5p^2+2p+4$

Одавде видимо да је $(2n)^2 = (2p^2+p+1)^2$, тј.

$4n^2 = 4p^2+4p^3+5p^2+2p+1.$

Када од ове једнакости одузмемо једнкост **(*)** добијамо квадратну једначину:

$$p^2-2p-3=0$$

чија су рјешења $p_1=-1$ и $p_2=3$. Дакле, $p=3$ је једини прост број који задовољава услов задатка.

Провјеримо: $1+3+3^2+3^3+3^4=121=11^2$ □

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

4 Разни задаци

Диофантове једначине, Кинеска теорема о остацима, Ојелрова ϕ функција...

247

Одредити сва рјешења једначине: $3x+9y=15$, ако су x и y цијели бројеви.

Доказ. Прво гледамо да ли једначина $ax+by=c$ има рјешење.
нзд$(3,9)=3$, па једначина има рјешење. Да би ријешили једначину прво је изједначимо са 1. Значи,

$$3x+9y=1$$

Користићемо Бланкиншип методу (енг. Blankinship method). Формирамо матрицу

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Желимо елементарним трансформацијама да добијемо матрицу облика

$$\begin{bmatrix} d & x_1 & y_1 \\ 0 & x_2 & y_2 \end{bmatrix}$$

Тада је $d=ax_1+by_1$. Дакле $a=3$, $b=9$

$$\begin{bmatrix} 3 & 1 & 0 \\ 9 & 0 & 1 \end{bmatrix} \text{(прву врсту помножимо бројем (-3) и додамо другој врсти)}$$

Дакле, добијамо следећу матрицу:

$$\begin{bmatrix} 3 & 1 & 0 \\ 0 & -3 & 1 \end{bmatrix}$$

Имамо $3=3\cdot 1+9\cdot 0 \qquad (d=ax_1+by_1)$

$k=\dfrac{c}{d}=\dfrac{15}{3}=5$

$x^*=x_1\cdot k=1\cdot 5=5$

$y^* = y_1 \cdot k = 0 \cdot 5 = 0$

Коначно,

$$x = x^* + \frac{b}{d} \cdot t = 5 + \frac{9}{3} \cdot t = 5 + 3 \cdot t$$
$$y = y^* - \frac{a}{d} \cdot t = 0 + \frac{3}{3} \cdot t = -t$$

$t \in \mathbb{Z}$ □

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`http://www.naukamladima.com/index.php?page=diofantove-jednacine`

248

Одредити сва рјешења једначине: $4x + 5y = 100$, ако су x и y цијели бројеви.

Доказ. Прво гледамо да ли једначина $ax + by = c$ има рјешење.
нзд$(4, 5) = 1$ и $1 \mid 100$ па једначина има рјешење. Изједначимо једначину са 1 да би користили Бланкиншип методу (енг. Blankinship method). Значи,

$$4x + 5y = 1$$

Формирамо матрицу

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Елементарним трансформацијама желимо да добијемо матрицу облика

$$\begin{bmatrix} d & x_1 & y_1 \\ 0 & x_2 & y_2 \end{bmatrix}$$

Тада је $d = ax_1 + by_1$. Дакле $a = 4$, $b = 5$

$$\begin{bmatrix} 4 & 1 & 0 \\ 5 & 0 & 1 \end{bmatrix} \text{(прву врсту помножимо бројем 5, а другу бројем 4)}$$

Добијамо следећу матрицу:

$$\begin{bmatrix} 20 & 5 & 0 \\ -20 & 0 & -4 \end{bmatrix} \text{(саберемо врсте)}$$

Па имамо

$$\begin{bmatrix} 20 & 5 & 0 \\ 0 & 5 & -4 \end{bmatrix}$$

Имамо $20 = 4 \cdot 5 + 0 \cdot 5 \qquad (d = ax_1 + by_1)$

$$k = \frac{c}{d} = \frac{100}{20} = 5$$

$x^* = x_1 \cdot k = 5 \cdot 5 = 25$
$y^* = y_1 \cdot k = 0 \cdot 5 = 0$

Коначно,

$$x = x^* + \frac{b}{d} \cdot t = 25 + \frac{5}{20} \cdot t = 25 + \frac{1}{4} \cdot t, \qquad t \in \mathbb{Z}$$

$$y = y^* - \frac{a}{d} \cdot t = 0 - \frac{4}{20} \cdot t = -\frac{1}{5} \cdot t, \qquad t \in \mathbb{Z}$$ □

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`http://www.naukamladima.com/index.php?page=diofantove-jednacine`

249

Одредити $d =$ нзд$(222, 102)$ и наћи цијеле бројеве x и y такве да је $222x + 102y = d$.

Доказ. Да нађемо нзд$(222, 102)$ користићемо Еуклидов алгоритам.

$222 = 102 \cdot 2 + 18$
$102 = 18 \cdot 5 + 12$
$18 = 12 \cdot 1 + 6$
$12 = 6 \cdot 2 + 0$

Дакле, нзд$(222, 102) = 6$, па тражимо рјешење једначине $222x + 102y = 6$ користећи Бланкиншип методу (енг. Blankinship method).

Формирамо матрицу

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Елементарним трансформацијама желимо да добијемо матрицу облика

$$\begin{bmatrix} d & x_1 & y_1 \\ 0 & x_2 & y_2 \end{bmatrix}$$

Тада је $d = ax_1 + by_1$. Дакле $a = 222$, $b = 102$

$$\begin{bmatrix} 222 & 1 & 0 \\ 102 & 0 & 1 \end{bmatrix} \; (II \cdot (-2) + I)$$

Добијамо матрицу:

$$\begin{bmatrix} 18 & 1 & -2 \\ 102 & 0 & 1 \end{bmatrix} \quad (I\cdot(-5)+II)$$

Па имамо

$$\begin{bmatrix} 18 & 1 & -2 \\ 12 & -5 & 11 \end{bmatrix} \quad (II\cdot(-2)+I)$$

Даљом трансформацијом добијамо

$$\begin{bmatrix} -6 & 11 & -24 \\ 12 & -5 & 11 \end{bmatrix} \quad (I\cdot 2+II)$$

На крају смо добили матрицу

$$\begin{bmatrix} -6 & 11 & -24 \\ 0 & 17 & -37 \end{bmatrix}$$

Имамо $-6 = 11\cdot 222 - 24\cdot 102 \qquad (d = ax_1 + by_1)$

$$k = \frac{c}{d} = \frac{6}{-6} = -1$$

$$x^* = x_1\cdot k = 11\cdot(-1) = -11$$
$$y^* = y_1\cdot k = -24\cdot(-1) = 24$$

Коначно,

$$x = x^* + \frac{b}{d}\cdot t = -11 - \frac{102}{6}\cdot t = -11 - 17\cdot t, \qquad t\in\mathbb{Z}$$

$$y = y^* - \frac{a}{d}\cdot t = 24 + \frac{222}{6}\cdot t = 24 + 37\cdot t, \qquad t\in\mathbb{Z}$$ □

(**Merван Дрпљанин 4/19 Ц**) задатак преузет са `http://elib.mi.sanu.ac.rs/files/journals/nm/245/nm581202.pdf`

250 ●●●●

Ријешити систем конгруенција:

$$m \equiv 11 \pmod{74}$$
$$m \equiv 13 \pmod{63}$$

Доказ. Ако је m рјешење тада је $m = 11 + 74x$, $x\in\mathbb{Z}$. Такође, $m = 13 + 63y$, $y\in\mathbb{Z}$. Када изједначимо ове двије једначине добијамо

$$11 + 74x = 13 + 63y$$

односно

$$74x - 63y = 2$$

Даље рјешавамо као Диофантову једначину користећи Бланкиншип методу (енг. Blankinship method). Ова једначина има рјешење јер нзд$(74, 63) = 1$ и $1 \mid 2$.
Формирамо матрицу

$$\begin{bmatrix} a & 1 & 0 \\ b & 0 & 1 \end{bmatrix}$$

Елементарним трансформацијама желимо да добијемо матрицу облика

$$\begin{bmatrix} d & x_1 & y_1 \\ 0 & x_2 & y_2 \end{bmatrix}$$

Тада је $d = ax_1 + by_1$. Дакле $a = 74$, $b = -63$
Матрица коју елементарним трансформацијама треба да сведемо на наведени облик (а коју читаоцу остављамо да одради сам) је

$$\begin{bmatrix} 74 & 1 & 0 \\ -63 & 0 & 1 \end{bmatrix}$$

Добијамо следећу матрицу

$$\begin{bmatrix} 60 & 120 & 140 \\ 0 & 126 & 148 \end{bmatrix}$$

Имамо $60 = 74 \cdot 120 - 63 \cdot 140 \qquad (d = ax_1 + by_1)$

$$k = \frac{c}{d} = \frac{2}{60} = \frac{1}{30}$$

$$x^* = x_1 \cdot k = 120 \cdot \frac{1}{30} = 4$$

$$y^* = y_1 \cdot k = 140 \cdot \frac{1}{30} = \frac{14}{3}$$

Коначно,

$$x = x^* + \frac{b}{d} \cdot t = 4 - \frac{63}{60} \cdot t, \qquad t \in \mathbb{Z}$$

$$y = y^* - \frac{a}{d} \cdot t = \frac{14}{3} - \frac{74}{60} \cdot t, \qquad t \in \mathbb{Z}$$

□

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`http://www.mathos.unios.hr/~mdjumic/uploads/diplomski/TOB02.pdf`

251

Ријешити систем конгруенција:

$$x \equiv -2 \pmod{6}$$
$$x \equiv 1 \pmod{5}$$
$$x \equiv 2 \pmod{7}$$

Доказ. Према Кинеској теореми о остацима рјешење добијамо по следећој формули:

$$x \equiv a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \ldots + a_n \cdot M_n \cdot y_n \pmod{M}$$

при чему је n број конгруенција (у овом случају $n = 3$).
Напоменимо,
$a_1, a_2 \ldots + a_n$ су десни коефицијенти конгруенције,
$m_1, m_2 \ldots + m_n$ су модули конгруенције,
$M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$,

$M_1 = \dfrac{M}{m_1}$, $M_2 = \dfrac{M}{m_2}$, $\ldots$, $M_n = \dfrac{M}{m_n}$.

Сада прелазимо на рачунање вриједности. Примијетимо да уколико је десни коефицијент конгруенције мањи од нуле, њега трансформишемо тако што додајемо вриједност модула све док коефицијент не буде позитиван. Дакле, $x \equiv -2 \pmod{6}$, $(-2) + 6 = 4$, па имамо $x \equiv 4 \pmod{6}$.

$$M = m_1 \cdot m_2 \cdot m_3 = 6 \cdot 5 \cdot 7 = 210$$

$$M_1 = \frac{M}{m_1} = \frac{210}{6} = 35$$
$$M_2 = \frac{M}{m_2} = \frac{210}{5} = 42$$
$$M_3 = \frac{M}{m_3} = \frac{210}{7} = 30$$

За коначно рјешење система конгруенције примјеном Кинеске теореме о остацима неопходно је да нађемо парцијалне конгруенције y_1, y_2, y_3.

$M_1 \cdot y_1 \equiv 1 \pmod{m_1}$, односно $35 \cdot y_1 \equiv 1 \pmod{6}$. Коефицијент уз y_1 можемо трансформисати по модулу 6, па имамо $5 \cdot y_1 \equiv 1 \pmod{6}$. Рјешење ове конгруенције можемо наћи међу бројевима који су мањи од модула за 1, тј. (0,1,2,3,4,5). Видимо да је рјешење 5. Дакле, $y_1 = 5$.

$M_2 \cdot y_2 \equiv 1 \pmod{m_2}$, односно $42 \cdot y_2 \equiv 1 \pmod{5}$. Трансформисаћемо коефицијент уз y_2 по модулу 5, па имамо $2 \cdot y_2 \equiv 1 \pmod{5}$. Рјешења тражимо међу бројевима (0,1,2,3,4). Рјешење је 3. Дакле, $y_2 = 3$.

$M_3 \cdot y_3 \equiv 1 \pmod{m_3}$, односно $30 \cdot y_3 \equiv 1 \pmod{7}$. Трансформацијом коефицијента уз y_3 по модулу 7 добијамо $2 \cdot y_3 \equiv 1 \pmod{7}$, па рјешења тражимо међу бројевима (0,1,2,3,4,5,6).

Рјешење је 4. Дакле, $y_3 = 4$.

Остаје да вриједности уврстимо у формулу. Добијамо

$x \equiv 4 \cdot 35 \cdot 5 + 1 \cdot 42 \cdot 3 + 2 \cdot 30 \cdot 4 \pmod{210}$
$x \equiv 700 + 126 + 240 \pmod{210}$

извршимо трансформацију бројева по модулу 210 (оних бројева који су већи од 210).

$x \equiv 70 + 126 + 30 \pmod{210}$
$x \equiv 226 \pmod{210}$

Такође трансформишемо 226 по модулу 210 и коначно добијамо

$x \equiv 16 \pmod{210}$. □

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`https://www.youtube.com/watch?v=DeJTT1uXFwY`

252

Ријешити систем конгруенција:

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \end{aligned}$$

Доказ. Према Кинеској теореми о остацима рјешење добијамо по следећој формули:

$$x \equiv a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \ldots + a_n \cdot M_n \cdot y_n \pmod{M}$$

при чему је n број конгруенција (у овом случају $n = 4$).

Напоменимо,
$a_1, a_2 \ldots + a_n$ су десни коефицијенти конгруенције,
$m_1, m_2 \ldots + m_n$ су модули конгруенције,
$M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$,

$M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, $\ldots$, $M_n = \frac{M}{m_n}$.

Сада прелазимо на рачунање вриједности.

$M = m_1 \cdot m_2 \cdot m_3 \cdot m_4 = 2 \cdot 3 \cdot 5 \cdot 7 = 210$

$M_1 = \frac{M}{m_1} = \frac{210}{2} = 105$

$$M_2 = \frac{M}{m_2} = \frac{210}{3} = 70$$
$$M_3 = \frac{M}{m_3} = \frac{210}{5} = 42$$
$$M_4 = \frac{M}{m_4} = \frac{210}{7} = 30$$

За коначно рјешење система конгруенције примјеном Кинеске теореме о остацима неопходно је да нађемо парцијалне конгруенције y_1, y_2, y_3, y_4.

$M_1 \cdot y_1 \equiv 1 \pmod{m_1}$, односно $105 \cdot y_1 \equiv 1 \pmod{2}$. Коефицијент уз y_1 можемо трансформисати по модулу 2, па имамо $1 \cdot y_1 \equiv 1 \pmod{6}$. Дакле, $y_1 = 1$.

$M_2 \cdot y_2 \equiv 1 \pmod{m_2}$, односно $70 \cdot y_2 \equiv 1 \pmod{3}$. Трансформисаћемо коефицијент уз y_2 по модулу 3, па имамо $1 \cdot y_2 \equiv 1 \pmod{5}$. Дакле, $y_2 = 1$.

$M_3 \cdot y_3 \equiv 1 \pmod{m_3}$, односно $42 \cdot y_3 \equiv 1 \pmod{5}$. Трансформацијом коефицијента уз y_3 по модулу 5 добијамо $2 \cdot y_3 \equiv 1 \pmod{5}$, па рјешења тражимо међу бројевима (0,1,2,3,4). Рјешење је 3. Дакле, $y_3 = 3$.

$M_4 \cdot y_4 \equiv 1 \pmod{m_4}$, односно $30 \cdot y_4 \equiv 1 \pmod{7}$. Трансформацијом коефицијента уз y_4 по модулу 7 добијамо $2 \cdot y_4 \equiv 1 \pmod{7}$, па рјешења тражимо међу бројевима (0,1,2,3,4,5,6). Рјешење је 4. Дакле, $y_3 = 4$.

Остаје да вриједности уврстимо у формулу. Добијамо

$$x \equiv 1 \cdot 105 \cdot 1 + 2 \cdot 70 \cdot 1 + 3 \cdot 42 \cdot 3 + 5 \cdot 30 \cdot 4 \pmod{210}$$
$$x \equiv 105 + 140 + 378 + 600 \pmod{210}$$

извршимо трансформацију бројева по модулу 210 (оних бројева који су већи од 210).

$$x \equiv 105 + 140 + 168 + 180 \pmod{210}$$
$$x \equiv 593 \pmod{210}$$

Такође трансформишемо 593 по модулу 210 и коначно добијамо

$x \equiv 173 \pmod{210}$. □

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`http://alas.matf.bg.ac.rs/~mm10030/tekst/Kineska%20teorema%20o%20ostacima.pdf`

253

Ријешити систем конгруенција:

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ x &\equiv 1 \pmod 7 \\ x &\equiv 6 \pmod 8 \end{aligned}$$

Доказ. Према Кинеској теореми о остацима рјешење добијамо по следећој формули:

$$x \equiv a_1 \cdot M_1 \cdot y_1 + a_2 \cdot M_2 \cdot y_2 + \ldots + a_n \cdot M_n \cdot y_n \pmod M$$

при чему је n број конгруенција (у овом случају $n = 3$).
Напоменимо,
$a_1, a_2 \ldots + a_n$ су десни коефицијенти конгруенције,
$m_1, m_2 \ldots + m_n$ су модули конгруенције,
$M = m_1 \cdot m_2 \cdot \ldots \cdot m_n$,

$M_1 = \dfrac{M}{m_1}$, $M_2 = \dfrac{M}{m_2}$, $\ldots$, $M_n = \dfrac{M}{m_n}$.

Сада прелазимо на рачунање вриједности.
$M = m_1 \cdot m_2 \cdot m_3 = 5 \cdot 7 \cdot 8 = 280$

$M_1 = \dfrac{M}{m_1} = \dfrac{280}{5} = 56$
$M_2 = \dfrac{M}{m_2} = \dfrac{280}{7} = 40$
$M_3 = \dfrac{M}{m_3} = \dfrac{280}{8} = 35$

За коначно рјешење система конгруенције примјеном Кинеске теореме о остацима неопходно је да нађемо парцијалне конгруенције y_1, y_2, y_3.

$M_1 \cdot y_1 \equiv 1 \pmod{m_1}$, односно $56 \cdot y_1 \equiv 1 \pmod 5$. Коефицијент уз y_1 можемо трансформисати по модулу 5, па имамо $1 \cdot y_1 \equiv 1 \pmod 5$. Видимо да је рјешење 1. Дакле, $y_1 = 1$.

$M_2 \cdot y_2 \equiv 1 \pmod{m_2}$, односно $40 \cdot y_2 \equiv 1 \pmod 7$. Трансформисаћемо коефицијент уз y_2 по модулу 7, па имамо $5 \cdot y_2 \equiv 1 \pmod 7$. Рјешења тражимо међу бројевима (0,1,2,3,4,5,6). Рјешење је 3. Дакле, $y_2 = 3$.

$M_3 \cdot y_3 \equiv 1 \pmod{m_3}$, односно $35 \cdot y_3 \equiv 1 \pmod 8$. Трансформацијом коефицијента уз y_3 по модулу 8 добијамо $3 \cdot y_3 \equiv 1 \pmod 8$, па рјешења тражимо међу бројевима (0,1,2,3,4,5,6,7). Рјешење је 3. Дакле, $y_3 = 3$.

Остаје да вриједности уврстимо у формулу. Добијамо

$x \equiv 3 \cdot 56 \cdot 1 + 1 \cdot 40 \cdot 3 + 6 \cdot 35 \cdot 3 \pmod{280}$
$x \equiv 168 + 120 + 630 \pmod{280}$

извршимо трансформацију бројева по модулу 280 (оних бројева који су већи од 280).

$x \equiv 168 + 120 + 70 \pmod{280}$
$x \equiv 358 \pmod{280}$

Такође трансформишемо 358 по модулу 280 и коначно добијамо

$x \equiv 78 \pmod{280}$. $\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`https://www.youtube.com/watch?v=zIFehsBHB8o&feature=youtu.be`

254

Да ли постоји природан број n такав да се $n!$ завршава са 11 нула?

Доказ. За $n \leqslant 49$ број $n!$ се завршава са мање од 11 нула.
Број 50! се завршава са 12 нула.
За $n \geqslant 50$ број се завршава са 12 или више нула.
Дакле, не постоји природан број n такав да се $n!$ завршава са 11 нула. $\square$

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
Теорија бројева - збирка задатака, Марија Станић, Небојша Икодиновић, 2004.

255

У скупу цијелих бројева ријешити једначину: $xy + 7x - 3y = 23$

Доказ. $xy + 7x - 3y = 23$
$x \cdot (y + 7) - 3y = 23$
$x \cdot (y + 7) = 3y + 23$

$$x = \frac{3y + 23}{y + 7}$$

$$x = \frac{3y + 21 + 2}{y + 7}$$

$$x = \frac{3 \cdot (y + 7) + 2}{y + 7}$$

$$x = \frac{3 \cdot (y + 7)}{y + 7} + \frac{2}{(y + 7)}$$

$$x = 3 + \frac{2}{(y+7)}$$

Да би x био цио број онда и $\frac{2}{(y+7)}$ мора бити цио број.

Рјешења тражимо у скупу бројева $\{\pm1; \pm2\}$, односно $y + 7 = \{\pm1; \pm2\}$.

$$\begin{array}{lll} y+7=-1 & y=-8 & x=1 \\ y+7=1 & y=-6 & x=5 \\ y+7=-2 & y=-9 & x=3 \\ y+7=2 & y=-5 & x=4 \end{array}$$

Ово су сва рјешења у скупу природних бројева. ☐

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
`http://www.naukamladima.com/index.php?page=diofantove-jednacine`

256

а) Од бројева 0,1,2,3,4,5,6,7,8,9 саставити три израза, тако да се искористе сви бројеви и да се ниједан од њих не понавља.

$$\square + \square = \square$$
$$\square + \square = \square$$
$$\square + \square = \square\square$$

б) Дјечак има 12 оловака: зелених исто колико и жутих, а црвених два пута више него плавих. Колико оловака сваке боје има дјечак?

Доказ. Један од аутора ове збирке наведени задатак сматра логичким и занимљивим за размишљање, тако да ће написати само рјешења, а читаоцима оставља доказе.

а) Једно рјешења је:

$$\boxed{2} + \boxed{7} = \boxed{9}$$
$$\boxed{3} + \boxed{5} = \boxed{8}$$
$$\boxed{4} + \boxed{6} = \boxed{10}$$

б) Зелених = жутих = 3, црвених = 4, плавих = 2. ☐

(**Мерван Дрпљанин 4/19 Ц**) задатак преузет са
мастер рад под називом "ЧЕТИРИ ЕТАПЕ РЕШАВАЊА ЗАДАТАКА ИЗ ЕЛЕМЕНТАРНЕ ТЕОРИЈЕ БРОЈЕВА", Тијана Спасић, Београд, 2017. година

257

Да ли постоји природан број који при дијељењу са 1001 даје остатак 23, а при дијељењу са 1170 остатак 42?

Доказ. Ако би постојао природан број n са овим својствима, онда би морало да важи:

$$n = 1001 \cdot x + 23$$
$$n = 1170 \cdot y + 42$$

Одузимањем ове двије неједначине добијамо:

$$1001x - 1170y = 19$$

Ако покажемо да дата Диофантова једначина има (нема) решење онда постоји (не постоји) природан број n са траженим својствима. Провјеравамо прво да ли нзд$(1001, 1170)$ дијели десну страну једначине.

Користећи Еуклидов алгоритам, имамо да је:

$$\begin{aligned} 1170 &= 1001 \cdot 1 + 169 \\ 1001 &= 169 \cdot 5 + 156 \\ 169 &= 156 \cdot 1 + \mathbf{13} \\ 156 &= 13 \cdot 12 \end{aligned}$$

$\Rightarrow$ нзд$(1001, 1170) = 13 \nmid 19$ па како није испуњен почетни услов то онда дата једначина нема решење. Самим тим не постоји природан број са датим својствима. ☐

(**Сандра Вујичић 2/19 Б**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

258

Ријешити систем конгруенција

$$\begin{cases} x \equiv 1 \pmod{3} \\ x \equiv 4 \pmod{5} \\ x \equiv 6 \pmod{7} \end{cases}$$

користећи Кинеску теорему о остацима.

Доказ. Пошто су нзд$(3, 5)$, нзд$(3, 7)$ и нзд$(5, 7)$ једнаки 1 можемо примјенити Кинеску теорему о остацима.Спровешћемо стандарни поступак. Наводимо вриједности стандарних промјенљивих

$$m_1 = 3 \quad m_2 = 5 \quad m_3 = 7 \implies m = 3 \cdot 5 \cdot 7 = 105$$
$$n_1 = \frac{m}{m_1} = 35 \quad n_2 = \frac{m}{m_2} = 21 \quad n_3 = \frac{m}{m_3} = 1$$

Сада формирамо нови систем

$$\begin{cases} n_1x \equiv 1 \pmod 3 \\ n_2x \equiv 4 \pmod 5 \\ n_3x \equiv 6 \pmod 7 \end{cases} \iff \begin{cases} 35x \equiv 1 \pmod 3 \\ 21x \equiv 4 \pmod 5 \\ 15x \equiv 6 \pmod 7 \end{cases} \iff \begin{cases} 2x \equiv 1 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$$

Потребно је пронаћи по једно рјешење за сваку од 3 конгруенције у посљедњем систему конгруенција . Лако уочавамо да су $x_1 = 2$, $x_2 = 4$, $x_3 = 6$ рјешења .

Сада формирамо рјешење почетног система конгруенција

$$x_0 = n_1x_1 + n_2x_2 + n_3x_3 = 2 \cdot 35 + 4 \cdot 21 + 6 \cdot 15 = 244$$

Тада сва рјешења почетног система конгруенција имају облик

$$x = x_0 + mt = 244 + 105t \ , \ t \in \mathbb{Z}$$

.

$\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`https://brilliant.org/wiki/chinese-remainder-theorem/`

259

Доказати да квадрат произвољног простог природног броја већег од 3 при дијељењу са 12 даје остатак 1.

Доказ. Нека је p произвољан прост број већи од 3. Тада се p може записати у облику $3k+1$ или $3k-1$, па је $p^2 \pmod 3 = 1$. Слично p може записати у облику $4k+1$ или $4k-1$, па је $p^2 \pmod 4 = 1$. Имамо да $3|(p^2-1)$ и $4|(p^2-1)$. Како су 3 и 4 узајамно прости то 12 дијели p^2-1. $\square$

(**Велибор Дошљак 15/19 Б**) задатак преузет из књиге
Збирка ријешених задатака из алгебре М. Анђић Р. Шћепановић

260

Из скупа $\{1, 2, 3, \dots, 2n\}$, $n \in \mathbb{N}$, произвољно је одабран $n+1$ број. Доказати да међу изабраним бројевима постоје таква два да је један дјељив другим .

Доказ. Нека су $a_1, a_2, \dots, a_n, a_{n+1}$ су произвољно изабрани бројеви из скупа $A = \{1, 2, \dots, 2n\}$. Као и сваки природан број и елементи скупа A се могу записати у облику 2^kq гдје је q непаран број.Како имамо n избора за q и $n+1$ елемент у скупу A , по Дирихлеовом принципу морају постојати индекси $i < j$ такви да a_i и a_j имају исти фактором q тј.

$$a_i = 2^{k_1}q \quad a_j = 2^{k_2}q \quad , k_1 < k_2$$

Тада $a_i \mid a_j$. Тиме смо доказали тврђење задатка . $\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`http://nasport.pmf.ni.ac.rs/materijali/175/Teorija_Brojeva_Vezbe.pdf`

261

Ријешити систем конгруенција
$x \equiv 3 \pmod{10}, \quad x \equiv 8 \pmod{15}, \quad x \equiv 5 \pmod{84}.$

Доказ. Уочавамо да бројеви 10, 15 и 84 нису у паровима релативно прости, па не можемо примијенити директно Кинеску теорему о остацима, а може се десити да такав систем уопште нема решења.
Систем је еквивалентан са:

$$x \equiv 3 \pmod 2, \quad x \equiv 3 \pmod 5, \quad x \equiv 8 \pmod 3, \quad x \equiv 8 \pmod 5,$$

$$x \equiv 5 \pmod 4, \quad x \equiv 5 \pmod 3, \quad x \equiv 5 \pmod 7.$$

Модули су нам степени простих бројева и сада упоредимо конгруенције које одговарају истом простом броју:

$$x \equiv 3 \pmod 2, \quad x \equiv 5 \pmod 4 \iff x \equiv 1 \pmod 4,$$

$$x \equiv 8 \pmod 3, \quad x \equiv 5 \pmod 3 \iff x \equiv 2 \pmod 3,$$

$$x \equiv 3 \pmod 5, \quad x \equiv 8 \pmod 5 \iff x \equiv 3 \pmod 5,$$

$$x \equiv 5 \pmod 7.$$

Према томе, наш систем је еквивалентан са системом:

$$x \equiv 1 \pmod 4, \quad x \equiv 2 \pmod 3, \quad x \equiv 3 \pmod 5, \quad x \equiv 5 \pmod 7$$

на који можемо примијенити Кинеску тепрему о остацима.
Имамо: $m = 4 \cdot 3 \cdot 5 \cdot 7 = 420$, $n_1 = 105$, $n_2 = 140$, $n_3 = 84, n_4 = 60$,

$$105x_1 \equiv 1 \pmod 4 \iff x_1 \equiv 1 \pmod 4 \implies x_1 = 1,$$

$$140x_2 \equiv 2 \pmod 3 \iff 2x_2 \equiv 2 \pmod 3 \implies x_2 = 1,$$

$$84x_3 \equiv 3 \pmod 5 \iff 4x_3 \equiv 3 \pmod 5 \implies x_3 = 2,$$

$$60x_4 \equiv 5 \pmod 7 \iff 4x_4 \equiv 5 \pmod 7 \implies x_4 = 3.$$

Решење је:

$$x \equiv 105 \cdot 1 + 140 \cdot 1 + 84 \cdot 2 + 60 \cdot 3 = 593 \equiv 173 \pmod{420}.$$

□

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

262

Доказати да се сваки цијели број може записати у облику $a^2+b^2-c^2$, за неке цијеле бројеве a, b і c.

Доказ. Разматрамо случајеве:
I Нека је n непаран број. Тада је:

$$n = 2k+1 = (k+1)^2 - k^2, \text{ за neki цијели број } k.$$

тако да узимајући да је $a = k+1$, $b = 0$, $c = k$ показали смо за случај непарног броја.

II Нека је n паран број. Тада опет разликујемо 2 случаја:
(1) $n = 2^{2k}(2l+1)$
(2) $n = 2^{2k+1}(2l+1)$, $k > 0$, l-цијели број.
У случају (1) је:

$$n = 2^{2k}(2l+1) = 2^{2k}((l+1)^2 - l^2) = \left(2^k(l+1)\right)^2 - (2^k l)^2$$

тако да узимајући $a = 2^k(l+1)$, $b = 0$, $c = 2^k l$ показали смо и овај случај.
У случају (2) је:

$$n = 2^{2k+1}(2l+1) = 2^{2k}\cdot 2\cdot(2l+1) = 2^{2k}(4l+2) = 2^{2k}(4l+1+1) = \\ 2^{2k}((2l+1)^2+1-(2l)^2) = (2^k(2l+1))^2 + 2^{2k} - (2^{k+1}l)^2)$$

тако да узимајући да је $a = 2^k(2l+1)$, $b = 2^k$, $c = 2^{k+1}l$ доказали смо да за сваки цијели број постоји тражени запис.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

263

Одредити све природне бројеве n за које је $\phi(n)$ непаран број.

Доказ. Знамо да је $\phi(n) = n\cdot\prod_{i=1}^{k}(1-\dfrac{1}{p_i})$ при чему је $\phi(1)=1$.

Примијетимо да је и $\phi(2) = 2\cdot(\frac{1}{2}) = 1$, па посматрајмо $n > 2$.
Ако у неком од чинилаца у горњем запису Ојлерове функције $\phi(n)$ постоји непаран фактор p_i, онда је $p_i - 1$ паран број, па ћемо у једном чиниоцу имати $\frac{p_i-1}{p_i}$ што значи да ће и $\phi(n)$ бити паран број.
Ако, са друге стране, не постоји непаран фактор p_i, онда је $n = 2^\alpha$ за неко $\alpha \geq 2$. Тада је $\phi(n) = 2^\alpha\cdot\frac{1}{2} = 2^{\alpha-1}$, па како је $\alpha - 1 \geq 1$, и у овом случају $\phi(n)$ биће паран број.
Закључујемо да је $\phi(n)$ непарно само за $n \in (1,2)$.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`http://e.math.hr`

264

Нека је n природан број. Ако $d \mid n$ онда $\phi(d) \mid \phi(n)$.

Доказ. Нека је $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_n^{\alpha_k}$ факторизација броја n. Пошто $d \mid n$, онда је $d = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_n^{\beta_k}$ гдје је $0 \leq \beta_i \leq \alpha_i, i = 1, ..., k$. Ово је јасно јер је $n = d \cdot s$ за неки природан број s, па се у факторизацији броја d налазе неки фактори који постоје и у факторизацији броја n.

Тада је, користећи мултипликативност Ојлерове функције:

$$\frac{\phi(n)}{\phi(d)} = \prod_{i=1}^{k} \frac{\phi(p_i^{\alpha_i})}{\phi(p_i^{\beta_i})} = \prod_{i=1}^{k} \frac{p_i^{\alpha_i - 1}}{p_i^{\beta_i - 1}} = \prod_{i=1}^{k} p_i^{\alpha_i - \beta_i}$$

па како је $\beta_i \leq \alpha_i$, онда је израз са десне стране природан број. Дакле, $\phi(d) \mid \phi(n)$.

Напомена: У доказу користили смо да за прост број p важи $\phi(p^k) = p^{k-1} \cdot (p-1)$, а то смо доказали на часу.

$\square$

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`http://e.math.hr`

265

Доказати да не постоји природан број такав да је $\phi(n) = 14$.

Доказ. Нека је $n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$. Претпоставимо да је $\phi(n) = 14$. На основу познате формуле за $\phi(n)$ добијамо

$$\phi(n) = \prod_{i=1}^{r} (p_i^{a_i} - p_i^{a_k - 1}) = \prod_{i=1}^{r} p_i^{a_i - 1}(p_i - 1)$$

Како $7 \mid \phi(n) = 14$ онда $7 \mid p_i$ или $7 \mid (p_i - 1)$ за неко $i = 1, 2, \ldots, r$. Ако $7 \mid p_i$ онда је $p_i = 7$, па даље $6 = p_i - 1 \mid \phi(n)$. Међутим $6 \nmid 14$, па је тај случај немогућ.

Преостаје да $7 \mid (p_i - 1)$ тј. $p_i = 7k + 1$. Тада $7k \mid \phi(n) = 14$ што намеће услов $k \leq 2$.Међутим за $k = 1$ $p_i = 7 \cdot 1 + 1 = 8$ и $k = 2$ $p_i = 7 \cdot 2 + 1 = 15$ смо добили бројеве који нијесу прости , па ни ова ситуација није могућа .

Дакле , не постоји природан број n такав да је $\phi(n) = 14$. $\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`http://www.cs.uleth.ca/~yazdani/courses/2011-2012/math3461/HW8-soln.pdf`

266

Наћи све природне бројеве за које важи да $\phi(n) \mid n$.

Доказ. Претпоставимо да је n природан број за који важи $\phi(n) \mid n$. Прво ћемо доказати да онда постоји највише један непаран прост фактор броја n .

Нека је $n = 2^s p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$, гдје су $p_1, p_2, \ldots, p_k$ различити непарни прости бројеви . Тада је $\phi(n) = 2^{s-1} \prod_{i=1}^{k} p_i^{a_i - 1}(p_i - 1)$. Примјетимо да је $p_i - 1$ парно , па је $p_i - 1 = 2m_i$ за $m_i \in \mathbb{N}$, $i = 1, \ldots, k$. Кад уврстимо добијамо

$$\phi(n) = 2^{s-1+k} \prod_{i=1}^{k} p_i^{a_i - 1} m_i$$

одакле добијамо да $2^{s-1+k} \mid \phi(n) \implies 2^{s-1+k} \mid n$. Познато је да $2^{s+1} \nmid n$, па онда вриједи да је $k \leq 1$. Тиме смо доказали да је неопходно да n има тачно 0 или 1 непаран прост фактор.

Дакле треба размотримити 4 случаја : $n = 1$, $n = 2^a$, $n = p^b$ и $n = 2^a p^b$.
Ако је $n = 1$ онда је $\phi(n) = 1$, па $\phi(n) \mid n$. Када је $n = 2^a$ онда је $\phi(n) = 2^a - 2^{a-1} = 2^{a-1}$, па $\phi(n) \mid n$. У случају $n = p^b$, $\phi(n) = p^b - p^{b-1} = p^{b-1}(p-1)$ што је паран број јер је $(p-1)$ паран . Тада $\phi(n) \nmid n$ јер $n = p^b$ непаран .

Преостао је случај $n = 2^a p^b$. Ако $\phi(n) \mid n$ онда

$$(p-1)2^{a-1}p^{b-1} \mid 2^a p^b$$

одакле слиједи да $(p-1) \mid 2p$. Како је нзд$(p, p-1) = 1$ јер су узастпони , онда мора важити да $p - 1 \mid 2 \implies p - 1 = 1$ или $p - 1 = 2$. Међутим , како је p прост број узимамо $p - 1 = 2$ тј. $p = 3$. Дакле , непоходан услов је да $n = 2^a 3^b$, $a, b > 0$. Примјетимо да је то и довољан услов .

Дакле , $\phi(n) \mid n$ када је $n = 1, 2^a$ или $2^a 3^b$. ☐

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`http://www.cs.uleth.ca/~yazdani/courses/2011-2012/math3461/HW8-soln.pdf`

267

Наћи све природне бројеве за које важи да $\phi(n) = \dfrac{n}{2}$.

Доказ. Претпоставимо је n природан број такав да је $\phi(n) = \dfrac{n}{2}$. Пошто је $\phi(n) = \dfrac{n}{2}$ онда је n паран број тј $n = 2m$, $m \in \mathbb{N}$.

Ојлерова функција се дефинише као кардиналност скупа

$$A = \{k \mid 1 \leq k \leq n-1 \text{ , нзд}(k, n) = 1\} \subseteq \{1, 2, \ldots, n-1\}$$

Бројеви $2, 4, \ldots, 2m - 2 \notin A$ и одатле слиједи $|A| \leq (2m-1) - (m-1) = m$. Ако би p био непаран прост фактор за n , онда $p \notin A$ што би повлачило да $|A| \leq m - 1 < m = \dfrac{n}{2}$.

Дакле , неопходно је да n буде облика 2^a , $a \geq 0$. За $n = 1$ тврђење очигледно не важи. Ако је $n = 2^a$, $a > 0$ онда је $\phi(n) = 2^{a-1} = \frac{n}{2}$.

Дакле , тражени бројеви имају облик 2^a , $a > 0$. $\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`http://nasport.pmf.ni.ac.rs/materijali/175/Teorija_Brojeva_Vezbe.pdf`

268

Доказати да међу 5 узастопних природних бројева постоји један који је узајамно прост са осталима .

Доказ. Посматрајмо пет узастопних природних бројева $(n-2), (n-1), n, (n+1), (n+2)$ гдје је $n \geq 3$. Број n може бити паран или непаран .

Ако је n паран онда су $n-1$ и $n+1$ непарни и бар један од њих није дјелив са 3 . Без губљења општости претпоставимо да $3 \nmid n-1$.Примјетимо

$$\begin{aligned}
&\text{нзд}(n-1, n-2) = 1 && (\text{ na osnovu zadatka 6(a) })\\
&\text{нзд}(n-1, n) = 1 && (\text{ na osnovu zadatka 6(a) })\\
&\text{нзд}(n-1, n+1) = 1 && (\text{ na osnovu zadatka 6(b) })\\
&\text{нзд}(n-1, n+2) = 1 && (\text{ na osnovu zadatka 6(d) })
\end{aligned}$$

слиједи да је $n-1$ узајмно прост са преостала четири броја .

Нека је сада n непаран . Примјетимо опет

$$\begin{aligned}
&\text{нзд}(n, n-2) = 1 && (\text{ na osnovu zadatka 6(b) })\\
&\text{нзд}(n, n-1) = 1 && (\text{ na osnovu zadatka 6(a) })\\
&\text{нзд}(n, n+1) = 1 && (\text{ na osnovu zadatka 6(a) })\\
&\text{нзд}(n, n+2) = 1 && (\text{ na osnovu zadatka 6(b) })
\end{aligned}$$

одакле слиједи да је n узајамно прост са преостала четири броја . Тиме смо доказали тврђење задатка .

$\square$

(**Велимир Ђоровић 5/19 Б**) задатак преузет са
`https://books.google.me/books?id=QGgLbf2oFUYC&pg=PA77#v=onepage&q&f=false`

269

Одредити највећи природан број n који се не може записати као збир три броја већа од 1 који су у паровима релативно прости.

Доказ. То је број 17. Докажимо да 17 не можемо написати као збир 3 броја која су у паровима релативно прости. Претпоставимо супротно. Тада та три броја морају бити непарни и међу њима се мора налазити број 3 јер би иначе најмањи могући збир био $5+7+9 = 21 > 17$. Због тога међу њима не смије бити број 9. Најмањи могући збир је $3 + 5 + 7 = 15 < 17$, а следећи најмањи је $3 + 5 + 11 = 19 > 17$. Дакле, немогуће је број 17 написати у траженом облику.

Докажимо сада да је сваки број већи од 17 могуће написати у датом облику. Докажимо прво за парне бројеве, и посматрајмо случајеве по модулу 6. Вриједи

$$6k + 4 = (6k - 1) + 2 + 3$$

$$6k + 2 = (6k - 5) + 3 + 4$$

$$6k = (6k - 5) + 2 + 3$$

За сваки од бројева лако се показује да су у паровима релативно прости. Докажимо даље тврдњу и за непарне бројеве. Ту ћемо раздвојити случајеве по модулу 12. Наиме,

$$12k + 3 = (6k + 1) + (6k - 1) + 3$$

$$12k + 9 = (6k + 1) + (6k - 1) + 9$$

$$12k + 7 = (6k - 1) + (6k + 5) + 3$$

$$12k + 1 = (6k - 7) + (6k - 1) + 9$$

$$12k + 5 = (6k - 5) + (6k + 1) + 9$$

$$12k + 11 = (6k + 1) + (6k + 7) + 3$$

И у овом случају тривијално се провјерава да су у свим случајевима бројеви у паровима релативно прости.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

270

Наћи све $x, y \in \mathbb{N}$ за које $x + 2y + \frac{3x}{y} = 2012$.

Доказ. Пошто су x и y цијели бројеви, видимо да ће $3x$ морати да буде дјељиво са y. Нека је $3x = ky$. Ако читаву јдначину помножимо са 3 имаћемо

$$3x + 6y + 3\frac{3x}{y} = 6036$$

$$ky + 6y + 3k = 6036$$

$$(y + 3)(x + 6) - 18 = 6036$$

$$(y + 3)(x + 6) = 6054$$

6054 се може записати као производ два броја у облику. $1 \cdot 6054$, $2 \cdot 3027$, $3 \cdot 2018$, $6 \cdot 1009$, $6054 \cdot 1$, $3027 \cdot 2$, $2018 \cdot 3$, $1009 \cdot 6$. Замјеном добијамо да су могућа рјешења $x = 1003, y = 3; x = 0, y = 1006; x = -2015, y = 2015; x = -4023, y = 3024; x = -10085, y = 6051$ □

(**Велибор Дошљак 15/19 Б**) задатак преузет са
`http://refkol.ro/matek/mathbooks/Olympiad%20Stuff/1220NT.pdf`

271

●●●●

Које су године рођене особе које су 1958. године напуниле онолико година колико је збир цифара године њиховог рођења?

Доказ. Претпоставимо да су те особе рођене $19xy$ године, гдје су $x, y \in \{0, 1, \ldots, 9\}$. Према условима задатка мора бити:

$$\begin{gathered}1958 - (1000 + 900 + 10x + y) = 1 + 9 + x + y \\ 11x + 2y = 48\end{gathered}$$

Рјешавамо дату Диофантову једначину.
Како нзд$(11, 2) = 1 \mid 48$, једначина има решење. Користећи Бланкиншип методу добијамо $x = 1$, $y = -5$, па ће једно партикуларно решење бити: $x^* = 48$, $y^* = -240$, а опште:

$$x = 48 + 2t$$

$$y = -240 - 11t, \quad t \in Z$$

Како су $x, y \in \{0, \ldots, 9\}$

$$0 \leq 48 + 2t \leq 9 \Leftrightarrow -24 \leq t \leq -\frac{39}{2}$$

$$0 \leq -240 - 11t \leq 9 \Leftrightarrow -\frac{249}{11} \leq t \leq -\frac{240}{11}$$

Једино t које ово задовољава је $t = -22$, па је $x = 4$ и $y = 2$ односно то су особе рођене 1942. године. Ако би биле рођене $18xy$, имали би једначину:

$$11x + 2y = 149, \quad x, y \in \{0, 1, \ldots, 9\}$$

Максимална вриједност израза била би за $x = y = 9$, а то је $117 < 149$, па закључујемо да је немогуће да особа буде рођена у 19. вијеку.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://mnm.hr/wp-content/uploads/2015/10/kongruencije.pdf`

272

●●●●

Када је број 4444^{4444} написан у бази 10 , збир његових цифара је A . Нека је B збир цифара броја A . Наћи збир цифара броја B .

Доказ. Примјетимо да је

$$4444^{4444} < 10000^{4444} = (10^4)^{4444} = 10^{17776}$$

Одатле закључујемо да 4444^{4444} има мање од 17776 цифара , $A < 9 \cdot 17775 = 159975$. Сума цифара броја A се максимизује кад је $A = 99999$ (A може имати и 6 цифара , али онда је сума прве двије цифре највише $1 + 5 = 6$) , па је $B \leq 45$. Примјетимо да је онда сума цифара броја B мања од или једнака 12 (максимална за 39).

Познато је да сваки број у бази 10 конгруентан збиру својих цифара по модулу 9 (види напомену) . На основу тога важи

$$4444^{4444} \equiv A \equiv B \equiv X \pmod 9$$

гдје је X збир цифара броја B . За X нам је познато да је

$$1 \leq X \leq 12 \quad \text{i} \quad 4444^{4444} \equiv X \pmod 9$$

Да бисмо нашли X покушајмо да уочимо неке обрасце за степене броја 4444 по модулу 9 . Примјетимо да

$$4444^1 \equiv 7 \pmod 9 \text{ ,} \quad 4444^2 \equiv 4 \pmod 9 \text{ ,} \quad 4444^3 \equiv 1 \pmod 9$$

и пошто је $4444 = 3 \cdot 1481 + 1$ онда

$$4444^{4444} \equiv 4444^{3 \cdot 1481 + 1} \equiv (4444^3)^{1481} \cdot 4444 \equiv 1^{1481} \cdot 4444 \equiv 7 \pmod 9$$

Дакле , $X = 7$ тј. збир цифара броја B је 7 .
Напомена Број $n = a_k \dots a_1 a_0$ је конгруентан збиру својих цифара по модулу 9 јер је

$$n \equiv a_k \cdot 10^k + \dots a_1 \cdot 10 + a_0 \equiv a_k \cdot 1^k + \dots a_1 \cdot 1 + a_0 \equiv a_k + \dots a_1 + a_0 \pmod{10}.$$

□

(**Велимир Ђоровић 5/19 Б**) задатак са ИМО 1975 (проблем 4)
`https://www.imo-official.org/problems.aspx`

273
● ● ● ●

Нека је $a_1, a_2, \dots$ низ цијелих бројева који садржи бесконачно много позитивних и бесконачно много негативних чланова. Ако сваки скуп $a_1, a_2, \dots a_n$ садржи n различитих остатака по $\pmod n$, доказати да се сваки цио број појављује тачно једном у низу a_n.

Доказ. Пошто имамо да за свако n, $a_1, a_2, \dots a_n$ дају различите остатке при дијељењу са n, то се сваки цио број појављује највише једном.
Докажимо да за свако n, $|a_n - a_i| \leq n - 1$ за $i < n$. Претпоставимо супротно $d = |a_n - a_i| > n$, тада у скупу $a_1, a_2, \dots, a_d$ постоје два броја која дају исти остатак при дијељењу са d. Што је немогуће, па закључујемо да $|a_n - a_i| <= n - 1$.
Докажимо да се сваки скуп $\{a_1, a_2, \dots, a_n\}$ састоји од n узастопних бројева. Доказ спроводимо математичком индукцијом.

За $n = 1$ тврђење очигледно важи.
Нека тврђење важи за $n = k$.

Претпоставимо да $\{a_1, a_2, \ldots, a_{k+1}\}$ није скуп узастопних цијелих бројева. Нека је $m = min\{a_1, a_2, ...a_k\}$ и $M = min\{a_1, a_2, \ldots, a_k\}$. Како за k тврђењеважи, то је једина могућност да тврђење не важи за $k+1$ да $a_{k+1} > M+1$, или $a_{k+1} < m-1$. Ако је $a_{k+1} > M+1$, тада је $|a_{k+1} - m| = |a_{k+1} - M + M - m| \geq |M - a_{k+1}| + |M - m| > k+1$ што је немогуће.
Долазимо до закључка да је $\{a_1, a_2, \ldots, a_n\}$ скуп узастопних цијелих бројева.
Како имамо бесконачно позитивних и бесконачно негативних цијелих бројева, не може да се деси да се неки број k не појављује у низу a_n. Иначе ако би било $k > a_1$ ни један број већи од к не би могао да се јави у низу, па би имали коначно позитивних елемената. Слично ако је $k < a_1$ ни један број мањи од к не би могао да се јави у низу. Закључујемо да се сваки цијели број јавља тачно једном у низу a_n. ☐

(**Велибор Дошљак 15/19 Б**) задатак са IMO Shortlist 2005

274

●●●●

Доказати да важи $\varphi(\varphi(m)) \leq \frac{m}{2}$, гдје је φ Ојлерова функција.

Доказ. Нека је n произвољан број који није степен 2. Нека се n разлаже на просте факторе у облику $n = {p_1}^{e_1} \cdot {p_2}^{e_2} \ldots {p_k}^{e_k}$. Тада имамо

$$\varphi(\varphi(n)) = \varphi(\varphi({p_1}^{e_1})\varphi({p_2}^{e_2}) \ldots \varphi({p_k}^{e_k}))$$

Како n није степен двојке то постоји неки p_i који је прост број већи од 2, па је $\varphi({p_i}^{e_i}) = (p_i - 1){p_i}^{e_i - 1}$. Закључујемо да је $\varphi({p_1}^{e_1})\varphi({p_2}^{e_2}) \ldots \varphi({p_k}^{e_k})$ паран број.
Нека је

$$\varphi({p_1}^{e_1})\varphi({p_2}^{e_2}) \ldots \varphi({p_k}^{e_k}) = 2^{l_1}{q_2}^{l_2} \ldots {q_r}^{l_r}$$

Па је

$$\varphi(\varphi(n)) = \varphi(2^{l_1}{q_2}^{l_2} \ldots {q_r}^{l_r})$$

$$= (2-1)2^{l_1-1} \cdot \varphi(2^{l_1})\varphi({q_2}^{l_2}) \ldots \varphi({q_r}^{l_r}) = 2^{l_1-1} \cdot \varphi(2^{l_1})\varphi({q_2}^{l_2}) \ldots \varphi({q_r}^{l_r})$$

Како је $\varphi(a) < a$ имамо да је

$$\varphi(\varphi(n)) = 2^{l_1-1} \cdot \varphi({q_2}^{l_2}) \ldots \varphi({q_r}^{l_r}) \leq \frac{1}{2} \cdot 2^{l_1}{q_2}^{l_2} \ldots {q_r}^{l_r} = \frac{1}{2} \cdot \varphi({p_1}^{e_1})\varphi({p_2}^{e_2}) \ldots \varphi({p_k}^{e_k}) \leq$$

$$\frac{1}{2}{p_1}^{e_1} \cdot {p_2}^{e_2} \ldots {p_k}^{e_k} = \frac{1}{2}n$$

Ако је n степен двојке имамо

$$\varphi(\varphi(2^k)) = 2^{k-1}(2-1) = 2^{k-1}$$

Закључујемо да тврђење важи за свеако $m > 1$. ☐

(**Велибор Дошљак 15/19 Б**) задатак инспирисан рјешењем проблема
`https://codeforces.com/problemset/problem/906D`

275

Доказати да је за сваки природан број n бар један од бројева $3^{3n}+2^{3n}$ и $3^{3n}-2^{3n}$ дјељив са 35.

Доказ. Ако је n непаран

$$3^{3n}+2^{3n}=(3^3+2^3)(3^{3n-1}-\ldots+2^{3n-1})=35\cdot M$$

Ако је n паран, тада је $n=2k$

$$3^{3n}-2^{3n}=3^{6k}-2^{6k}=665(3^{3n-1}+\ldots+2^{3n-1})$$

□

(**Велибор Дошљак 15/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

276

Да ли једначина $x^3+y^3+z^3=2003$ има цјелобројна рјешења.

Доказ. Остаци при са дијељењу са 9 могу бити

$$a:\ 0\ 1\ 2\ 3\ 4\ 5\ 6\ 7\ 8$$

$$a^2:\ 0\ 1\ 4\ 0\ 7\ 7\ 0\ 4\ 1$$

$$a^3:\ 0\ 1\ 8\ 0\ 1\ 8\ 0\ 1\ 8$$

Видимо да су могућности за суму 3 куба по модулу 9 $\{0,\ 1,\ 2,\ 3,\ 8,\ 7,\ 6\}$. Па је немогуће да се 2003 представи као сума 3 куба, јер је $2003 \pmod 9 = 5$. □

(**Велибор Дошљак 15/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

277

Нека је $p\geq 7$ прост број. Доказати да $p\mid a$, гдје је

$$a=\underbrace{11\ldots1}_{\text{p-1}}$$

Доказ. Посматрајмо

$$9a=9\frac{10^{p-1}-1}{9}=10^{p-1}-1$$

Како су 10 и p узајамно прости, можемо да примијенимо Малу Фермаову лему.

$$9a \pmod p = 0$$

Одакле закључујемо да је $9a$ дјељив са p. Како $p \nmid 9$ и p прост број, закључујемо да $p \mid a$. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из
104 Number Theory Problems From the Training of the USA IMO Team

278

Нека је p прост број. Доказати да p дијели $ab^p - ba^p$ за свако $a, b \in \mathbb{N}$.

Доказ.

$$ab^p - ba^p = ab(b^{p-1} - a^{p-1})$$

Ако $p \mid ab$ доказ је завршен.

Ако $p \nmid ab$, тада $NZD(p,a) = 1$ и $NZD(p,b) = 1$. Примјеном Мале Фермаове теореме имамо

$$b^{p-1} - a^{p-1} \equiv 1 - 1 = 0 \pmod p$$

Закључујемо да тврђење важи. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из
104 Number Theory Problems From the Training of the USA IMO Team

279

Нека је $n > 1$ природан број. Наћи суму природних бројева мањих од n који су узајамно прости са n.

Доказ. Нека је нзс$(a, n) = 1$ тада је и нзс$(n - a, n) = 1$ Број бројева узајамно простих са $n = \varphi(n)$.
Нека n није степен двојке. Тада је $n = p^k \cdot M$, гдје је p непаран прост број. Па је $\varphi(n) = \varphi(p^k) \cdot \varphi(M) = p^{k-1}(p-1)\varphi(M)$ Па је $\varphi(n)$ паран број.
Ако је n степен двојке већи од 2. Тада је $\varphi(2^k) = (2-1)2^{k-1}$, па је $\varphi(n)$ паран број.
Имамо да је $\varphi(n)$ паран број. Нека су $d_1, \ldots d_\varphi(n)$ бројеви чију суму тражимо поређани рестуће. Тада ће сваки од њих имати одговарајући пар.

$$d_1 + d_\varphi(n) = n$$

$$d_2 + d_{\varphi(n)-1} = n$$

$$\ldots$$

Тада је сума $\sum_{i=1}^{\varphi(n)} d_i = n \cdot \frac{\varphi(n)}{2}$ За $n = 2$ провјером утврђујемо да важи иста једнакост. ☐

(**Велибор Дошљак 15/19 Б**) задатак преузет из
104 Number Theory Problems From the Training of the USA IMO Team

280

Доказати да не постоје природни бројеви $a,\ b,\ c,\ d$ такви да је $a^a+b^b+c^c=d^d$.

Доказ. Нека је без губљења општости $a \leq b \leq c < d$
За $c \geq 3$:

$$d^d = a^a + b^b + c^c \leq 3c^c \leq c^{c+1} < (c+1)^{c+1}$$

Закључујемо да је $d < c+1$, што је немогуће.
За $c = 2, a = b = 1$:

$$1 + 1 + 4 = 6 \neq d^d$$

За $c = 2, a = b = 2$:

$$4 + 4 + 4 = 12 \neq d^d$$

За $c = 2, a = 1b = 2$:

$$4 + 1 + 4 = 9 \neq d^d$$

Не постоје природни бројеви $a,\ b,\ c$ и d тако да важи $a^a + b^b + c^c = d^d$.

☐

(**Велибор Дошљак 15/19 Б**)

281

Наћи све непарне природне бројеве n за које је $n = 2019 \cdot \underbrace{\phi(\phi(...\phi(n)...))}_{10 \text{ пута}}$ гдје је ϕ Ојлерова функција.

Доказ. У доказу користићемо да ако $a \mid b$ тада и $\phi(a) \mid \phi(b)$ (задатак доказан у овом поглављу). Најприје уведимо ознаке:

$$\phi^k(n) = \phi(\phi^{k-1}(n)), \ \ \phi^1(n) = \phi(n).$$

Како је $2019 = 3 \cdot 673$, n се може представити као:

$$n = 3^\alpha \cdot 673^\beta \cdot k, \ \ \text{нзд}(2019, k) = 1$$

Такође, k не може бити паран јер је n непаран, па је нзд$(4038, k) = 1$.
Докажимо да је $k = 1$.
На неком од претходних задатака показали смо да је само за $k = 1, 2$ $\phi(k)$ непаран број, па за $k \neq 1$ $\phi(k)$ је паран. Да покажемо да је $k = 1$, претпоставимо супротно. Тада $2 \mid \phi(k)$.

$$\phi(n) = 3^{\alpha-1} \cdot 2 \cdot 673^{\beta-1} \cdot 672 \cdot \phi(k) = 2^6 \cdot 3^\alpha \cdot 673^{\beta-1} \cdot 7 \cdot \phi(k).$$

Одавде како је $\phi(k) = 2m$ за неки природан број m, имамо:

$$2^7 \cdot 3^\alpha \cdot 7 \mid \phi(n)$$

$$\Rightarrow 2^8 \cdot 3^\alpha \mid \phi(\phi(n)) = \phi^2(n)$$
$$\Rightarrow 2^8 \cdot 3^{\alpha-1} \mid \phi^3(n)$$
$$\Rightarrow 2 \mid \phi^{10}(n)$$

а то је контрадикција. Дакле,

$$n = 3^\alpha \cdot 673^\beta$$

Докажимо сада да је $\alpha = \beta = 1$. Претпоставимо супротно тј.да је бар један од бројева $\alpha, \beta > 1$, и нека је без смањења општости $\alpha \geq 2$.
Као и у првом дијелу,

$$\phi(n) = 2^6 \cdot 3^\alpha \cdot 673^{\beta-1} \cdot 7$$

па редом:

$$2^6 \cdot 3^\alpha \cdot 7 \mid \phi(n)$$
$$\Rightarrow 2^7 \cdot 3^\alpha \mid \phi^2(n)$$
$$\Rightarrow 2^7 \cdot 3^{\alpha-1} \mid \phi^3(n)$$
$$\Rightarrow 2^7 \mid \phi^4(n)$$
$$\Rightarrow 2 \mid \phi^{10}(n)$$

што поново доводи до контрадикције. Дакле, једино решење је $n = 3 \cdot 673 = 2019$. ☐

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

282

Одредити све природне бројеве n за које важи $\varphi(n) = 12$.

Доказ. Ако је $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ онда је

$$\varphi(n) = p_1^{\alpha_1 - 1}(p_1 - 1) \dots p_r^{\alpha_r - 1}(p_r - 1).$$

Из $(p_i - 1) \mid 12$ слиједи $p_i \in \{2, 3, 5, 7, 13\}$. Ако је $p_i = 2$, онда је $\alpha_i \leq 3$; ако је $p_i = 3$, онда је $\alpha_i \leq 2$; а ако је $p_i \neq 2, 3$, онда је $\alpha_i = 1$. Имамо четири могућности (са k означавамо број облика $2^\alpha 3^\beta$) :

- $n = 13 \cdot k \Longrightarrow \varphi(n) = 12 \cdot \varphi(k) = 12$
  $\varphi(k) = 1 \Longrightarrow k = 1$ или $k = 2 \Longrightarrow n = 13$ или $n = 26$
- $n = 7 \cdot k \Longrightarrow \varphi(n) = 6 \cdot \varphi(k) = 12$
  $\varphi(k) = 2 \Longrightarrow k = 3,\ k = 4$ или $k = 6 \Longrightarrow n = 21,\ n = 28$ или $n = 42$
- $n = 5 \cdot k \Longrightarrow \varphi(n) = 4 \cdot \varphi(k) = 12$
  $\varphi(k) = 3$, што нема решења.
- $n = k \Longrightarrow \varphi(n) = 2^{\alpha-1}3^{\beta-1} \cdot 2 = 12$
  $\alpha = 2,\ \beta = 2 \Longrightarrow n = 36.$

Решења су: $n = 13, 21, 26, 28, 36, 42$. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf`

283

Одредити све троцифрене бројеве који при дијељењу са 11 дају остатак једнак збиру квадрата својих цифара.

Доказ. Нека је тражени троцифрени број $\overline{abc}$. Како је

$$\overline{abc} = 100a + 10b + c = 11(9a + b) + a - b + c,$$

то је остатак при дијељењу траженог броја са 11 једнак $a - b + c$.
Према условима задатка је

$$a - b + c = a^2 + b^2 + c^2, \text{ тј. } a^2 + b^2 + c^2 - a + b - c = 0.$$

Множењем добијене једнакости са 2 добија се

$$2a^2 + 2b^2 + 2c^2 - 2a + 2b - 2c = 0$$

или

$$a^2 + b^2 + c^2 + (a - 1)^2 + (b + 1)^2 + (c - 1)^2 = 3.$$

Јасно је да једначина има рјешење ако су три од датих сабирака једнаки нули, а преостала три једнака јединици. Како је $\overline{abc}$ троцифрен број, слиједи да је $a \geq 1$, па је $a = 1$.
Слично је $b \geq 0$, па је $b + 1 \geq 1$ и због тога је $b = 0$ и $b + 1 = 1$. На основу тога је

$$a^2 + b^2 + c^2 + (a - 1)^2 + (b + 1)^2 + (c - 1)^2 = 1 + 0 + c^2 + 0 + 1 + (c - 1)^2 = 3,$$

па се разликују два случаја:

- $c = 0$ и $(c - 1)^2 = 1$.
- $c = 1$ и $(c - 1)^2 = 0$.

Тражени бројеви су очигледно 100 и 101. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/ZBIRKA.pdf`

284

Одредити све двоцифрене природне бројеве који су једнаки квадрату збира својих цифара.

Доказ. Нека је тражени број $\overline{xy} = 10x+y$. Из услова задатка се добија да је $10x+y = (x+y)^2$ или $9x + (x + y) = (x + y)^2$. Како је $x \neq 0$, то је и $(x + y) \neq 0$ па се дијељењем добијене једнакости са $(x + y)$ добија једнакост:

$$\frac{9x}{x+y} + 1 = x + y.$$

Ако је највећи заједнички дјелилац са x и y једнак d, онда постоје узајамно прости бројеви a и b такви да је $1 \leq x = ad \leq 9$ и $0 \leq y = bd \leq 9$. Тада једначина постаје

$$\frac{9ad}{(a+b)d} + 1 = (a + b)d$$

или

$$\frac{9a}{a+b} + 1 = (a + b)d.$$

Како количник $\frac{9a}{a+b}$ мора бити природан број и како су a и $(a + b)$ узајамно прости, то су могућа три случаја:

- Ако је $a + b = 1$, онда је $9a + 1 = d$. Овај случај је немогућ, јер из $a + b = 1$ слиједи, због $x \neq 0$, да је $a = 1$, $b = 0$. У том случају је $d = 10$, што је немогуће јер је $d \leq 9$.
- Ако је $a + b = 3$, онда је $3a + 1 = 3d$. И овај случај је немогућ, јер добијена једначина нема цјелобројних решења.
- Ако је $a + b = 9$, онда је $a + 1 = 9d$ или $a = 9d - 1$. Како је $1 \leq x \leq 9$, то је $1 \leq x = ad = (9d - 1)d \leq 9$, па је $d = 1$. То значи да је $a = 8$ и $b = 1$.

Дакле тражени број је $81 (= (8 + 1)^2)$. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/ZBIRKA.pdf`

285
●●●●

Одредити све цијеле бројеве и тако да задовољавају једначину:
$x^4 + y^4 = 6x^2 + 14y^2 - 53$.

Доказ. Трансформацијом дате једначине добија се њој еквивалентна једначина $(x^2 - 3)^2 + (y^2 - 7)^2 = 5$. Како је збир квадрата једнак 5 само ако је један од њих 1, а други 4, разликују се следеће могућности:

1) $(x^2 - 3)^2 = 1$ и $(y^2 - 7)^2 = 4$. Дакле, $|x^2 - 3| = 1$ и $|y^2 - 7| = 2$. Како једначине $x^2 = 2$ и $y^2 = 5$ немају решења у скупу цијелих бројева то је $x^2 = 4$ и $y^2 = 9$, а тражена решења су уређени парови бројева $(x, y) \in \{(2, 3); (2, -3); (-2, 3); (-2, -3)\}$.
2) $(x^2 - 3)^2 = 4$ и $(y^2 - 7)^2 = 1$. Слиједи, $|x^2 - 3| = 2$ и $|y^2 - 7| = 1$. Како једначине $y^2 = 8$ и $y^2 = 6$ немају решења у скупу цијелих бројева то једначина у овом случају нема цјелобројних решења.

$\square$

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/ZBIRKA.pdf`

286

Постоје ли природни бројеви x, y, z такви да важи једнакост $x! + y! = z!$?

Доказ. Како је $x! + y! = z!$ и како је $x! \geq 1$ и $y! \geq 1$, то је очигледно $x < z$ и $y < z$. Тада је

$$x! + y! = z! = z(z-1)...(y+1)y(y-1)...3 \cdot 2 \cdot 1 = z(z-1)...(y+1)y!.$$

Значи да је

$$x! = z(z-1)...(y+1)y! - y! = y!(z(z-1)...(y+1) - 1).$$

Разликујемо три случаја:

- Ако је $x < y$ онда је $x! < y!$, па једначина нема рјешења;
- Ако је $x = y$, онда је $z(z-1)...(y+1) - 1 = 1$, па је $z(z-1)...(y+1) = 2$, што значи да је $z = 2$. Тада је $x = y = 1$.
- Ако је $x > y$, онда је $x \geq 2$ и

$$x! = x(x-1)...(y+1)y! = y!(z(z-1)...(y+1) - 1).$$

Након дијељења са $y!$ добија се да је $x(x-1)...(y+1) = z(z-1)...(y+1) - 1$. Како је лијева страна увијек парна, а десна непарна, једначина нема рјешења.

Према томе, једино рјешење је $x = y = 1$ и $z = 2$. $\square$

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/ZBIRKA.pdf`

287

Одредити све уређене парове (x, y) природних бројева x и y тако да је $x! + 5y = 6666$.

Доказ. Јасно је да број 6666 при дијељењу са 5 даје остатак 1. Према томе и број $x! + 5y$ при дијељењу са 5 мора давати остатак 1. Како је $5y$ увијек дјељиво са 5, остаје да се види када је остатак при дијељењу $x!$ са 5 једнак 1. Зна се да је за $x \geq 5$, број $x!$ увијек дјељив са 5, па у обзир долазе вриједности које су мање од 5, дакле $1, 2, 3, 4$. Како само $1! = 1$ и $3! = 6$ при дијељењу са 5 дају остатак 1, то су тражена рјешења

$$5y = 6665$$

или

$$5y = 6660.$$

Значи да су сва рјешења уређени парови: $(1, 1333); (3, 1332)$. □

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/ZBIRKA.pdf`

288

Ријешити једначину $x^2 + y^2 = 2^{1999}$ у скупу природних бројева.

Доказ. Како је 2^{1999} паран број, онда су бројеви x^2 и y^2 исте парности, па постоје двије могућности:

1. Бројеви x и y су непарни, тј. $x = 2m + 1$ и $y = 2n + 1$ $(m, n \in \mathbb{N})$.
   Тада је $x^2+y^2 = (2m+1)^2+(2n+1)^2 = 4m^2+4m+1+4n^2+4n+1 = 2^{1999}$. Слиједи да је $4m(m+1)+4n(n+1) = 2^{1999}-2 = 2(2^{1998}-1)$, односно $2m(m+1)+2n(n+1) = 2^{1998}-1$. Како је лијева страна једнакости паран број, а десна непаран број, у овом случају једначина нема цјелобројних решења.

2. Бројеви x и y су парни, тј. $x = 2^m a$ и $y = 2^n b$ гдје су a и b непарни природни бројеви, а m и n су природни бројеви мањи од 1000. Тада је

   $$x^2 + y^2 = (2^m a)^2 + (2^n b)^2 = 2^{2m}a^2 + 2^{2n}b^2 = 2^{1999},$$

   па се разликују три могућности:

   2.1. Ако је $m > n \geq 1$, онда је $2^{2m}a^2 + 2^{2n}b^2 = 2^{2n}(2^{2m-2n}a^2 + b^2) = 2^{1999}$. Слиједи да је $2^{2m-2n}a^2 + b^2 = 2^{1999-2n}$. Како је $(2^{2m-2n}a^2 + b^2 = 2^{1999-2n})$ непаран број, а $2^{1999-2n}$ паран број, то једначина нема решења.

   2.2. Ако је $m = n$, онда је $2^{2m}a^2 + 2^{2n}b^2 = 2^{2n}(a^2 + b^2) = 2^{1999}$, тј. $a^2 + b^2 = 2^{1999-2n}$. Како је $2^{1999-2n}$ паран број и непаран степен броја 2, то су евидентна два случаја:

      2.2.1. Ако је $n \leq 998$ онда је $2^{1999-2n}$ дјељиво са 4. Како су бројеви a и b непарни, то $a^2 + b^2$ при дијељењу са 4 даје остатак 2, па једначина нема решења.

      2.2.2. Ако је $n = 999$, онда је $a^2+b^2 = 2^{1999-1998} = 2$, па је $a = b = 1$, а $x = y = 2^{999}$.

   2.3. Ако је $1 \leq m < n$, онда је $2^{2m}a^2 + 2^{2n}b^2 = 2^{2m}(a^2 + 2^{2n-2m}b^2) = 2^{1999}$ или $a^2 + 2^{2n-2m}b^2 = 2^{1999-2m}$. Како је $(a^2 + 2^{2n-2m}b^2)$ непаран број, а $2^{1999-2m}$ паран број, то једначина нема решења.

   Дакле, једина решења дате једначине су $x = y = 2^{999}$.

□

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`http://www.diofant.org/FAJLOVI/PDF%20UCENJE/ZBIRKA.pdf`

289

●●●●

Наћи све природне бројеве n такве да је број

$$2^4 \cdot 3^{16} + 5^2 \cdot 3^{14} + 3^n$$

потпун квадрат.

Доказ. Нека је

$$A = 2^4 \cdot 3^{16} + 5^2 \cdot 3^{14} + 3^n = 3^{14}(16 \cdot 9 + 25) + 3^n = 3^{14} \cdot 169 + 3^n = t^2.$$

Ако је $n < 14$, тада је $A = 3^n(3^{14-n} \cdot 169 + 1)$, одакле слиједи да је n паран број и да је $3^{14-n} \cdot 169 + 1 = u^2$, што је немогуће јер је

$$3^{14-n} \cdot 169 + 1 \equiv 2 \pmod 4,$$

док је $u^2 \equiv 0 \pmod 4$ (u је паран број).

Ако је $n = 14$, број $A = 3^{14} \cdot 170$ није потпун квадрат.

Нека је $n \geq 14$. Тада је $A = 3^{14}(169+3^{n-14})$. Нека је $k = n-14$. Тада је $169+3^k = v^2$, тј. $3^k = (v-13)(v+13)$. Пошто је $(v+13)-(v-13) = 26$ слиједи једина могућност $v-13 = 1$ и $v+13 = 3^k$. Дакле, $v = 14$ и $27 = 3^k$, тј. $k = 3$ и $n-14 = 3$. Коначно, добијамо да је $n = 17$. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

290

●●●●

Ријешити у скупу цијелих бројева:

$$x^5 - x^3 - x^2 + 1 = y^2.$$

Доказ. Факторизацијом лијеве стране добијамо

$$(x-1)^2(x+1)(x^2+x+1) = y^2.$$

Ако је $x = 1$ тада је $y = 0$. У случају $x \neq 1$, горњу једначину трансформишемо у облик

$$(x+1)(x^2+x+1) = \left(\frac{y}{x-1}\right)^2.$$

Дакле, $(x-1) \mid y$. Означимо $A = x+1$, $B = x^2+x+1$. Будући да је $B - xA = 1$, слиједи $(A, B) = 1$. Како је $B = (x+\frac{1}{2})^2 + \frac{3}{4} > 0$, A и B су потпуни квадрати. За $x > 1$ је $x^2 < x^2+x+1 < (x+1)^2$, а за $x \leq -2$ је $x^2 \geq x^2+x+1 > (x+1)^2$, па зато B не може бити квадрат цијелог броја. Преостају случајеви $x = -1$ и $x = 0$ из којих редом добијамо $y = 0$, односно $y = \pm 1$.

☐

(**Невена Гиговић 1/19 Ц**) задатак преузет из
Елементарна теорија бројева Игор Долинка

291

Доказати да конгруенција $6x^2+5x+1 \equiv 0 \pmod{m}$ има рјешење за сваки позитивни цјелобројни *modul* m, иако једначина $6x^2+5x+1=0$ нема цјелобројна рјешења.

Доказ. Почетну једначину $6x^2+5x+1=0$ можемо записати као

$$6x^2+5x+1=(3x+1)(2x+1)$$

што имплицира да једначина нема цјелобројна рјешења. Нека је m произвољни позитивни цијели број. Нека је даље, $m=2^k m_1$, гдје је k цијели број ≥ 0, а m_1 је непаран. Како је нзд$(2^k, m_1)=1$, тада постоји позитиван цијели број x такав да је $3x \equiv -1 \pmod{2^k}$ и $2x \equiv -1 \pmod{m_1}$, па слиједи да

$$m=2^k m_1 \mid (3x+1)(2x+1)$$

па према томе важи да је $6x^2+5x+1 \equiv 0 \pmod{m}$. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

292

Доказати да је последња цифра сваког парног савршеног броја увијек 6 или 8.
Напомена: Сваки парни савршени број је облика $2^{p-1}(2^p-1)$ гдје су p и 2^p-1 прости бројеви.

Доказ. За $p=2$ добијамо број 6. Ако је $p>2$, тада је p прост број облика $4k+1$ или $4k+3$.

- Ако је $p=4k+1$ тада је

  $$2^{p-1}=2^{4k+1-1}=2^{4k}=16^k,$$

  па је последња цифра броја 2^{p-1} очигледно 6.
  Даље имамо да је

  $$2^p-1=2^{4k+1}-1=2\cdot 2^{4k}-1=2\cdot 16^k-1,$$

  па је последња цифра броја 2^p-1 очигледно 1. Дакле, последња цифра производа $2^{p-1}(2^p-1)$ је 6.

- Ако је $p=4k+3$ тада је

$$2^{p-1} = 2^{4k+3-1} = 2^{4k+2} = 4 \cdot 2^{4k} = 4 \cdot 16^k,$$

па је последња цифра броја 2^{p-1} очигледно 4.
Даље имамо да је

$$2^p - 1 = 2^{4k+3} - 1 = 8 \cdot 2^{4k} - 1 = 8 \cdot 16^k - 1,$$

па је последња цифра броја $2^p - 1$ очигледно 7. Дакле, последња цифра производа $2^{p-1}(2^p - 1)$ је 8.

□

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

293 ●●●●

Доказати да једначина

$$3x^4 + 2013 = 25y^2 - 24x^2$$

нема цјелобројна рјешења.

Доказ. Напишимо дату једначину у облику

$$3x^4 + 24x^2 - 25y^2 + 2013 = 0.$$

Како су сви сабирци осим $25y^2$ дјељиви са 3, тада и $25y^2$ мора бити дјељив са 3, па и y мора бити дјељив са 3. Нека је $y = 3y_1$. Након дијељења са 3, посматрана једначина постаје

$$x^4 + 8x^2 - 75y_1^2 + 671 = 0.$$

Ако је x дјељиво са 3 онда су сви сабирци осим 671 дјељиви са 3, што је немогуће. Ако x није дјељив са 3, онда његов квадрат даје остатак 1 при дијељењу са 3, а исто важи и за његов четврти степен. То значи да је $x^4 + 8x^2$ дјељиво са 3 ($x^4 + 8x^2 \equiv 1 + 8 \cdot 1 \equiv 0 \pmod 3$). И у овом случају је $x^4 + 8x^2 - 75y_1^2$ дјељиво са 3, а 671 није дјељиво са 3. Дакле, дата једначина нема цјелобројних рјешења. □

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

294 ●●●●

Одредити задњу цифру производа првих 100 природних бројева који при дијељењу са 5 дају остатак 3.

Доказ. Сви природни бројеви који при дијељењу са 5 дају остатак 3 могу се записати у облику $5k + 3, k \in \mathbb{N}_0$. Запишимо производ првих сто таквих бројева:

$$3 \cdot 8 \cdot 13 \cdot 18 \cdot 23 \cdots (5k+3) \cdots 498 =$$
$$(3 \cdot 8)(13 \cdot 18) \cdots ((5k-2)(5k+3)) \cdots (493 \cdot 498).$$

Сваки од 50 производа у заградама завршава се цифром 4. Заиста,

$$n = (5k-2)(5k+3) \equiv -6 \equiv 4 \pmod 5,$$

па је очигледно n паран број. Према Кинеској теореми о остацима, систем конгруенција

$$n \equiv 4 \pmod 5$$
$$n \equiv 0 \pmod 2,$$

има јединствено рјешење по модулу 10, па је то на примјер 4, а сва су рјешења
$n \equiv 4 \pmod{10}$.
Задња цифра нашег производа је задња цифра израза 4^{50}. Како је $4^{50} = 16^{25}$, а степен броја 16 увијек се завршава цифром 6, слиједи да се тражени производ забршава цифром 6. □

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

295

Нека је скуп $\{1, 2, \ldots, 1998\}$ разбијен у парове $\{a_i, b_i\}$, $i = 1, 2, \ldots, 999$ такве да је $|a_i - b_i|$ једнако 1 или 6 . Доказати да се сума

$$S = |a_1 - b_1| + |a_1 - b_1| + \cdots + |a_{999} - b_{999}|$$

завршава цифром 9 .

Доказ. Из услова задатка да $|a_i - b_i|$, $i = 1, 2, \ldots, 999$ једнако 1 или 6 закључујемо да је

$$|a_i - b_i| \equiv 1 \pmod 5$$

па је онда

$$S = |a_1 - b_1| + |a_2 - b_2| + \cdots + |a_{999} - b_{999}| = 999 \equiv 1 \pmod 5 \ .$$

Осим тога лако можемо примјетити да важи

$$|m - n| \equiv m - n \equiv m + n \pmod 2 \ , \ m, n \in \mathbb{Z} \ .$$

Користећи претходно добијамо

$$S = |a_1 - b_1| + |a_2 - b_2| + \cdots + |a_{999} - b_{999}| =$$
$$= a_1 + b_1 + a_2 + b_2 + \cdots + a_{999} + b_{999} = 999 \cdot 1999 \equiv 1 \pmod 2$$

Дакле добили смо систем

$$\begin{cases} S \equiv 4 & \pmod 5 \\ S \equiv 1 & \pmod 2 \end{cases}$$

Примјеном стандардног поступка из Кинеске теореме о остацима добијамо

$$S = 9 + 10t \ , \ t \in \mathbb{Z} \iff S \equiv 9 \pmod{10}$$

Дакле , посљедња цифра броја S је 9. □

(**Велимир Ђоровић 5/19 Б**) задатак са USAMO 1998
`https://prase.cz/kalva/usa/usa98.html`

296

Нека су p и q прости бројеви већи од 2. Доказати да је

$$\lfloor \frac{p^q + q^p}{pq} \rfloor$$

паран број.

Доказ. Ако је $p = q$, добијамо да је $\frac{p^q+q^p}{pq} = 2p^{p-2}$, што је паран број.
Ако је $p \neq q$, по малој Фермаовој теореми:

$$p^q \equiv p \pmod{q} \Rightarrow q \mid p^q - p \Rightarrow pq \mid p^q - p \qquad \textbf{(1)}$$

Слично:

$$q^p \equiv q \pmod{p} \Rightarrow p \mid q^p - q \Rightarrow pq \mid q^p - q \qquad \textbf{(2)}$$

Из **(1)** и **(2)**:

$$pq \mid p^q - p + q^p - q = p(p^{q-1} - 1) + q(q^{p-1} - 1)$$

Пошто су p и q прости бројеви већи од 2, p и q морају бити непарни па је $p^q - p + q^p - q$ паран. Како је $p + q < pq$:

$$\lfloor \frac{p^q + q^p}{pq} \rfloor = \frac{p^q + q^p - p - q}{pq}$$

закључујемо да је дати број паран.

□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

297

Наћи све цијеле бројеве n такав да је $n(n-8)$ потпун квадрат .

Доказ. Претпоставимо да је $n(n-8)$ потпун квадрат тј.

$$n(n-8) = p^2 \ .$$

Тада је:

$$n^2 - 8n - p^2 = 0$$

одатле добијамо m

$$n_{1,2} = \frac{8 \pm \sqrt{64 + 4p^2}}{2} = 4 \pm \sqrt{16 + p^2} \ .$$

Пошто желимо да m буде цио број онда тражимо да је $16+p^2$ потпун квадрат. Даље разматрамо

$$16+p^2=l^2 \implies 16=l^2-p^2 \implies$$
$$(l-p)(l+p)=2^4$$

Дакле, постоји 5 случајева

$$\textbf{(I)} \qquad \begin{cases} l-p=1 \\ l+p=16 \end{cases} \implies l=\frac{17}{2}$$

$$\textbf{(II)} \qquad \begin{cases} l-p=2 \\ l+p=8 \end{cases} \implies l=5$$

$$\textbf{(III)} \qquad \begin{cases} l-p=4 \\ l+p=4 \end{cases} \implies l=4$$

$$\textbf{(IV)} \qquad \begin{cases} l-p=8 \\ l+p=2 \end{cases} \implies l=5$$

$$\textbf{(V)} \qquad \begin{cases} l-p=1 \\ l+p=16 \end{cases} \implies l=\frac{17}{2}$$

Одабуцујемо $l=\frac{17}{2}\notin\mathbb{Z}$ и

$$n_{1,2}=4\pm\sqrt{16+p^2}=4\pm l$$

па су једина рјешења за n

$$\{4\pm 4, 4\pm 5\}=\{-1,8,9\}\,.$$

☐

(**Велимир Ћоровић 5/19 Б**) задатак инспирисан потребама следећег задатка

298 ●●●●

Наћи све цијеле ненулте бројеве m и n које задовољавају

$$(m^2+n)(m+n^2)=(m-n)^3$$

Доказ. Множењем добијамо

$$m^3+mn+m^2n^2+n^3=m^3-3m^2n+3mn^2-n^3$$

даље кратимо m^3 и дијелимо са $n\neq 0$

$$2n^2+(m^2-3m)n+(3m^2+m)=0.$$

Тиме смо добили квадратну једначину по n и тражимо да је њена дискриминанта

$$D = (m^2 - 3m)^2 - 8(3m^2 + m) = m^4 - 6m^3 - 15m^2 - 8m$$

потпун квадрат . Факторизацијом дискриминанте добијамо $D = m(m-8)(m+1)^2$. Примјетимо да је D потпуно квадрат ако и само ако је $m(m-8)$ потпун квадрат.

На основу претходног задатка закључујемо да су за m једине ненулте могућности за $-1, 8, 9$.

Уврштавањем $m = -1, 8, 9$ у једначину $2n^2 + (m^2 - 3m)n + (3m^2 + m) = 0$ добијамо сва могућа рјешења (m, n)

$$\{(-1, -1), (8, -10), (9, -6), (9, -21)\}.$$

□

(**Велимир Ђоровић 5/19 Б**) задатак са USAMO 1987
`https://prase.cz/kalva/usa/usa87.html`

299

Методом свођења на Диофантову једначину ријешити конгруенције:
a) $3x \equiv 5 \pmod 7$
b) $2x \equiv 6 \pmod{10}$

Доказ. a) Како је $NZD(3, 7) = 1$, а $1 \mid 7$,ова конгруенција има јединствено решење.
Из дате конгруенције,слиједи да $7 \mid 3x - 5$, тј. постоји $y \in Z$ такво да је

$$y = \frac{3x - 5}{7},$$

одакле слиједи

$$3x - 7y = 5.$$

Очигледно,једно рјешење Диофантове једначине $(x_0, y_0) = (4, 1)$, па слиједи

$$3x_0 - 7y_0 = 5.$$

Одузимајући једначине,добијамо:

$$3(x - x_0) - 7(y - y_0) = 0,$$

па слиједи

$$y - y_0 = \frac{3(x - x_0)}{7},$$

Како је $y - y_0$ цио број , онда мора и $\frac{3(x-x_0)}{7}$ бити цио број, а како су 3 и 7 узајамно прости бројеви, слиједи да $x - x_0$ мора бити дјељив са 7, тј.

$$x - x_0 = 7t, t \in Z$$

Закључујемо да је рјешење полазне конгруенције

$$x = 7t + 4, t \in Z$$

тј.

$$x \equiv 4, \pmod 7$$

b) $NZD(2, 10) = 2$ па како $2 \mid 6$ полазна конгруенција има два рјешења.
Аналогно претходном примјеру добијамо Диофантову једначину

$$2x - 10y = 6,$$

чије је једно рјешење (8,1) ,па је рјешење конгруенције

$$x = 8 + \frac{-10}{2}t = 8 - 5t, t \in \{0, 1\}$$

Тако смо добили да је рјешење дате конгруенције

$x \equiv 8 \pmod 5$ i $x \equiv 3 \pmod 5$

□

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

300 ●●●●

Одредити све цијеле бројеве x и y тако да:

$$x^2 - xy + 2x - 3y = 6$$

Доказ.

$$x^2 - xy + 2x - 3y = 6$$

$$x^2 + 2x - xy - 3y = 6$$

$$x(x + 2) - y(x + 3) = 6$$

$$y(x + 3) = x(x + 2) - 6$$

$$y = \frac{x(x + 2) - 6}{(x + 3)}$$

$$y = \frac{x^2 + 2x - 6}{x + 3}$$

$$y = \frac{x^2 + 2x + 4x + 9 - 4x - 9 - 6}{x + 3}$$

$$y = \frac{x^2 + 6x + 9 - 4x - 15}{x+3}$$

$$y = \frac{(x+3)^2 - 4x - 15}{x+3}$$

$$y = \frac{(x+3)^2}{x+3} - \frac{4x+15}{x+3}$$

$$y = x + 3 - \frac{4x+15}{x+3}$$

Да би y био цијели број , онда и $a = \frac{4x+15}{x+3}$ мора да буде цијели број.

$a = \frac{4x+15}{x+3}$

$a = \frac{4x+12+3}{x+3}$

$a = \frac{4(x+3)+3}{x+3}$

$a = 4 + \frac{3}{x+3}$

Да би a био цијели број, онда и $\frac{3}{x+3}$ мора да буде цијели број.

$x + 3 = -3$, $x = -6$ и $y = 2$
$x + 3 = 3$, $x = 0$ и $y = -2$
$x + 3 = -1$, $x = -4$ и $y = -2$
$x + 3 = 1$, $x = -2$ и $y = -6$ □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.naukamladima.com/index.php?page=diofantove-jednacine`

301

Ријешити једначину $\varphi(n) = 3600$, ако су 3,5, и 7 једини прости фактори броја n.

Доказ. Нека је $n = 3^x + 5^y + 7^z$. Тада је

$3600 = \varphi(n) = 3^{x-1} + 5^{y-1} + 7^{z-1} \cdot (3-1) \cdot (5-1) \cdot (7-1)$

$= 3^{x-1} + 5^{y-1} + 7^{z-1} \cdot 2 \cdot 4 \cdot 6$,

односно $3^{x-1} + 5^{y-1} + 7^{z-1} = 3 \cdot 5^2$ па је
$x = 2$
$y = 3$
$z = 1$
Тада је $n = 3^2 \cdot 5^3 \cdot 7 = 7875$ □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

302

Претпоставимо да се сви позитивни дјелиоци природног броја n (укључујући 1 и n) могу подијелити у дисјунктне парове на такав начин да је збир бројева у сваком пару прост број. Доказати да су овако добијени прости бројеви међусобно различити.

Доказ. Запишимо n у облику $n = p^k m$ за неки прост број p и природне бројеве k, m гдје $p \nmid m$. Нека је $d(m)$ број дјелилаца броја m. Тада n има тачно $d(m)$ дјелилаца који нијесу дјељиви са p, односно $kd(m)$ дјелилаца који су дјељиви са p (дјелиоци броја m помножени са неким степеном броја p, не већим од k-тог).
Пошто се у сваком пару из формулације задатка мора налазити барем један број који није дјељив са p (у супротном збир би био дјељив са p, па не би био прост број) важи да је $d(m) \geq kd(m) \Rightarrow k = 1$.
Дакле, n не може бити дјељив ниједним квадратом простог броја. Осим тога, n мора бити паран број јер би у супротном сви његови дјелиоци били непарни, па како их год подијелили у парове, збир бројева у сваком пару био би паран број и самим тим не би сви збирови били прости бројеви.
Закључујемо да n мора бити облика $n = 2p_1 ... p_k$ гдје су $p_1 ... p_k$ различити непарни прости бројеви.
Примијетимо да n може бити у пару једино са бројем 1 јер ако би био у пару са неким својим дјелиоцем, збир би им био дјељив са тим дјелиоцем и не би био прост број. Самим тим, сваки од бројева $\frac{n}{p_i}$ у пару је са неким бројем који је узајамно прост са њим, а то мора бити p_i. Слично, $\frac{n}{p_i p_j}$ у пару је са $p_i p_j$ итд. што значи да сви парови морају бити облика $(x, \frac{n}{x})$.

Претпоставимо да два пара имају исти збир тј.

$$x + \frac{n}{x} = y + \frac{n}{y}$$

Множећи са xy добијамо

$$xy(x-y) = n(x-y) \Leftrightarrow (xy-n)(x-y) = 0$$

Дакле, мора бити $x = y$ или $y = \frac{n}{x}$ тј. $(x, \frac{n}{x}) = (y, \frac{n}{y})$, а то смо и требали да докажемо. □

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

303

За сваки природан број обиљежимо са x_n број који се добија узастопним записивањем природних бројева од 1 до n (нпр. $x_{11} = 1234567891011$). Одредити све природне бројеве n за које $27 \mid {x_n}^2 + x_n - 2$.

Доказ. Нека је n неки природан број за који важи услов задатка. Лако је видјети да је

$$ {x_n}^2 + x_n - 2 = (x_n - 1)(x_n + 2). $$

Како $27 \mid (x_n - 1)(x_n + 2)$ закључујемо да

$$ 9 \mid (x_n - 1) \text{ или } 9 \mid (x_n + 2). $$

Нека нпр. $9 \mid (x_n - 1)$. Тада $3 \mid (x_n - 1)$ па како $3 \mid x_n + 2 - (x_n - 1) = 3$ то онда и $3 \mid (x_n + 2)$. Овим смо доказали да важи:

$$ 27 \mid {x_n}^2 + x_n - 2 \Leftrightarrow (9 \mid (x_n - 1)) \lor (9 \mid (x_n + 2)) \Leftrightarrow (x_n \equiv 7 \pmod 9) \lor (x_n \equiv 1 \pmod 9) \qquad \mathbf{(1)} $$

Користећи чињеницу да природан број при дијељењу са 9 даје исти остатак као и његов збир цифара, важи да је:

$$ x_n \equiv 1 + 2 + \ldots + n = \frac{n(n+1)}{2} \pmod 9 \qquad \mathbf{(2)} $$

Како су $0, 1, \ldots, 8$ могући остаци при дијељењу броја n са 9, лако се показује да број $\frac{n(n+1)}{2}$ при дијељењу са 9 даје остатке из скупа $\{0, 1, 3, 6\}$.
Из **(1)** и **(2)** добијамо да су решења они бројеви n који при дијељењу са 9 дају остатак 1, 4 или 7 односно они који при дијељењу са 3 дају остатак 1.

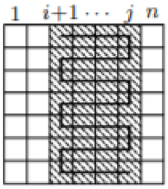
□

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb/`

304

Нека су m и n природни бројеви. У свако поље квадратне табле $n \times n$ уписан је по један цијели број. *Пут* је низ међусобно различитих поља у коме је прво поље у првој врсти, а последње у n-тој, и свака два узастопна поља имају заједничку страницу. Доказати да:
(а) Ако је $m \leq n$, увијек постоји пут у коме је збир уписаних бројева дјељив са m.
(б) Ако је $m > n$, такав пут не мора да постоји.

Доказ. (а) Нека је S_i - збир елемената у првих i колона, $i = 1, 2, \ldots, n$. Примијетимо да ако имамо n бројева (збирова) и посматрамо остатке при дијељењу ових бројева (збирова) са m, пошто је $m \leq n$, сигурно ће постојати барем два збира која дају исти остатак. Нека су то рецимо S_i и S_j гдје је $i < j$. Тада $m \mid S_j - S_i$, односно збир бројева у колонама од $(i+1)$-ве до j-те је дјељив са m. Било који пут који обилази сва ова поља (такав постоји - видјети слику) задовољава услов задатка.



(б) Контрапримјер: Упишимо у сва поља прве врсте јединице, а у сва остала нуле. Тада је збир бројева на сваком путу између 1 и n, а како је $m > n$ тај збир никада неће бити дјељив са m.

☐

(**Сандра Вујичић 2/19 Б**) задатак преузет са
`https://imomath.com/srb`

305 ●●●●

Одредити троцифрени завршетак броја $2003^{2002^{2001}}$.

Доказ. Стратегија за рјешавање овог задатка јесте да разматрања сведемо на што мање бројеве.Основне особине конгруенција нам омогућавају да смањимо основу степена,Ојлерова теорема нам помаже да смањимо експонент, а кинеска теорема о остацима може бити корисна да се разматрање сведе на конгруенције мањег модула.
Посматрајмо конгруенцију по модулу 1000 датог броја:

$$2003^{2002^{2001}} \equiv 3^{2002^{2001}} \pmod{1000}$$

. Из Ојлерове теореме имамо да је $3^{400} \equiv 1 \pmod{1000}$, јер је $NZD(3, 1000) = 1$
а $\phi(1000) = 400$, па ће онда бити

$$3^{2002^{2001}} \equiv 3^{2^{2001}} \pmod{1000}$$

Пронађимо сада остатак при дијељењу 2^{2001} са 400 да бисмо поново примијенили резултат који смо добили из Ојлерове теореме.Како $400 = 16 \cdot 25$, а 2^{2001} је дјељиво са 16 остаје да одредимо остатак при дијељењу са 25.
Како је $\phi(25) = 20$, то је $2^{2001} \equiv 2 \pmod{25}$. Из $2^{2001} \equiv 2 \pmod{25}$ и $2^{2001} \equiv 0 \pmod{16}$ имамо по Кинеској теореми о остацима:

$$2^{2001} \equiv 352 \pmod{400}$$

Отуда је

$$3^{2^{2001}} \equiv 3^{352} \pmod{1000}$$

Како је $1000 = 8 \cdot 125$,сада тражимо остатке при дијељењу 3^{352} са 8 и са 125.

$$3^{352} = (3^2)^{176} \equiv 1 \pmod{8}$$

Како је $\phi(125) = 100$ имамо да је $3^{352} \equiv 3^{52} \pmod{125}$. Користићемо да је $3^6 \equiv 4 \pmod{125}$

$$3^{52} = 3^4 \cdot 3^{48} = 3^4 \cdot (3^6)^8 \equiv 3^4 \cdot 4^8 \equiv 81 \cdot (2^7)^2 \cdot 4 \equiv$$

$$\equiv 81 \cdot 3^2 \cdot 4 \equiv 324 \cdot 9 \equiv 74 \cdot 9 \equiv 666 \equiv 41 \pmod{125}$$

Како је $3^{52} \equiv 1 \pmod{8}$ и $3^{52} \equiv 41 \pmod{125}$ имамо да је

$$3^{52} \equiv 41 \pmod{1000}$$

Отуда слиједи да се $2003^{2002^{2001}}$ завршава са 041. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

306

Нека су m и n природни бројеви са особином да за све природне бројеве k важи $(11k-1, m) = (11k-1, n)$. Доказати да тада за неки цијели број s важи $\frac{m}{n} = 11^s$.

Доказ. Нека је $m = 11^a p$, $n = 11^b q$, при чему је $a, b \geq 0$ и бројеви p, q нису дјељиви са 11. Доказаћемо да је $p = q$, одакле слиједи тврђење задатка.

Како је $(p, 11) = 1$, по Кинеској теореми о остацима постоји природан број x који задовољава:

$$x \equiv 0 \pmod{p}, \quad x \equiv -1 \pmod{11}.$$

Али, тада је $x = 11k - 1$ за неки природан број k, па је:

$$p = (x, 11^a p) = (11k-1, m) = (11k-1, n) = (x, 11^b q) = (x, q) \leq q.$$

Потпуно аналогно можемо показати да је $q \leq p$, па слиједи закључак да је $p = q$ чиме је доказ завршен. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет из
Елементарна теорија бројева Игор Долинка

307

Доказати да постоји бесконачно много парова природних бројева (m, n) таквих да је $4mn - m - n + 1$ потпун квадрат.

Доказ. Посматрајмо једначину

$$4mn - m - n + 1 = k^2.$$

Након множења са 4 и одузимања 3 од обје стране, могуће је факторисати лијеву страну, тако да се добија

$$(4m-1)(4n-1) = 4k^2 - 3.$$

Идеја која води налажењу бесконачног низа решења ове једначине је да се за k уведе одговарајућа смјена која ће $4k^2 - 3$ трансформисати у разлику квадрата. Очигледно, линеарна смјена облика $k = at + b$ $(a, b \in \mathbb{Z})$ није одговарајућа, јер након квадрирања остаје линеарни члан. Због тога ћемо покушати са смјеном $k = at^2 + b$. Тада је

$$\begin{aligned} 4k^2 - 3 &= 4(at^2+b)^2 - 3 = 4a^2t^4 + 8abt^2 + (4b^2 - 3) \\ &= (2at^2 + b)^2 - (-4abt^2) + (3b^2 - 3). \end{aligned}$$

Према томе, ако изаберемо коефицијенте a, b тако да је $b^2 = 1$, $ab < 0$ и да $-ab$ буде потпун квадрат, постићи ћемо наш циљ. Очито је $a = 1$, $b = -1$ један од адекватних избора, па тако за $k = t^2 - 1$ имамо

$$4k^2 - 3 = (2t^2 - 1)^2 - 4t^2 = (2t^2 - 2t - 1)(2t^2 + 2t - 1).$$

Како су бројеви $2t^2 - 2t = 2t(t-1)$ и $2t^2 + 2t = 2t(t+1)$ дјељиви са 4, можемо њих "прогласити" за $4m$, односно $4n$. Тако, имамо жељени низ решења: наиме, ако је $t \in \mathbb{N}$, за

$$m = \frac{1}{2}t(t-1), \quad n = \frac{1}{2}t(t+1),$$

важи $4mn - m - n + 1 = (t^2 - 1)^2$. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет из
Елементарна теорија бројева Игор Долинка

308

За које цијеле бројеве x и y број $x^4 + y^4$ при дијељењу с 25 даје остатак 3?

Доказ. Тражимо бројеве x и y такве да је $x^4 + y^4 = 25m + 3$ за неки $m \in \mathbb{Z}$. Уочимо да тада $x^4 + y^4$ и при дијељењу с 5 даје остатак 3. Погледајмо какве остатке при дијељењу с 5 може давати четврти степен цијелог броја:

- $x \equiv 0 \pmod 5 \quad \Rightarrow x^4 \equiv 0 \pmod 5$;
- $x \equiv \pm 1 \pmod 5 \quad \Rightarrow x^4 \equiv (\pm 1)^4 = 1 \pmod 5$;
- $x \equiv \pm 2 \pmod 5 \quad \Rightarrow x^4 \equiv (\pm 2)^4 = 16 \equiv 1 \pmod 5$;

Дакле, x^4 и y^4 при дијељењу с 5 могу дати само остатке 0 или 1, па онда $x^4 + y^4$ при дијељењу с 5 може дати остатке 0, 1 или 2, а никако 3. Слиједи да тражени бројеви x и y не постоје. ☐

(**Невена Гиговић 1/19 Ц**) задатак преузет са
`https://www.scribd.com/doc/95036949/02-Bur-A`

309

Нека је $C(n)$ збир свих позитивних дјелилаца природног броја n. Природан број m зовемо *јаким* ако за све $1 \leq k < m$ важи

$$\frac{C(k)}{k} < \frac{C(m)}{m}.$$

Доказати да има бесконачно много јаких бројева.

Доказ. Означимо са $a_m = \frac{C(m)}{m}$. Јасно, број m је јак ако и само ако је $a_k < a_m$ за све $k < m$. Сада је довољно доказати да низ $a_n, n \in \mathbb{N}$, нема највећи елемент, пошто је тада лако извести да постоји бесконачно много јаких бројева. Наиме, ако је број m јак, нађимо најмање $m' > m$ тако да је $a_m < a_{m'}$. Тада је број m' очигледно јак.
Дакле, нека је n произвољан природан број. За сваки његов дјелилац d важи да $2d \mid 2n$. Како, осим тога, тривијално важи да $1 \mid 2n$, добијамо неједнакост

$$C(2n) \geq 2C(n) + 1.$$

Одавде дијељењем са $2n$ одмах слиједи $a_{2n} > a_n$, па добијамо тражени резултат. □

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

310

Број n је *добар* ако се може представити као збир (не обавезно различитих) природних бројева чији је збир реципрочних вриједности једнак 1. Ако је познато да су бројеви $33, ..., 73$ добри, доказати да су сви бројеви ≥ 33 добри.

Доказ. Нека је n добар број, при чему је за неке природне бројеве a_i испуњено:

$$a_1 + ... + a_k = n, \frac{1}{a_1} + ... + \frac{1}{a_k} = 1.$$

Тада је

$$\frac{1}{2a_1} + ... + \frac{1}{2a_k} = \frac{1}{2},$$

па због $\frac{1}{2} = \frac{1}{4} + \frac{1}{4} = \frac{1}{3} + \frac{1}{6}$ низови

$$(4, 4, 2a_1, ..., 2a_k) \text{ и } (3, 6, 2a_1, ..., 2a_k)$$

имају збир реципрочних вриједности једнак 1. Отуда добијамо да су бројеви $2n+8$ и $2n+9$ такође добри. Међутим, $2 \cdot 33 + 8 = 74$ и $2 \cdot 33 + 9 = 75$, па једноставном примјеном индукције добијамо, на основу дате хипотезе, да су сви бројеви ≥ 33 добри. □

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

311

Број 9 се може представити као збир два узастопна природна броја $9 = 4+5$. Међутим, он се може записати као сума бар два узастопна природна броја на тачно два начина:

$$9 = 4 + 5 = 2 + 3 + 4.$$

Да ли постоји природан број који се може представити као збир 1990 узастопних природних бројева и који се може записати као збир бар два узастопна природна броја на тачно 1990 начина?

Доказ. Претпоставимо да број N има тражена својства. Први од два услова задатка се може записати као

$$N = m + (m + 1) + ... + (m + 1989) = 995(2m + 1989),$$

за неко m, према томе је N непаран број, дјељив са 5 и 199. Други услов је да постоји тачно 1990 парова природних бројева (n, k) за које је

$$N = n + (n + 1) + ... + (n + k) = \frac{(k+1)(2n+k)}{2}.$$

Према томе, постоји тачно 1990 начина да прикажемо $2N$ у облику:

$$2N = (k + 1)(2n + 5),$$

при чему је $k \geq 1$. Пошто је N непаран број, то је један од ова два фактора непаран, док је други дјељив са 2, али не и са 4. Како је $k + 1 < 2n + k$, слиједи да свака описана факторизација броја $2N$ једнозначно даје тражени пар (n, k). Ако запишемо

$$2N = 2 \cdot 5^{s_1} \cdot 199^{s_2} \cdot p_3^{s_3} \cdots p_r^{s_r},$$

гдје су p_i прости бројеви различити од $2, 5$ и 199, добијамо да је број дјелилаца броја $2N$ једнак

$$(1 + 1)(s_1 + 1)(s_2 + 1)...(s_r + 1).$$

Тако, факторизација $2N = uv, u < v$, има $(s_1 + 1)(s_2 + 1)...(s_r + 1)$, а пошто тривијална факторизација $2N = 1 \cdot 2N$ даје $k = 0$, описаних парова (n, k) има

$$(s_1 + 1)(s_2 + 1)...(s_r + 1) - 1.$$

Сада је $(s_1 + 1)(s_2 + 1)...(s_r + 1) = 1991 = 11 \cdot 181$. Како важи да $5 \cdot 199 \mid N$ имамо $s_1, s_2 > 0$, закључујемо да је $s_1 = 10, s_2 = 180$ или $s_1 = 180, s_2 = 10$, као и $s_3 = ... = s_r = 0$. То значи да је $N = 5^{10} \cdot 199^{180}$ или $N = 5^{180} \cdot 199^{10}$, па смо тако добили јединa два броја са траженим особинама. ☐

(**Радоман Гледовић 6/19 Ц**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

312

На колико различитих начина се могу од првих 18 природних бројева изабрати 3 броја тако да им збир буде дјељив са 3?

Доказ. При дијељењу неког броја са 3, остатак може бити 0, 1 или 2. Зато ових 18 бројева можемо подијелити у 3 групе према томе који остатак дају при дијељењу са 3. Свака од те три групе ће садржати по 6 бројева. Како би збир одабраних бројева био дјељив са 3, збир остатака при дијељењу такође мора бити дјељив са 3.
То је могуће у два случаја:
-сви одабрани бројеви су из исте групе
-сви одабрани бројеви су из различите групе.
У првом случају три од 6 бројева се може одабрати на $\binom{6}{3} = 20$ начина. Како имамо 3 групе, то имамо $20 \cdot 3$ могућности.
У другом случају број из сваке групе можемо одабрати на 6 начина, па је укупан број

начина $6 \cdot 6 \cdot 6 = 216$.
Дакле, укупан број могућности је $216 + 60 = 276$. ☐

(**Шћекић Лазар 6/19 Б**) задатак са интернета
`http://forum.matemanija.com/viewtopic.php?f=42&t=973`

313 ●●●●

Наћи све природне бројеве n,за које

$$n \mid (2^n - 1)$$

Доказ. Очигледно, $n = 1$ задовољава тражени услов. Претпоставимо да постоји $n \geq 2$ које задовољава наведени услов. Нека q_n означава најмањи прост фактор броја n. Докажимо да важи: ако је $n > 1$ и $p|(2^n - 1)$, тада је $p > q^n$. У том случају, имаћемо очигледну контрадикцију, јер $n \mid (2^n - 1)$ повлачи $q^n \mid (2^n - 1)$.Треба примијетити, да ако за природне бројеве a и b важи

$$2^a \equiv 2^b \equiv 1 \pmod{p}$$

, тада је

$$2^{(a,b)} \equiv 1 \pmod{p}$$

. Ако је $a \geq$ и $a = qb + r$,тада важи

$$2^r \equiv (2^b)^q 2^r = 2^a \equiv 1 \pmod{p}$$

. Настављајући очигледну примјену Еуклидовог алгоритма у експоненту добијамо управо жељени закључак. Како према Малој Фермаовој теореми важи $2^{p-1} \equiv 1 \pmod{p}$ за $d = (n, p-1)$ имамо $2^d \equiv 1 \pmod{p}$. Због тога је $d > 1$,па важи $q_n \leq d$. Са друге стране,$d \mid (p-1)$ па слиједи $p > d \geq q_n$.
Сходно томе,$n = 1$ је једино решење. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

314

а) Ријешити Диофантову једначину

$$23x + 29y = 1$$

б) Наћи цјелобројна решења x и y једначине

$$23x + 29y = 7$$

ц) Постоје ли цијели бројеви x и y такви да

$$3456x + 246y = 73$$

Доказ.

$$\begin{aligned}
29 : 23 = 1(6) &\implies 29 = 23 \cdot 1 + 6 \\
23 : 6 = 3(5) &\implies 23 = 6 \cdot 3 + 5 \\
6 : 5 = 1(1) &\implies 6 = 5 \cdot 1 + 1 \\
5 : 1 = 5(0) &\implies \text{нзд}(23, 29) = 1
\end{aligned}$$

Решење за остатке:

$$\begin{aligned}
6 &= 29 \cdot 1 + 23 \cdot (-1) \\
5 &= 23 \cdot 1 + 6 \cdot (-3) \\
1 &= 6 \cdot 1 + 5 \cdot (-1)
\end{aligned}$$

Па,

$$\begin{aligned}
1 &= 6 \cdot 1 + 5 \cdot (-1) = \\
&= 6 \cdot 1 + (23 \cdot 1 + 6 \cdot (-3)) \cdot (-1) = \\
&= 6 \cdot 4 + 23 \cdot (-1) = \\
&= (29 \cdot 1 + 23 \cdot (-1)) \cdot 4 + 23 \cdot (-1) = \\
&= 29 \cdot 4 + 23 \cdot (-5)
\end{aligned}$$

Дакле, $x = -5$, $y = 4$.

б) Из претходног претходног дијела задатка, имали смо

$$23 \cdot (-5) + 29 \cdot 4 = 1$$

Када помножимо обије стране једнакости са 7, добијамо

$$23 \cdot (-35) + 29 \cdot 28 = 7$$

из чега видимо да су тражена решења $x = -35$, $y = 28$.

ц) нзд$(3456, 246) = 2$ и $2 \nmid 73$ па не постоје цјелобројна решења x и y тако да важи ова једнакост. ☐

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

315

Игра се игра са картама на следећи начин. Након сваке игре, у зависности од исхода, играч добија a или b поена ($a, b \in \mathbb{N}$, $a > b$) и његов скор се акумулира од игре до игре. Примјећено је да постоји 35 недостижних скорова и један од њих је 58. Наћи a и b.

Доказ. Достижни скорови су ненегативни цијели бројеви облика $ax+by$. Ако је нзд$(a, b) > 1$, онда постоји бесконачно много таквих цијелих бројева. Закључујемо да мора нзд$(a, b) = 1$.
Да бисмо ријешили овај задатак, користићемо следећу теорему:
Теорема(Фробениус): Нека су a и b позитивни цијели бројеви. Ако је нзд$(a, b) = 1$, онда број позитивних цијелих бројева m који не може бити записан у облику $ar + bs = m$ за ненегативне цијеле бројеве r и s једнак је $\frac{(a-1)(b-1)}{2}$.
Дакле, $\frac{(a-1)(b-1)}{2} = 35 \implies (a-1)(b-1) = 70$
$70 = 2 \cdot 35 = 5 \cdot 14 = 7 \cdot 10$
Услови нзд$(a, b) = 1$, $a > b$ дозвољавају следећа два решења:

$$(a, b) = (71, 2)$$

$$(a, b) = (11, 8)$$

Како $71x + 2y = 71 \cdot 0 + 2 \cdot 29 = 58$, први пар отпада.
Друга могућност $11x + 8y = 58$ важи за $(x, y) = (6, -1)$ и $(x, y) = (-2, 10)$ па слиједи да $(a, b) = (11, 8)$ је јединствено решење. ☐

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

316

Нека су p и q два различита проста броја таква да $a^p \equiv a \pmod{q}$, $a^q \equiv a \pmod{p}$. Доказати да $a^{pq} \equiv a \pmod{pq}$.

Доказ. Из Мале Фермаове теореме знамо да $a^p \equiv a \pmod p$ и $a^q \equiv a \pmod q$ важи за било које $a \in \mathbb{Z}$.

$$a^p \equiv a \pmod p \implies (a^p)^q \equiv a^q \equiv a \pmod p \implies a^{pq} \equiv a \pmod p$$

$$a^q \equiv a \pmod q \implies (a^q)^p \equiv a^p \equiv a \pmod q \implies a^{pq} \equiv a \pmod q$$

То значи да $a^{pq} = px + a = qy + a$ за неке цијеле бројеве x и y. Из овога такође видимо да $px = qy$ из чега слиједи да $x = qk$, $y = pk$ за неко $k \in \mathbb{Z}$ јер су p и q прости бројеви.
Према томе, $a^{pq} = p(qk) + a = q(pk) + a = (pq)k + a \implies a^{pg} \equiv a \pmod{pq}$.

□

(**Милена Јововић 1/19 Б**) задатак преузет са
`http://math.cmu.edu/~cargue/arml/archive/15-16/number-theory-09-27-15-solutions.pdf`

317

а) У скупу природних бројева ријешити једначину

$$x^2 - xy + 2x - 3y = 1992$$

б) Доказати да једначина

$$5x^2 - 4y^2 = 1999$$

нема цијелобројних решења.

Доказ. а) Малом трансформацијом добијемо $x^2 + 2x - 1992 = (3 + x)y$

$$y = \frac{x^2 + 2x - 1992}{x + 3} = \frac{x^2 + 2x - 3 - 1989}{x + 3} = \frac{(x-1)(x+3) - 1989}{x + 3} =$$
$$= x - 1 - \frac{1989}{x + 3}$$

Да би број $\frac{1989}{x+3}$ био природан, $x + 3$ мора бити дјелиоц броја 1989, тј. један од бројева $1, 3, 9, 13, 17, 39, 51,$
$117, 153, 221, 663$ или 1989. Како је и y природан број, првих шест вриједности за $x + 3$ (а самим тим и за x) не долазе у обзир, па имамо следећих шест решења (x, y) за дату једначину: $(48, 8), (114, 96), (150, 136), (218, 208), (660, 656), (1986, 1984)$.

б)

$$\begin{aligned}
&5x^2 - 4y^2 = 1999\\
&5x^2 - 4y^2 = 1994 + 5\\
&5(x^2 - 1) - 4y^2 = 1994\\
&5(x-1)(x+1) - 4y^2 = 1994
\end{aligned}$$

С обзиром да је $5x^2 - 4y^2 = 1999$ непаран број, закључујемо да је x непарно. Тада је $(x-1)(x+1)$ производ узастопних парних бројева и дјељив је са 4. Ако се горња једначина подијели са 4, онда је њена лијева страна цијели број, а десна није. $\square$

(**Милена Јововић 1/19 Б**) задатак преузет са
"Бројеви, нестандардни задаци"Ратко Тошић, Драгољуб Милошевић

318
●●●●

Одредити остатак збира

$$S_{2013} = 1^{2501} + 2^{2501} + \ldots + 2012^{2501} + 2013^{2501}$$

при дијељењу са 625.

Доказ. Како је $\varphi(625) = \varphi(5^4) = 625 \cdot (1 - \frac{1}{5}) = 500$, то за природан број a који је узајамно прост са 625, из Ојлерове теореме слиједи да је

$$a^{2501} = (a^{500})^4 \cdot a \equiv 1^4 \cdot a \equiv a \pmod{625}$$

Ако природан број a није узајамно прост са 625, тада $5 \mid a$ па је $a = 5q,\ q \in \mathbb{N}$. Тада је

$$a^{2501} = (5q)^{2501} = 5^4 \cdot 5^{2497} q^{2501} = 625 \cdot 5^{2497} q^{2501}$$

одакле видимо да

$$a^{2501} \equiv 0 \pmod{625}$$

у случају да $5 \mid a$.
Због тога је

$$S_{2013} \equiv (1 + 2 + \ldots + 2013) - (5 + 10 + \ldots + 2010) \pmod{625}$$

Како је

$$1 + 2 + \ldots + 2013 = \frac{2013 \cdot 2014}{2} = 2027091$$

и

$$\begin{aligned} 5 + 10 + \ldots + 2005 + 2010 &= 5 \cdot 1 + 5 \cdot 2 + \ldots + 5 \cdot 401 + 5 \cdot 402 = \\ &= 5(1 + 2 + \ldots + 401 + 402) = \\ &= 5\frac{402 \cdot 403}{2} = \\ &= 405015 \end{aligned}$$

Из претходне двије једнакости слиједи да је

$$S_{2013} \equiv 1622076 \pmod{625}$$

односно

$$S_{2013} \equiv 201 \pmod{625}$$

$\square$

(**Милена Јовановић 1/19 Б**) задатак преузет са
`http://www.imvibl.org/dmbl/meso/mat_kol_19_3_2013/mat_kol_19_3_35_44.pdf`

319

●●●●

Доказати да за сваки природан број n, бројеви облика n^{4k+1}, $k \in \mathbb{N}$ и n имају исту задњу цифру.

Доказ. Треба да покажемо да је

$$n^{4k+1} \equiv n \pmod{10}, \ \forall n \in \mathbb{N}$$

Ако је нзд$(n, 10) = 1$, онда тврдња слиједи из Ојлерове теореме јер

$$n^{\varphi(10)} = n^4 \equiv 1 \pmod{10}$$

па важи и

$$n^{4k+1} = n^{4k}n \equiv n \pmod{10}$$

Ако је нзд$(n, 10) \neq 1$, постоје следеће могућности:
1) нзд$(n, 10) = 2$
Тада је $n \equiv 0 \pmod 2$ па је и

$$n^{4k+1} \equiv 0 \equiv n \pmod 2 \quad (1)$$

Како је нзд$(n, 5) = 1$, онда из Мале Фермаове теореме слиједи $n^4 \equiv 1 \pmod 5$ односно

$$n^{4k+1} \equiv n \pmod 5 \quad (2)$$

Из (1) и (2) слиједи тврдња.
2) нзд$(n, 10) = 5$
Тада је $n \equiv 1 \pmod 2$ па је и

$$n^{4k+1} \equiv 1 \equiv n \pmod 2 \quad (3)$$

а из $n \equiv 0 \pmod 5$ слиједи

$$n^{4k+1} \equiv 0 \equiv n \pmod 5 \quad (4)$$

Из (3) и (4) слиједи тврђење.
3) нзд$(n, 10) = 10$
Тада је $n \equiv 0 \pmod{10}$, па је и

$$n^{4k+1} \equiv 0 \equiv n \pmod{10}$$

□

(**Милена Јовановић 1/19 Б**) задатак преузет са
`http://www.imvibl.org/dmbl/meso/mat_kol_19_3_2013/mat_kol_19_3_35_44.pdf`

320

Показати да ако је n позитиван цијели број, онда

$$\varphi(2n)=\begin{cases}\varphi(n) & \text{, ако је } n \text{ непарно}\\ 2\varphi(n) & \text{, ако је } n \text{ парно}\end{cases}$$

Доказ. Нека је $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ проста (канонска) факторизација броја n.
Како је $(1-\frac{1}{p_1})p_1^{\alpha_1}=p_1^{\alpha_1-1}(p_1-1)$, Ојлерову формулу $\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_k})$ можемо записати и на следећи начин

$$\varphi(n)=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1)\quad(*)$$

коју ћемо користити у даљој изради задатка.
Радимо прво случај када је n непарно. Тада $p_i\neq 2\ \forall i=1,\dots,k$ па је канонска факторизација броја

$$2n=2p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

Па користећи формулу $(*)$ имамо

$$\varphi(2n)=2^{1-1}(1)p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1)=\varphi(n)$$

Ако је n парно, онда број n садржи фактор 2 па можемо претпоставити $p_1=2$ т.д. је $n=2^ap_2^{\alpha_2}\cdots p_k^{\alpha_k}$ канонска факторизација броја n. Па користећи опет формулу $(*)$

$$\varphi(n)=2^{a-1}(1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1)$$

Примјетимо сада да је канонска факторизација броја $2n=2^{a+1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ па добијамо

$$\varphi(2n)=2^{a+1-1}(1)p_2^{\alpha_2}\cdots p_k^{\alpha_k}=2\varphi(n)$$

□

(**Милена Јововић 1/19 Б**) задатак преузет са
`http://zimmer.csufresno.edu/~tkelm/teaching/math116/homework/hw6soln_116_s07.pdf`

321

Показати да ако једначина $\varphi(n)=k$ има тачно једно решење, онда $36\mid n$.

Доказ. Доказаћемо контрапозицију. Претпоставимо да $\varphi(n)=k$ и $36\nmid n$. Показаћемо да постоји још неки број m т.д. $\varphi(m)=k$.
Нека је $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ проста (канонска) факторизација броја n.

$$k=\varphi(n)=p_1^{\alpha_1-1}(p_1-1)p_2^{\alpha_2-1}(p_2-1)\cdots p_k^{\alpha_k-1}(p_k-1)$$

Прво примјетимо да ако је n непарно, користећи претходни задатак видимо да $\varphi(2n)=k$ чиме смо доказали контрапозицију.
Сада претпоставимо да је n парно. Онда можемо претпоставити да је $p_1=2$ па је $n=$

$2^a p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ канонска факторизација броја n.
Ако је $a = 1$, onda $\frac{n}{2} = p_2^{\alpha_2}\cdots p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ па је $\varphi(n) = \varphi(\frac{n}{2})$.
Претпоставимо да је $a \geq 2$. Ако број n нема фактор 3, онда је број $\tilde{n} = 2\cdot 3\cdot p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ различит од n и можемо израчунати да је $\varphi(\tilde{n}) = \varphi(n)$.
Сада претпоставимо да је $p_2 = 3$ т.д. $n = 2^a 3^b \cdots p_k^{\alpha_k}$ гдје $a \geq 2$, $b \geq 1$. Како b не може бити веће или једнако од 2, јер би у том случају $36 \mid n$ што не одговара нашој претпоставци, слиједи да је $b = 1$. Па је $n = 2^a 3\cdots p_k^{\alpha_k}$. Сада посматрајмо број $\hat{n} = 2^{a+1}\cdots p_k^{\alpha_k}$ (умјесто 3 смо додали 2). Тада, када израчунамо, добићемо $\varphi(\hat{n}) = \varphi(n)$.
Прошли смо кроз све могуће случајеве и коначно, показали да све док $36 \nmid n$ да постоји још неки број $m \neq n$ т.д. $\varphi(n) = \varphi(m)$.
Напомена: Задатак није гласио "ако и само ако", тј. у супротном смјеру не мора да важи. На примјер, $\varphi(36) = 12$ као и $\varphi(13) = 12$. ☐

(**Милена Јовович 1/19 Б**) задатак преузет са
`http://zimmer.csufresno.edu/~tkelm/teaching/math116/homework/hw6soln_116_s07.pdf`

322

Ако је p непаран прост број, помоћу Фермаове теореме показати да $x^2 \equiv -1 \pmod{p}$ има решење само ако је $p \equiv 1 \pmod{4}$.

Доказ. Претпоставимо да $a^2 \equiv -1 \pmod{p}$, одакле слиједи да $p \nmid a$ па из Фермаове теореме $1 \equiv a^{p-1} \equiv (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.
Како је p непаран прост број, $1 \not\equiv -1 \pmod{p}$, па $1 \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$ важи једино ако је $\frac{p-1}{2}$ паран број, тј. $\frac{p-1}{2} = 2k$ гдје је k позитивни цијели број. Одатле видимо да $p = 4k+1$, тј. $p \equiv 1 \pmod{4}$. ☐

(**Милена Јовович 1/19 Б**) задатак преузет са
`https://www.math.lsu.edu/~adkins/m4181/4181f19ps5a`

323

Ријешити систем

$$\begin{aligned} 2x &\equiv 5 \pmod{7} \\ 4x &\equiv 2 \pmod{6} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

Доказ. Прво ћемо ријешити сваку конгруенцију појединачно, а онда ћемо искористити Кинеску теорему о остацима да ријешимо систем.
Прво посматрамо $2x \equiv 5 \pmod{7}$. Како је $4\cdot 2 = 8 \equiv 1 \pmod{7}$, прва конгруенција има решење $x \equiv 4\cdot 5 \equiv -1 \pmod{7}$.
Сада посматрајмо конгруенцију $4x \equiv 2 \pmod{6}$. Како је нзд$(4,6) = 2$ и $2 \mid 2$, постоје 2

решења конгруенције. Прво решење је

$$\begin{aligned}
&4x \equiv 2 \pmod 6\\
&2x \equiv 1 \pmod 6\\
&-x \equiv 1 \pmod 6\\
&x \equiv -1 \pmod 6
\end{aligned}$$

Друго решење је $-1 + (\frac{6}{2})k \pmod 6$, тј. $-1 + 3 = 2 \pmod 6$.
Трећа конгруенција је већ дата у форми решења.
Дакле, имамо два система конгруенција да ријешимо.

$$\begin{array}{lcl}
x \equiv -1 \pmod 7 & & x \equiv -1 \pmod 7\\
x \equiv -1 \pmod 6 & \text{и} & x \equiv 2 \pmod 6\\
x \equiv 3 \pmod 5 & & x \equiv 3 \pmod 5
\end{array}$$

Како $\text{нзд}(7, 6) = \text{нзд}(7, 5) = \text{нзд}(6, 5) = 1$, можемо примјенити Кинеску теорему о остацима.

$$\begin{aligned}
(6 \cdot 5)x = 30x &\equiv 1 \pmod 7\\
(7 \cdot 5)x = 35x &\equiv 1 \pmod 6\\
(7 \cdot 6)x = 42x &\equiv 1 \pmod 5
\end{aligned}$$

Ријешавамо прву конгруенцију

$$\begin{aligned}
&30x \equiv 1 \pmod 7\\
&2x \equiv 1 \pmod 7\\
&x \equiv 4 \pmod 7
\end{aligned}
\qquad
\begin{aligned}
&35x \equiv 1 \pmod 6\\
&5x \equiv 1 \pmod 6\\
&-x \equiv 1 \pmod 6\\
&x \equiv -1 \pmod 6
\end{aligned}
\qquad
\begin{aligned}
&42x \equiv 1 \pmod 5\\
&2x \equiv 1 \pmod 7\\
&x \equiv 3 \pmod 5
\end{aligned}$$

Па добијамо да први систем конгруенција има решење

$$\begin{aligned}
x_1 &= 30 \cdot 4 \cdot (-1) + 35 \cdot (-1) \cdot (-1) + 42 \cdot 3 \cdot 3 =\\
&= -120 - 35 + 378 = 293\\
&\equiv 83 \pmod{210}
\end{aligned}$$

А други систем има решење

$$\begin{aligned}
x_2 &= 30 \cdot 4 \cdot (-1) + 35 \cdot (-1) \cdot 2 + 42 \cdot 3 \cdot 3 =\\
&= -120 - 70 + 378 = 293\\
&\equiv 188 \pmod{210}
\end{aligned}$$

Дакле, два решења почетног система конгруенција су 83 и 188 $\pmod{210}$.

□

(**Милена Јововић 1/19 Б**) задатак преузет са
`https://www.math.lsu.edu/~adkins/m4181/4181f19ps5a`

324

Низ природних бројева $(a_n)_{n\in N}$ дефинисан је са $a_1 = 3$ и $a_{n+1} = 3^{a_n}$, $n \geq 1$. Одредити посљедње двије цифре бројева a_{2013} и a_{2014}.

Доказ. Подсјетимо се појма Ојлерове функције:
За произвољан природан број $n > 1$, Ојлерова функција $\varphi(n)$ означава број свих природних бројева мањих од n који су узајамно прости са n.
Нека је n природан број и p_1, p_2,…,p_k прости бројеви који се појављују у растављању броја n на просте чиниоце, при чему се број p_1 појављује α_1 пута, p_2 α_2 пута,…, p_k α_k пута. Тада је

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}.$$

Такође, може се показати да ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја n, тада је

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Ојлерова теорема има сљедећу формулацију:
Нека је $a \in Z$, и $m > 0$ тако да је НЗД(a,m)=1. Тада је $a^{\varphi(m)} \equiv 1 \pmod{m}$.
Како је НЗД(3,4)=1 и НЗД(3,25)=1, по Ојлеровој теореми имамо да је $3^2 \equiv 1 \pmod 4$ и $3^{20} \equiv 1 \pmod{25}$, па је $3^{20} \equiv 1 \pmod{100}$. Из $a_1 = 3$ и $a_2 = 3^3$ слиједи да је

$$a_3 = 3^{a_2} = 3^{27} = 3^{20} \cdot 3^7 \equiv 1 \cdot 37 \pmod{100} \equiv 81 \cdot 27 \pmod{100} \equiv 87 \pmod{100}$$

Ако је $a_n \equiv 87 \pmod{100}$, тада је $a_n = 100k + 87 = 20(5k + 4) + 7$, одакле је

$$a_{n+1} = 3^{a_n} = 3^{100k+87} = (3^{20})^{5k+4} \cdot 3^7 \equiv 3^7 \pmod{100} \equiv 87 \pmod{100}$$

Дакле, $a_n \equiv 87 \pmod{100}$, за $n \geq 3$. Бројеви a_{2013} и a_{2014} се завршавају цифрама 87. ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`https://www.pmf.ni.ac.rs/mii-content/2014/Broj%202014%20u%20zanimljivim%20zadacima.pdf`

325

Да ли конгруенције:
(1) $x^2 \equiv 68 \pmod{113}$
(2) $x^2 \equiv 310 \pmod{521}$
(3) $x^2 + 174 \equiv 0 \pmod{619}$
имају решења ?

Доказ. 1) Примијетимо најприје да су бројеви 113,521,619 прости.
Примјеном теорема 1. и 2. имамо да је:
$\frac{68}{113} = (\frac{2}{113})^2(\frac{17}{113})$ према теореми 1.2,јер је $68 = 2^2 \cdot 17$

$= \frac{113}{17}$ јер је $(\frac{2}{113})^2 = 1$ и према теореми 2

$= (\frac{17}{113})(\frac{113}{17}) = (-1)^{\frac{17-1}{2}\cdot\frac{113-1}{2}} = 1$

$= (\frac{11}{17})$, према теореми 1.1 ,јер је $113 \equiv 11 \pmod{17}$

$= (\frac{17}{11})$, према теореми 2 је $= (\frac{11}{17})(\frac{17}{11}) = 1$

$= (\frac{6}{11})$ јер је $17 \equiv 6 \pmod{11}$

$= (\frac{2}{11})(\frac{3}{11})$ јер је $6 = 2 \cdot 3$

$= (-\frac{3}{11})$ према теореми 1(5)

$= (\frac{2}{11}) = (-1)^{\frac{11^2-1}{8}} = -1$

$= (\frac{11}{3})$ јер је $= (\frac{3}{11})(\frac{11}{3}) = 1$

$= (\frac{2}{3})$ јер је $11 \equiv 2 \pmod{3}$

$= -1,$
одакле слиједи да дата конгруенција нема решења.
2)Из једнакости

$$(\frac{310}{521}) = (\frac{2}{521})(\frac{5}{521})(\frac{31}{521})$$
$$= (\frac{521}{5})(\frac{521}{31})$$
$$= (\frac{1}{5})(\frac{25}{31}) = (\frac{5^2}{31}) = 1,$$

слиједи да дата конгруенција има два решења.
3)Из једнакости

$$(\frac{-174}{619}) = (\frac{-1}{619})(\frac{2}{619})(\frac{3}{619})(\frac{29}{619})$$
$$= (\frac{3}{619})(\frac{29}{619}) = -(\frac{619}{3})(\frac{619}{29})$$
$$= (-\frac{1}{3})(\frac{10}{29}) = -(\frac{2}{29})(\frac{5}{29})$$
$$= (\frac{29}{5}) = (\frac{2^2}{5}) = 1,$$

одакле слиједи да дата конгруенција нема решења.

Теореме коришћене у овом задатку:
Теорема 1. Нека је p непаран прост број.
(1)Ако су a и b цијели бројеви узајамно прости са p такви да је $a \equiv b \pmod{p}$ тада је

$$(\frac{a}{p}) = (\frac{b}{p})$$

(2)Ако су $a_1, a_2, \ldots, a_n$ цијели бројеви такви да је $(a_i, p) = 1, i = 1, 2, .., n$ при чему је p непаран прост број,тада је:

$$(\frac{a_1, a_2, \ldots, a_n}{p}) = (\frac{a_1}{p})(\frac{a_2}{p}) \ldots (\frac{a_n}{p}).$$

(3) Ако је a цијели број узајамно прост са непарним простим бројем p ,тада важи

$$(\frac{a^2}{p}) = 1$$

(4) $(\frac{-1}{p}) = \begin{cases} +1, \text{ако је} p \equiv 1 \pmod 4 \\ -1, \text{ако је} p \equiv 3 \pmod 4 \end{cases}$

(5) $(\frac{2}{p}) = (-1)^{(\frac{p^2-1}{8})}$

Теорема 2(Гаусов закон реципроцитета) Нека су p и q различити непарни прости бројеви. Ако су p и q оба облика $4k + 3$,онда је једна од једначина:

$$x^2 \equiv p \pmod q, x^2 \equiv q \pmod p$$

рјешива, а друга није. Ако p и q нису оба облика $4k + 3$ тада су или обје једначине рјешиве или ниједна није,или еквивалентн,за непарне и различите просте бројеве p и q важи:
$(\frac{p}{q})(\frac{q}{p}) = \begin{cases} -1, \text{ако је} p \equiv 3 \pmod 4 q \equiv 3 \pmod 4 \\ 1, \text{ако је} p \equiv 1 \pmod 4 q \equiv 1 \pmod 4 \end{cases}$
тј.

$$(\frac{p}{q}) \cdot (\frac{q}{p}) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

□

(**Јелена Недовић 02/19 Ц**)

326 ●●●●

Наћи све природне бројеве који имају тачно 16 дјелилаца (укључуујући и сам тај број) тако да је збир свих делилаца једнак 4032.

Доказ. $4302 = 2^6 \cdot 3^2 \cdot 7$
Ако број има тачно 16 дјелилаца,онда он има један од следећих факторизација:
$p^{15}, p^7q, p^3q^3, p^3qr, pqrs$ гдје су p, q, r, s различити прости бројеви. Збир свих дјелилаца (који је једнак $4302 = 2^6 \cdot 3^2 \cdot 7$) у сваком од ових случајева је:
$1 + p + p^2 \cdots + p^{15} = (1 + p)(1 + p^2)(1 + p^4)(1 + p^8)$;
$(1 + p + p^2 ... + p^7)(1 + q) = (1 + p)(1 + p^2)(1 + p^4)(1 + q)$;
$(1 + p + p^2 + p^3)(1 + q + q^2 + q^3) = (1 + p)(1 + p^2)(1 + q)(1 + q^2)$;
$(1 + p + p^2 + p^3)(1 + q)(1 + r) = (1 + p)(1 + p^2)(1 + q)(1 + r)$;
$(1 + p)(1 + q)(1 + r)(1 + s)$.

Фактор $1+p^2$ јавља се у прва четири случаја. Пошто број тог облика није дјељив са 3,4 или 7 ови бројеви не воде решењу.
Не умањујући општост,можемо претпоставити да важи $p<q<r<s$.
Запишимо редом просте бројеве:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots$$

Тада број 4032 треба написати као производ четири броја из низа:

$$3, 4, 6, 8, 12, 14, 18, 20, 24, 30, 32, 38, 42, \ldots$$

(1) Нека је $1+p=3$. Онда је $(1+q)(1+r)(1+s)=2^6\cdot 3\cdot 7$.
Ако је $1+q=4$,тада је $(1+r)(1+s)=2^4\cdot 3\cdot 7$. Како је

$$2^4\cdot 3\cdot 7=6\cdot 56=8\cdot 42=12\cdot 28=14\cdot 24$$

то постоје двије могућности $2\cdot 3\cdot 7\cdot 41=1722$ и $2\cdot 3\cdot 13\cdot 23=1794$.
Ако је $1+q=6$,тада је $(1+r)(1+s)=2^5\cdot 7$. Како је

$$2^5\cdot 7=8\cdot 28=14\cdot 16,$$

то у овом случају нема решења.
Ако је $1+q=8$,тада је $(1+r)(1+s)=2^3\cdot 3\cdot 7$. Пошто је $2^3\cdot 3\cdot 7=12\cdot 14$ имамо решење $2\cdot 7\cdot 11\cdot 13=2002$.

(2)Нека је $1+p=4$. Тада је $(1+q)(1+r)(1+s)=2^4\cdot 3^2\cdot 7$.
Ако је $1+q=6$,тада је $(1+r)(1+s)=2^3\cdot 3\cdot 7$.
Пошто је $2^3\cdot 3\cdot 7=8\cdot 21=12\cdot 14$ добијамо решење $3\cdot 5\cdot 11\cdot 13=2145$.
Ако је $1+q\geq 8$, тада је $(1+q)(1+r)(1+s)\geq 8\cdot 12\cdot 14>2^4\cdot 3^2\cdot 7$,
што значи да у овом случају нема решења.
Даље, пошто је $6\cdot 8\cdot 12\cdot 14>2^6\cdot 3^2\cdot 7$, то нема других решења.
Према томе,постоје четири природна броја која задовољавају услове задатка :
1722,1794 ,2002 и 2145. $\square$

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

327

Одредити цифре x и y тако да број $1993xy$ буде дјељив и са 9 и са 8.

Доказ. Како је дати број дјељив са 9,то је и збир његових цифара дјељив са 9,тј. треба да важи $9\mid 4+x+y$.
То је могуће само у два случаја: ако је $x+y=5$ или $x+y=14$.
Дати број може се написати у облику

$$199300+10x+y=8\cdot 24912+4+8x+2x+y$$

а он је дјељив са 8 ако и само ако $8\mid 2x+y+4$. У првом случају,када је $x+y=5$, да би број $2x+y+4=x+9$ био дјељив са 8, мора бити $x=7$,што је немогуће јер $x+y=7+y=5$, а

y је цифра.
Дакле,преостаје други начин када $x+y=14$. Тада је $2x+y+4=x+18$ дјељиво са 8 једино ако је $x=6$, а онда је $y=8$. Тражени број је 199368. □

(**Јелена Недовић 02/19 Ц**) задатак преузет са
`http://www.matf.bg.ac.rs/p/files/43-VEZBE_Prvi_deo.pdf`

328

Доказати да не постоје цијели бројеви x и y такви да је $x^2+y^2=2006$.

Доказ. Збир бројева x^2 и y^2 је 2006, дакле паран, па се разликују само два случаја, јер случај да су x и y различите парности немогућ, пошто би тада збир x^2+y^2 био непаран.

1) Ако су бројеви x и y парни, онда постоје цијели бројеви k и l такви да је $x=2k$ и $y=2l$. Тада је $4k^2+4l^2=2006$. Како је лијева страна једначине дјељива са 4, а десна није, то једначина у овом случају нема рјешења.

2) У случају да су бројеви x и y непарни, онда постоје цијели бројеви k и l такви да је $x=2k+1$ и $y=2l+1$. Тада је $4k^2+4k+1+4l^2+4l+1=2006$, односно $4k^2+4k+4l^2+4l=2004$. Упрошћавањем једначине добија се $k(k+1)+l(l+1)=501$. Како је с лијеве стране једначине увијек паран број, а с десне непаран, то једначина ни у овом случају нема рјешења.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет из Мала збирка Диофантових једначина , В.Андрић

329

Одредити најмањи и највећи природан број чије су све цифре различите, ако је производ цифара тог броја 720.

Доказ. Најмањи број је онај који се може направити са што мање цифара. Како је $720=2^4\cdot 3^2\cdot 5$, то најмањи број не може бити троцифрен, јер се ни 5 ни 9 не могу комбиновати са 2. Према томе најмањи такав број је 2589.

Највећи је онај број који има што више цифара, а такав је број чије су цифре 1, 2, 3, $2\cdot 2$, 5, $2\cdot 3$, дакле број 654321.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет из Мала збирка Диофантових једначина , В.Андрић

330

●●●●

Постоји ли двоцифрен број који је једнак збиру своје цифре десетица и квадрата цифре јединица?

Доказ. Нека је тражени двоцифрени природан број xy.

Тада је:

$$10x + y = x + y^2$$

Дакле:

$$9x = y^2 - y = y(y-1)$$

Како су бројеви $y-1$ и y узастопни, они су и узајамно прости, што значи да немају заједничких дјелилаца.

Пошто је лијева страна једнакости дјељива са 9, то је са 9 дјељив или број y или $y-1$.

Дакле или је $y = 9$ или $y-1 = 9$, односно $y = 10$. Други случај отпада, па као потенцијално y остаје само $y = 9$.

Тада је:

$$9x = y(y-1) = 9 \cdot 8$$

што значи да је $x = 8$. Тражени двоцифрени број је $89 = 8 + 9^2$.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет из Мала збирка Диофантових једначина , В.Андрић

331

●●●●

Одредити све природне бројеве x такве да је $2^x + 1$ квадрат природног броја.

Доказ. Ако је:

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

онда је

$$y^2 - 1 = (y+1)(y-1) = 2^x$$

.

Једини чиниоци броја 2^x су степени броја 2.

Нека је $2^x = 2^a \cdot 2^b (a \geqslant b)$, гдје је $a + b = x$.

Тада је $y + 1 = 2^a$ и $y - 1 = 2^b$, па је $2^a - 2^b = 2$.

Слиједи да је

$$2^b(2^{a-b} - 1) = 2.$$

Јасно је да је $2^b = 2$ и $2^{a-b} - 1 = 1$,

па је $b = 1$ и $a - b = 1$.

Дакле $a = 2$ и $b = 1$ и $x = a + b = 3$.

Према томе је $2^3 + 1 = 9 = 3^2$, па је $y = 3$. □

(**Андрија Бошковић 14/19 Б**) задатак преузет из Мала збирка Диофантових једначина , В.Андрић

332

Риjешити jедначину $x(x+1)(x+7)(x+8)=y^2$ у скупу циjелих бројева.

Доказ. Погодним множењем израза добија се да је дата једначина еквивалентна са једначином

$$(x^2+8x)(x^2+8x+7)=y^2$$

Множењем са 4 добија се

$$(2x^2+16x+7-7)(2x^2+16x+7+7)=4y^2,$$

а даљом трасформацијом

$$(2x^2+16x+7)^2-49=4y^2,$$

па је

$$(2x^2+16x+7)^2-(2y)^2=49.$$

Одавде се добија производ

$$(2x^2+16x+7-2y)(2x^2+16x+7+2y)=49.$$

Разликују се сљедећи случајеви:
$2x^2+16x+7-2y=1$ и $2x^2+16x+7+2y=49$
$2x^2+16x+7-2y=7$ и $2x^2+16x+7+2y=7$
$2x^2+16x+7-2y=49$ и $2x^2+16x+7+2y=1$
$2x^2+16x+7-2y=-1$ и $2x^2+16x+7+2y=-49$
$2x^2+16x+7-2y=-7$ и $2x^2+16x+7+2y=-7$
$2x^2+16x+7-2y=-49$ и $2x^2+16x+7+2y=-1$
Из добијених система једначина слиједе сљедећи системи квадратних, односно линеарних једначина:
$4x^2+32x+14=50$ и $4y=48$ или $x^2+8x-9=0$ и $y=12$
$4x^2+32x+14=14$ и $4y=0$ или $x^2+8x=0$ и $y=0$
$4x^2+32x+14=50$ и $4y=-48$ или $x^2+8x-9=0$ и $y=-12$
$4x^2+32x+14=-50$ и $4y=-48$ или $x^2+8x+16=0$ и $y=-12$
$4x^2+32x+14=-14$ и $4y=0$ или $x^2+8x+7=0$ и $y=0$
$4x^2+32x+14=-50$ и $4y=48$ или $x^2+8x+16=0$ и $y=12$
Сва рјешења дате Диофантове једначине су: (-9,12),(1,12),(0,0),(-8,0),(-9,-12),(1,-12),(-4,-12),(-7,0),(-1,0),(-4,12). □

(**Андрија Бошковић 14/19 Б**) задатак преузет из Мала збирка Диофантових једначина , В.Андрић

333

Доказати: ако је p прост број и α је позитиван цио број, онда

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1},$$

а затим израчунај:
а) $\varphi(32)$
б) $\varphi(125)$.

Доказ. Желимо да израчунамо број ненегативних цијелих бројева који су мањи од $n = p^\alpha$ такви да су узајамно прости са n. Као и у многим случајевима, испоставља се да је лакше да се израчуна број оних цијелих бројева који **нису** узајамно прости са n, па се тражени број добија одузимањем овог броја од укупног.
Набројимо ненегативне цијеле бројеве мање од p^α: $0, 1, 2, \cdots, p^\alpha - 1$. Има их p^α. Број оних који имају заједничке дјелиоце са p^α (оних који нису узајамно прости са n) су садржаоци од p: 0, p, 2p,..., тј. сваки $p-$ти број. Зато је $\frac{p^\alpha}{p} = p^{\alpha-1}$ бројева у овом низу, па је

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

$\varphi(32) = \varphi(2^5) = 2^5 - 2^{5-1} = 32 - 16 = 16$
$\varphi(125) = \varphi(5^3) = 5^3 - 5^{3-1} = 125 - 25 = 100.$ ☐

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`https://www.whitman.edu/mathematics/higher_math_online/section03.08.html`

334

Да ли постоји неки природан број који при дијељењу са 1001 даје остатак 23,а при дијељењу са бројем 1170 даје остатак 42?

Доказ. Када би постојао природан број n са овим својством,онда би морало да важи:

$$n = 1001x + 23$$

$$n = 1170y + 42,$$

тј.

$$n = 1001x - 1170y = 19$$

Дакле проблем се своди на рјешавање ове Диофантове једначине. Уколико она има решења такав број постоји и можемо наћи ког су облика ти бројеви, а уколико једначина нема решења природан број са овим својствима не постоји.
Провјеравамо да ли ова Диофантова једначина има решења. Тражимо $NZD(1170, 1001)$:

$$1170 = 10001 \cdot 1 + 169$$

$$1001 = 169 \cdot 5 + 156$$

$$169 = 156 \cdot 1 + 13$$

$$156 = 13 \cdot 12$$

закључујемо да је $NZD(1170, 1001) = 13$. Како $13 \nmid 19$ слиједи да једначина нема решења, тј. да не постоји природан број n са овим својствима. Решење је коректно јер смо задатак свели на рјешавање Диофантове једначине, а она заиста нема рјешења уколико $NZD(1170, 1001) \nmid 19$. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са `http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

335

Нека су $d_1, d_2, \ldots, d_k$ сви дјелиоци природног броја n,такви да је $1 = d_1 < d_2 < \ldots < d_k = n$. Наћи све просте бројеве n за које је $k \leq 4$ и важи

$$d_1^2 + d_2^2 + d_3^2 + d_4^2 = n$$

Доказ. Прво је потребно доказатии да је n паран број. Претпоставимо супротно; нека је n непаран број. Тада су сви дјелиоци броја n непарни,па су зато d_1, d_2, d_3, d_4 непарни. Међутим тада је број $n = d_1^2 + d_2^2 + d_3^2 + d_4^2$ паран,што је противно полазној претпоставци. Како је n паран број,то је $d_2 = 2$. Из једнакости

$$1^2 + 2^2 + d_3^2 + d_4^2 = n$$

слиједи да је један од бројева d_3 и d_4 паран,а други непаран. Размотрићемо два случаја. (1)$d_3 = 2a, a > 1$. Како је a дјелилац броја n мањи од d_3,то је $a = 2$. Дакле,$d_3 = 4$. Како је

$$n = 1^2 + 2^2 + 4^2 + d_4^2 = 21 + d_4^2,$$

то n није дјељиво са $4 = d_3$ (квадрати непарних бројева при дијељењу са 4 дају остатак 1,а број облика $4k + 22$ није дјељив са 4). Контрадикција!

(2) $d_4 = 2, a > 1$. Како је $a < d_4$ и $a \mid n$,то је $a = d_2 = 2$ или је $a = d_3$.
У првом случају би било
$d_4 = 4, d_3 = 3$ и $n = 1^2 + 2^2 + 3^2 + 4^2 = 30$.
Како $4 \nmid 30$ овај случај отпада. Преостаје да је $a = d_3$. У том случају имамо да је

$$n = 1^2 + 2^2 + d_3^2 + 4d_3^2 = 5(1 + d_3^2)$$

Како $d_3 \mid n$ и како су бројеви d_3 и $1 + d_3^2$ узајамно прости, то је $d_3 = 5$. Слиједи да је $d_4 = 10$ и $n = 1^2 + 2^2 + 5^2 + 10^2 = 130$.
Дакле,једини број који задовољава дати услов је 130. ☐

(**Јелена Недовић 02/19 Ц**) задатак преузет са `http://www.matf.bg.ac.rs/p/files/43-teor_brojeva3_online.pdf`

336

Ријешити једначине:
а) $\varphi(7^x) = 294$,
б) $\varphi(3^x 5^y) = 360$, гдје су $x, y \in Z$.

Доказ. а) Број 7 је прост, а x је цио број, па можемо да примијенимо теорему која је раније у **секцији 4** доказана:

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1},$$

гдје је $p-$прост број, а $\alpha-$позитиван цијели број.
Користећи поменуту теорему имамо:

$$\varphi(7^x) = 7^x - 7^{x-1} = 7^{x-1}(7-1) = 7^{x-1} \cdot 6 = 294$$

$$7^{x-1} = 49$$

$$7^{x-1} = 7^2,$$

па је $x - 1 = 2$, односно $x = 3$.
б) Да бисмо ријешили другу једначину користићемо својство хомоморфизма Ојлерове функције, односно:
Ако су a и b релативно прости и $a \cdot b = n$, onda важи:

$$\varphi(n) = \varphi(a \cdot b) = \varphi(a) \cdot \varphi(b).$$

Зато имамо:

$$\varphi(3^x 5^y) = \varphi(3^x) \cdot \varphi(5^y) = 360$$

Користећи теорему поменуту у задатку под а) добијамо:

$$\varphi(3^x) \cdot \varphi(5^y) = (3^x - 3^{x-1})(5^y - 5^{y-1}) = 360$$

$$3^{x-1}(3-1) \cdot 5^{y-1}(5-1) = 3^{x-1} \cdot 2 \cdot 5^{y-1} \cdot 4 = 360$$

$$8 \cdot 3^{x-1} 5^{y-1} = 360$$

$$3^{x-1} 5^{y-1} = 45$$

Растављањем на просте чиниоце број 45 добијамо:
$45 = 3^2 \cdot 5$. Када уврстимо ову једначину у претходну, добијамо:

$$3^{x-1} 5^{y-1} = 3^2 \cdot 5.$$

Изједначавајући степене бројева 3 и 5 са лијеве и десне стране, добијамо:

$$x = 3, y = 2,$$

што је рјешење једначине. □

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://kvant.mccme.ru/pdf/2000/01/kv0100senderov.pdf`

337

Одредити највећи природан број k такав да постоји природан број $n \geq k$ за који је сваки од бројева $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{k}$ потпун квадрат.

Доказ. За $k = 2$ и $n = 9$ сваки од датих бројева тј. $\binom{9}{0} = 1, \binom{9}{1} = 9, \binom{9}{2} = 36$ је потпун квадрат. Докажимо да је $k = 2$ највећи број са датом особином. Претпоставимо супротно тј. да постоји $n \geq k \geq 3$ такво да је сваки од бројева $\binom{n}{0}, \binom{n}{1}, \binom{n}{2}$ и $\binom{n}{3}$ потпун квадрат. Нека је

$$a^2 = n, \quad b^2 = \binom{n}{2} = \tfrac{n(n-1)}{2}, \quad c^2 = \binom{n}{3} = \tfrac{n(n-1)(n-2)}{6}$$

Из $a^2(n-1) = 2b^2$ добијамо да $a \mid b$ и $n-1$ је паран број. Аналогно, из $b^2(n-2) = 3c^2$ добијамо да $b \mid c$ и $n-2$ је дјељив са 3. Дакле, n даје остатак 1 при дијељењу са 2, и остатак 2 при дијељењу са 3, па је $n = 6s + 5$ за неки цијели број s. Даље замјеном у једнакост $a^2(n-1) = 2b^2$ налазимо да је $a^2(3s+2) = b^2$ па је $3s+2$ потпун квадрат, што није могуће. Дакле, $k = 2$ је највећи број са датом особином.

□

(**Александар Вујовић 4/19 Б**) задатак преузет са `https://imomath.com/srb`

338

Доказати да је број $\operatorname{tg}(17^{3^{2012}})^\circ$ ирационалан.

Доказ. Одредимо остатак при дијељењу броја $17^{3^{2012}}$ са 180. Примијетимо да је $17^2 \equiv 109 \pmod{180}$, па је $17^4 \equiv 109^2 \equiv 1 \pmod{180}$. Како је $3^{2012} \equiv 1 \pmod 4$ (јер је $3^4 \equiv 1 \pmod 4$), то је према претходном $17^{3^{2012}} \equiv 17 \pmod{180}$, па је $\operatorname{tg}(17^{3^{2012}})^\circ = \operatorname{tg}(17)^\circ$. Дакле, довољно је доказати да је $\operatorname{tg}(17)^\circ$ ирационалан број.
Претпоставимо супротно, тј. $\operatorname{tg}(17)^\circ$ је рационалан број. Како је

$$\operatorname{tg}(\alpha+\beta) = \tfrac{\operatorname{tg}\alpha + \operatorname{tg}\beta}{1 - \operatorname{tg}\alpha \cdot \operatorname{tg}\beta},$$

то из чињенице да су $\operatorname{tg}\alpha$, $\operatorname{tg}\beta$ рационални бројеви слиједи и $\operatorname{tg}(\alpha+\beta)$ је рационалан број. Самим тим из дате претпоставке, индукцијом слиједи да је $\operatorname{tg}(n \cdot 17)^\circ$ рационалан број за сваки природан број n такав да $90 \nmid n$. За $n = 5$ закључујемо да је $\operatorname{tg}(85)^\circ$ рационалан број па је и $\operatorname{tg}(5)^\circ = \frac{1}{\operatorname{tg}(85)^\circ}$ рационалан. Слично претходном, сада је и $\frac{1}{\sqrt{3}} = \operatorname{tg}(30)^\circ = \operatorname{tg}(6 \cdot 5)^\circ$ рационалан број. Контрадикција. Дакле, број $\operatorname{tg}(17^{3^{2012}})^\circ$ је ирационалан. □

(**Александар Вујовић 4/19 Б**) задатак преузет са `https://imomath.com/srb`

339

Користећи Ојлерову теорему и кинеску теорему о остацима, наћи остатак при дијељењу броја 5^{509} са 1323.

Доказ. Заправо рјешавамо једначину $x \equiv 5^{509} \pmod{1323}$.
Обзиром на то да је $1323 = 27 \cdot 49$, а да је нзд$(27, 49) = 1$, то је дата једначина еквивалентна систему:
$$\begin{cases} x \equiv 5^{509} \pmod{27} \\ x \equiv 5^{509} \pmod{49} \end{cases} \iff \begin{cases} x \equiv 5^{5} \pmod{27} \\ x \equiv 5^{5} \pmod{49} \end{cases} \iff \begin{cases} x \equiv 20 \pmod{27} \\ x \equiv 38 \pmod{49} \end{cases}$$
У претходним корацима смо упростили систем користећи Ојлерову теорему и својства модуларне аритметике. Посљедњи систем ћемо рјешавати користећи кинеску теорему о остацима. Ми смо "намјестили"да посматрамо дијељење са 27 и 49, који су узајамно прости, па је први услов кинеске теореме задовољен. Сљедећи корак је формирање коефицијената m и n_j, $j \in 1, 2$.
$m = m_1 \cdot m_2$
$n_j = \frac{m}{m_j}, j \in 1, 2$, гдје су $m_1 = 27$ и $m_2 = 49$. Добијамо да је $n_1 = 49$ и $n_2 = 27$.

$$49x_1 \equiv 1 \pmod{27} \iff x_1 \equiv 16 \pmod{27}$$
$$27x_2 \equiv 1 \pmod{49} \iff x_2 \equiv 20 \pmod{49}.$$

Одавде слиједи да је:

$$x \equiv 20 \cdot 16 \cdot 49 + 38 \cdot 20 \cdot 27 = 20 \cdot 1810 \equiv 479 \pmod{1323},$$

односно, 479 је тражени резултат. □

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://www.uni.bsu.by/arrangements/inputinmath/themes/theme1.pdf`

340 ●●●●

Ако су a, k, $m-$природни бројеви, $a > 1$, тада $a^m - 1$ је дјељиво са $a^k - 1$ ако и само ако је m дјељиво са k.

Доказ. Смјер $(\Longleftarrow)$:
Ако је $m = kn$, то важи:

$$a^m - 1 = (a^k - 1)(a^{k(n-1)} + a^{k(n-2)} + \ldots + a^k + 1).$$

Показали смо један смјер.
Смјер ($\Longrightarrow$):
Овај смјер ћемо доказати контрапозицијом.
Обрнуто, ако m није дјељиво са k, онда је:

$$m = kn + r, 0 < r < k,$$

У овом случају разматрамо једнакост:

$$a^{kn+r} - 1 = a^{kn+r} - a^r + a^r - 1 = a^r(a^{kn} - 1) + (a^r - 1).$$

Број $a^r - 1$ није дјељив са $a^k - 1$, зато што $0 < a^r - 1 < a^k - 1$. Тврђење доказано. □

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`file:///C:/Users/Lazar/Desktop/kriptografija%20zbirke%20zadataka/kv0300senderov.pdf`

341

Наћи остатак при дијељењу 3^{10^5} са 35.

Доказ. Како је нзд$(3, 35) = 1$, на основу Ојлерове теореме, слиједи

$$3^{\varphi(35)} \equiv 1 \pmod{35}$$

$$\varphi(35) = \varphi(7) \cdot \varphi(5) = 6 \cdot 4 = 24$$

$$10^5 = 10000 = 24 \cdot 4166 + 16,$$

одавде слиједи

$$3^{10^5} \equiv (3^{24})^{4166} \cdot 3^{16} \pmod{35}.$$

Како је

$$\begin{aligned} 3^{24} \equiv 1 \pmod{35} &\implies 3^{10^5} \equiv 3^{16} \pmod{35} \\ 3^4 \equiv 11 \pmod{35} &\implies 3^{16} \equiv 11^4 \pmod{35} \\ 11^2 \equiv 16 \pmod{35} &\implies 11^4 \equiv 15^2 \pmod{35} \\ 16^2 \equiv 11 &\pmod{35}. \end{aligned}$$

Дакле, остатак је 11. □

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4790/masSarcevic_Petra.pdf?sequence=1`

342

Нека је n цио број. Доказати: ако је број

$$2 + 2\sqrt{28n^2 + 1}$$

природан, онда је он потпун квадрат.

Доказ. Претпоставимо да је

$$2 + 2\sqrt{28n^2 + 1} = 2(1 + \sqrt{28n^2 + 1}) = m,$$

за неки природан број m. Тада је $\sqrt{28n^2 + 1}$ непаран природан број, одакле слиједи да m мора бити дјељив са 4, тј. $m = 4k$ за неко $k \in \mathbb{N}$. Уврштавајући ово у горњу једнакост, добијамо $\sqrt{28n^2 + 1} = 2k - 1$, одакле квадрирањем слиједи $28n^2 + 1 = 4k^2 - 4k + 1 = 4k(k - 1) + 1$, односно

$$7n^2 = k(k - 1).$$

Будући да је нзд$(k, k-1) = 1$, постоје цијели бројеви q, r тако да важи једна од двије могућности:

1. $k = q^2, k-1 = 7r^2$,

2. $k = 7q^2, k-1 = r^2$.

У случају (1) тражени закључак непосредно слиједи, пошто је тада

$$m = 4k = 4q^2 = (2q)^2.$$

С друге стране, случај (2) је немогућ, пошто бисмо тада имали $r^2 = 7q^2 - 1$, што би значило да важи $r^2 \equiv -1 \pmod 7$. Међутим, лако се провјерава да квадрати цијелих бројева дају остатке $0, 1, 2, 4$ при дијељењу са 7.

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

343 ●●●●

Доказати да за све природне бројеве m постоји природан број $n > m$ такав да се декадни запис броја 5^n добија дописивањем цифара извјесног броја с лијева декадном запису броја 5^m.

Доказ. Услов задатка се може записати као $10^r \mid (5^n - 5^m)$, гдје је r број цифара у декадном запису броја 5^m, тј. $r = \left\lfloor \log_{10} 5^m \right\rfloor + 1$. Пошто је $r \leq m$, посматрана релација дјељивости је еквивалентна са $2^r \mid (5^n - 5^m) = 5^m(5^{n-m} - 1)$, тј. са

$$2^r \mid (5^{n-m} - 1).$$

По Ојлеровој теореми, важи:

$$5^{\varphi(2^r)} \equiv 1 \pmod{2^r}.$$

Али, тада је очигледно да се за n облика

$$n = m + \varphi(2^r)k = m + 2^{r-1}k,$$

$k \in \mathbb{N}$, добијамо

$$5^n = 5^m (5^{\varphi(2^r)})^k \equiv 5^m \pmod{2^r},$$

и тиме је доказ завршен.

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

344

Доказати да не постоји природан број n такав да $6^n - 1 \mid 7^n - 1$.

Доказ. Будући да $6^n - 1 \mid 7^n - 1$ слиједи да $6 - 1 = 5 \mid 7^n - 1$. Задња цифра броја 7^n за $n \in \mathbb{N}$ може бити редом $7, 9, 3, 1, 7, \ldots$ па ће број $7^n - 1$ бити дјељив са 5 ако и само ако је $n = 4k$ за неко $k \in \mathbb{N}$.

Сада испитујемо за које $k \in \mathbb{N}$ важи $6^{4k} - 1 \mid 7^{4k} - 1$. Будући да је

$$6^{4k} - 1 = (6^{2k} - 1)(62k + 1) = (36^k - 1)(6^{2k} + 1) = 35 \cdot m,$$

за неко $m \in \mathbb{N}$, слиједи да $35 \mid 7^{4k} - 1$, тј. $7 \mid 7^{4k} - 1$ што је немогуће. □

(**Шћепан Радевић 16/19 Б**) задатак преузет са `https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

345

Производ два природна броја је 68040, а њихов најмањи заједнички садржалац је 3780. Одредити те бројеве.

Доказ. Нека су a и b тражени бројеви и $a < b$. Тада је $a \cdot b = 68040$ и нзс$(a, b) = 3780$. Знамо да важи нзд$(a, b) \cdot$ нзс$(a, b) = |ab|$ па слиједи:

$$\text{нзд}(a, b) = 68040 : 3780 = 18.$$

Тада је $a = 18x$ и $b = 18y$ за неко $x, y \in \mathbb{N}$, нзд$(x, y) = 1$ и $x < y$. Сада имамо:

$$18x \cdot 18y = 68040 \iff 324xy = 68040 \iff x \cdot y = 210.$$

Како 210 можемо написати као:

$$210 = 1 \cdot 210 = 2 \cdot 105 = 3 \cdot 70 = 5 \cdot 42 = 6 \cdot 35 = 7 \cdot 30 = 10 \cdot 21 = 14 \cdot 15$$

слиједи да је

$$(x, y) \in \{(1, 210), (2, 105), (3, 70), (5, 42), (6, 35), (7, 30), (10, 21), (14, 15)\}.$$

Дакле, тражени бројеви су:

$$(a, b) \in \{(18, 3780), (36, 1890), (54, 1260), (90, 756), (108, 630), (126, 540), (180, 378), (252, 270)\}.$$

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

346

●●●●

За које цијеле бројеве p једначина

$$\frac{1}{(x-4)^2} - \frac{p-1}{16-x^2} = \frac{p}{(x+4)^2}$$

има јединствено цјелобројно рјешење?

Доказ. Уз услов да је $x \neq 4$ и $x \neq -4$, након множења дате једначине са $(x+4)^2(x-4)^2$ добијамо:

$$\begin{gathered}
(x+4)^2 + (p-1)(x+4)(x-4) = p(x-4)^2,\\
x^2 + 8x + 16 + (p-1)(x^2-16) = p(x^2 - 8x + 16)\\
x^2 + 8x + 16 + px^2 - 16p - x^2 + 16 = px^2 - 8px + 16p\\
8x + 32 - 16p = -8px + 16p\\
8x(p+1) = 32p - 32\\
x(p+1) = 4p - 4.
\end{gathered}$$

Очигледно да $p = -1$ није рјешење. Стога је $p \neq -1$ и

$$x = \frac{4p-4}{p+1}.$$

Отуда добијамо

$$x = \frac{4p-4}{p+1} = \frac{4p+4-8}{p+1} = 4 - \frac{8}{p+1}.$$

Да би рјешење x било цјелобројно, $p+1$ мора дијелити број 8. Тада $p+1 \in \{\pm1, \pm2, \pm4, \pm8\}$, односно $p \in \{-9, -5, -3, -2, 0, 1, 3, 7\}$. Због почетног услова $x \neq 4$ и $x \neq -4$, p не смије бити једнак 0.

Коначно добијамо $p \in \{-9, -5, -3, -2, 1 - 3, -7\}$. ☐

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

347

●●●●

Нека је k дати природан број. Доказати да постоји бесконачно много потпуних квадрата облика $2^k n - 7$.

Доказ. Докажимо најприје да за сваки природан број k постоји природан број a_k са особином:

$$a_k^2 \equiv -7 \pmod{2^k}.$$

Примијетимо да избор $a_k = 1$ задовољава тражени услов за $k \leq 3$. За $k \geq 4$, пођимо од претпоставке $a_k^2 \equiv -7 \pmod{2^k}$. Сада очигледно имамо двије могућности:

$$a_k^2 \equiv -7 \pmod{2^{k+1}},$$

или

$$a_k^2 \equiv 2^k - 7 \pmod{2^{k+1}}\ .$$

У првом случају дефинишемо $a_{k+1} = a_k$, а у другом $a_{k+1} = a_k + 2^{k-1}$. Пошто је a_k непарно, у посљедњем случају слиједи:

$$a_{k+1}^2 = a_k^2 + 2^k a_k + 2^{2k-2} \equiv a_k^2 + 2^k a_k \equiv a_k^2 + 2^k \equiv -7 \pmod{2^{k+1}},$$

користећи индуктивну претпоставку.

Најзад, примијетимо да низ a_K није ограничен, пошто мора бити $a_k^2 \geq 2^k - 7$, што значи да посматрани низ има бесконачно много различитих вриједности. Отуда добијамо тражени резултат, пошто за $m \geq k$ имамо $a_m^2 \equiv -7 \pmod{2^k}$ и можемо дефинисати

$$n = \frac{a_m^2 + 7}{2^k}.$$

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf

348
●●●●

Наћи све аритметичке прогресије у којима су за све $n \in \mathbb{N}$ збирови првих n чланова потпуни квадрати.

Доказ. Ако је a први члан аритметичке прогресије, а d њена разлика, тада имамо формулу за суму првих n чланова прогресије:

$$S_n = \frac{1}{2} n(2a + (n-1)d).$$

Специјално, имамо $S_1 = a$ и $S_4 = 2(2a + 3d)$, одакле је $a = b^2$ и $d = 2d_1$ за неке природне бројеве b и d_1, па слиједи:

$$S_n = n(b^2 + (n-1)d_1) = n(nd_1 + (b^2 - d_1)).$$

За произвољан прост број p из $p \mid S_p$ слиједи $p^2 \mid S_p$, што на основу горње једнакости повлачи $p \mid (b^2 - d_1)$. То је могуће ако и само ако је $b^2 - d_1 = 0$, тј. $d = 2b^2$.

С друге стране, ако су чланови аритметичке прогресије облика $(2n-1)b^2$, гдје је b произвољан природан број, тада су одговарајуће суме $S_n = n^2 b^2$, што значи да смо нашли све тражене прогресије.

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

349

Одредити све природне бројеве x, y за које важи $1! + 2! + \cdots + x! = y^2$.

Доказ. Разликујемо сљедеће случајеве:

- Ако је $x = 1$, $1! = 1^2$
- Ако је $x = 2$, $1! + 2! = 3 \neq y^2$.
- Ако је $x = 3$, $1! + 2! + 3! = 9 = 3^2$.
- Ако је $x = 4$, $1! + 2! + 3! + 4! = 33 \neq y^2$. Ако је $x \geq 5$, онда $x!$ завршава цифром 0, а збир $1! + 2! + 3! + 4! + \cdots + x!$ завршава цифром 3. Будући да се квадрат природног броја y не може завршавати цифром 3 једина рјешења добијамо за $x = 1$ и $x = 3$, односно
$$(x, y) \in \{(1, 1), (3, 3)\}.$$

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

350

Одредити све тројке природних бројева (m, n, k) такве да важи $3^m + 7^n = k^2$.

Доказ. Будући да је $7^n = k^2 - 3^m$ слиједи да k^2 и 3^m морају давати исти остатак при дијељењу са 7, а то је могуће само ако је m паран број. Заиста, $k^2 \equiv 1, 2, 4 \pmod 7$, а $3^m \equiv 1, 2, 4 \pmod 7$ само ако је m паран. Дакле, $m = 2l$ за неки природан број l, па можемо писати
$$7^n = (k - 3^l)(k + 3^l).$$

Из горње једначине слиједи да су оба чиниоца степени броја 7, тј.

$$k - 3^l = 7^a,$$

$$k + 3^l = 7^b,$$

гдје су a и b неки ненегативни цијели бројеви и $a < b$. Одузимањем прве једначине од друге добијамо:

$$2 \cdot 3^l = 7^b - 7^a = 7^a(7^{b-a} - 1).$$

Будући да $2 \cdot 3^l$ није дјељиво са 7, слиједи да је $a = 0$ и

$$1 + 2 \cdot 3^l = 7^b.$$

За $l = 1$ добијемо да је $m = 2$, $b = 1$ и $k = 4$, па је $n = 1$.
Ако је $l \geq 2$, онда $7^b = 1 + 2 \cdot 3^l$ даје остатак 1 при дијељењу са 9. Према Ојлеровој теореми је

$$7^{\varphi(9)} = 7^6 \equiv 1 \pmod 9.$$

За најмање $d \in \mathbb{N}$ такав да је $7^d \equiv 1 \pmod 9$ (тј. за ред броја 7 модуло 9) мора важити да $d \mid \varphi(9) = 6$. Стога испитајмо

$$7^2 \equiv 4 \pmod 9,\ 7^3 \equiv 1 \pmod 9$$

и закључујемо да је $d = 1$, па је $7^{3s} \equiv 1 \pmod 9$ за све $s \in \mathbb{N}$. Дакле,

$$7^{3x} - 1 = 2 \cdot 3^l,$$

за неки $s \in \mathbb{N}$. Очигледно је лијева страна претходне једнакости дјељива са $7^3 - 1 = 342 = 2 \cdot 3^2 \cdot 19$, тј. са 19, а десна то није, па закључујемо да нема рјешења у случају $l \geq 2$.

Једино рјешење је (m, n, k)=(2, 1, 4). ☐

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

351

а) Одредити остатак при дијељењу броја $(7^{2012})^{2014} - (3^{12})^{14}$ са 10.
б) Одредити задње три цифре броја $2^{2015} - 2^{2013} + 2^{2010}$.

Доказ. а) Будући да је нзд$(7, 10) = 1$ према Ојлеровој теореми слиједи

$$7^{\varphi(10)} = 7^4 \equiv 1 \pmod{10},$$

па је

$$7^{2012} \equiv 1 \pmod{10},$$

те

$$(7^{2012})^{2014} \equiv 1 \pmod{10}.$$

Аналогно,

$$3^{\varphi(10)} = 3^4 \equiv 1 \pmod{10},$$

из чега слиједи да је

$$(3^{12})^{14} \equiv 1 \pmod{10}.$$

Имамо да је $(7^{2012})^{2014} - (3^{12})^{14} \equiv 0 \pmod{10}$, па закључујемо да је остатак броја $(7^{2012})^{2014} - (3^{12})^{14}$ при дијељењу са 10 једнак 0.

б) Након издвајања заједничког члана добијамо:

$$2^{2015} - 2^{2013} + 2^{2010} = 2^{2010}(2^5 - 2^3 + 1) = 2^{2010} \cdot 25 = 2^{2008} \cdot 2^2 \cdot 25 = 2^{2008} \cdot 100.$$

Степени броја 2 (већи од 1) имају задњу цифру редом $2, 4, 8, 6, 2, 4, 8, 6, \ldots$ Дакле, ако им је експонент дјељив са 4, задња цифра је 6. Тада је задња цифра броја 2^{2008} једнака 6, а множењем са 100 добијамо да су задње три цифре 6, 0, 0.

□

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

352 ●●●●

Постоји ли 14 узастопних цијелих бројева од којих је сваки дјељив са једним или више простих бројева p из интервала $2 \leq p \leq 11$?

Доказ. Прво, уочимо да за било којих 14 узастопних позитивних цијелих бројева, тачно 7 је парних (дјељивих са 2) и стога задовољавају критеријум. Дакле, проблем можемо поједноставити на сљедеће питање, еквивалентно почетном: *Постоји ли 7 узастопних позитивних непарних цијелих бројева од којих је сваки дјељив са једним или више простих бројева* p *из интервала* $3 \leq p \leq 11$?
Међу узастопних 7 позитивних непарних цијелих бројева важи:

- 2 или 3 дјељива су са 3,
- 1 или 2 дјељива су са 5,
- тачно 1 је дјељив са 7,
- 0 или 1 дјељива су са 11.

Да би сваки од тих 7 бројева био дјељив са 3, 5, 7 или 11, међу њима мора бити 3 садржаоца 3, 2 садржаоца броја 5, 1 садржалац броја 7 и 1 садржалац броја 11. Додатно, нити један од тих бројева не смије бити садржалац од никоја два од претходно споменута четири проста броја. Нека су $a_1, a_2, \ldots, a_7$ узастопни позитивни непарни цијели бројеви. Тада a_1, a_4 и a_7 морају бити садржаоци броја 3 те стога не могу бити садржаоци бројева 5, 7, или 11. Но, ако постоје два садржаоца броја 5, морају бити један од два пара (a_1, a_6) и (a_2, a_7). Међутим, сваки од тих парова садржи садржалац броја 3, те стога барем један од 7 узастопних позитивних непарних цијелих бројева није дјељив нити с једним од простих бројева 3, 5, 7 или 11.
Дакле, одговор је негативан. □

(**Шћепан Радевић 16/19 Б**) задатак преузет са
`https://zir.nsk.hr/islandora/object/pmf%3A3333/datastream/PDF/view`

353

(а) Наћи сва рјешења једначине

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x}=m,$$

тако да је $m \in \mathbb{N}$, а x, y и z су узајамно прости, цијели, позитивни бројеви.

(б) Доказати да дата једначина нема рјешења у скупу цијелих бројева, за $m = 1$.

Доказ. (а) Наша једначина је еквивалентна једначини $x^2z + y^2x + z^2y = mxyz$ и x, y, z су различити од 0 и у паровима узајамно прости. Слиједи да

$$\begin{aligned} y &\mid x^2z, \\ z &\mid y^2x, \\ x &\mid z^2y. \end{aligned}$$

Како је нзд$(x, y) = 1$ и нзд$(z, y) = 1$, из чега слиједи нзд$(x^2z, y) = 1$, из $y \mid x^2z$ добијамо $y = \pm 1$. На сличан начин добијамо $z = \pm 1$ и $x = \pm 1$.

Ако су сва три броја x, y, z истог знака, онда из наше једначине слиједи $1 + 1 + 1 = m$. Одатле је $m = 3$. Ако су два позитивна а један негативан или два негативна а један позитиван, онда из наше једначине слиједи да је m негативан, што је супротно претпоставци.

Тако да, за позитиван цијели број m, једначина

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x}=m$$

има рјешење у скупу цијелих бројева, тако да су x, y, z узајамно прости, само за $m = 3$. У овом случају постоје само два рјешења: $x = y = z = 1$ и $x = y = z = -1$. За позитиван цијели број $m \neq 3$ наша једначина нема тражено рјешење.

(б) Имамо

$$\frac{x}{y}\cdot\frac{y}{z}\cdot\frac{z}{x}=1,$$

па бројеви (рационални,позитивни) $\frac{x}{y}, \frac{y}{z}, \frac{z}{x}$ не могу сви бити мањи од 1. Ако је макар један од њих $\geq$ од 1, онда је

$$\frac{x}{y}+\frac{y}{z}+\frac{z}{x}>1$$

и лијева страна не може бити једнака 1, за позитивне цијеле бројеве x, y и z.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

354

Доказати да, ако су x, y, z позитивни цијели бројеви такви да је нзд$(x, y) = 1$ и $x^2+y^2 = z^4$, онда $7 \mid xy$. Показати да је услов нзд$(x, y) = 1$ неопходан.

Доказ. **Дефиниција:** Уређену тројку природних бројева (x, y, z) називамо Питагорина тројка, ако су x и y катете, а z хипотенуза неког правоуглог троугла, тј. ако важи

$$x^2 + y^2 = z^2.$$

Ако су x, y, z узајамно прости, онда кажемо да је (x, y, z) примитивна Питагорина тројка. Такав троугао називамо примитивни Питагорин троугао.

Тврђење: У свакој примитивној Питагориној тројки, тачно је један од бројева x и y непаран. Заиста, ако би x и y били парни, онда тројка не би била примитивна, а ако би x и y били непарни, онда би из $x^2 + y^2 \equiv 2 \pmod 4$ и $z \equiv 0 \pmod 4$, добили контрадикцију.

Теорема: Све примитивне Питагорине тројке (x, y, z) у којима је y паран, дате су формулом

$$x = m^2 - n^2, y = 2mn, z = m^2 + n^2,$$

гдје је $m > n$ и m, n су узајамно прости природни бројеви различите парности.

Услов нзд$(x, y) = 1$ је неопходан, на примјер за $15^2 + 20^2 = 5^4$ $(7 \nmid 15 \cdot 20)$.

Сада, ако је нзд$(x, y) = 1$ и x, y, z су позитивни цијели бројеви такви да $x^2 + y^2 = z^4$, онда знамо из Питагорине теореме да постоје бројеви m, n такви да,на примјер, важи $x = m^2 - n^2, y = 2mn, z^2 = m^2 + n^2$.

Претпоставимо да $7 \nmid y$, одакле слиједи да $7 \nmid m$ и $7 \nmid n$. Лако је видјети да 2.степен неког броја који није дјељив са 7, таквим дијељењем даје остатак $1, 2$ или 4. Како $1+2, 1+4$ и $2+4$ не могу бити такви остаци, нити су дјељиви са 7, из једначине $z^2 = m^2 + n^2$ слиједи да бројеви m и n морају дати исте остатке, при дијељењу са 7. Слиједи да имамо $7 \mid x = m^2 - n^2$.
□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

355 ●●●●

Пронађите све могућности за позитивне цијеле бројеве x, y и z такве да је $x \leq y \leq z$ и

$$x^3(y^3+z^3) = 2012(xyz+2)$$

.

Доказ. Примијетимо да је $2012 = 2 \cdot 2 \cdot\ 503$, па је десна страна дјељива са овим бројевима, дакле да би једнакост била испуњена и лијева страна мора да буде дјељива са 503 и 2^2. То ћемо искористити да испитамо могућности за x, y и z.

Ако $503 \mid x$, тада 503^3 дијели лијеву страну једнакости, док највише 503^1 дијели десну страну. Одатле закључујемо да $503 \nmid x$. Како x дијели лијеву страну једнакости, јасно је да мора да дијели и $2012(xyz+2)$. Ако $x \nmid 2012$, тада $x \mid xyz+2$, па $x \mid 2$ (јер $x \mid xyz$), што је супротно претпоставци да $x \nmid 12$. Када $x \mid 2012$ мора бити $x = 2^\alpha$, гдје је $\alpha \in \{0,1,2\}$. Ако је $x = 2^2$ тада 2^6 дијели лијеву страну док највише 2^3 дијели лијеву страну. Дакле, $x \in \{1,2\}$.

Како је 503 прост број, на основу Мале Фермаове теореме имамо

$$y^{502} \equiv z^{502} \pmod{503}.$$

Из тога слиједи да $503 \mid x(y^3+z^3)$ и $503 \nmid x$. Имамо да $503 \mid (y^3+z^3)$, односно

$$\begin{gathered} y^3+z^3 \equiv 0 \pmod{503} \\ y^3 \equiv -z^3 \pmod{503}. \end{gathered}$$

Даље имамо

$$\begin{gathered} y^{3 \cdot 167} \equiv -z^{3 \cdot 167} \pmod{503} \\ \implies y \equiv -z \pmod{503}. \end{gathered}$$

Тако да $503 \mid y+z$, па је $y+z = 503k$, гдје је k природан број.

1. случај: $x = 1$
Једначина тада постаје:

$$\begin{aligned} & y^3+z^3 = \\ & = 2012(yz+2) = \\ & = 503k(y^2-yz+z^2) = \\ & = 2012(yz+2) = \\ & = k(y^2-yz+z^2) = \\ & = 4yz+8 = \\ & = k(y-z)^2+yz(k-4) = \\ & = 8. \end{aligned}$$

Како је $yz(k-4) \leq 8$, мора бити $k \leq 4$ јер је $yz+1 \geq y+z = 503k \geq 503 \implies yz \geq 502$. Пошто је $(y^3+z^3) = 2012(yz+2)$ закључујемо да (y^3+z^3) мора бити паран број, што даље значи да ће y и z бити исте парности. Али како имамо да је $y + z = 503k$, закључујемо да је k паран. Дакле, $k \in \{2, 4\}$.

Ако је $k = 4$, тада $(y - z)^2 = 2$ што је немогуће. Ако је $k = 2$, тада $2 - (y - z)^2 - 2yz = 8$. Одатле слиједи $(y + z)^2 - 5yz = 4$, па је $2^2 \cdot 503^2 - 4 = 5yz$, али лијева страна није дјељива са 5 тако да рјешења нема када је $x = 1$.

2.случај: $x = 2$
Једначина тада постаје:

$$y^3 + z^3 = 503(yz + 1)$$
$$k(y^2 - yz + z^2) = yz + 1.$$

Ако је $|y - z| > 1$, тада $k(y^2 - yz + z^2) \geq y^2 - yz + z^2 > yz + 1$, што није тачно, дакле $y = z$ или $|y - z| = 1$. Одатле имамо $2y^3 = 503y^2 + 503$, дакле 503 дијели десну страну па $503^3 \mid 2y^3$, али како 503^3 не дијели десну страну, то је контрадикција. Значи, $k = 1$ и онда је рјешење $(x, y, z) = (2, 251, 252)$.

Провјеримо директним израчунавањем да ли наше рјешење задовољава услове:

$$\begin{aligned}
&x^3(y^3 + z^3) = \\
&= 2012(xyz + 2) = \\
&= 2^3(251^3 + 252^3) = \\
&= 8 \cdot (251 + 252)(251^2 - 251 \cdot 252 + 252^2) = \\
&= 8 \cdot 503(251 \cdot 252 - 251 - 251 \cdot 252 + 251 \cdot 252 + 252) = \\
&= 8 \cdot 503(252 \cdot 251 + 1) = \\
&= 4 \cdot 503(2 \cdot 251 \cdot 252 + 2).
\end{aligned}$$

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

356
●●●●

Доказати да за сваки непаран број n важи $n \mid 2^{n!} - 1$.

Доказ. За све природне бројеве n имамо да важи $\varphi(n) \mid n!$. Заправо, то је тачно за $n = 1$. Ако је $n > 1$ и ако је $n = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$, тако да је $q_1 < q_2 < \ldots < q_k$, онда

$$\varphi(n) = q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \cdots q_k^{\alpha_k - 1}(q_1 - 1) \cdots (q_k - 1)$$

и имамо $q_1^{\alpha_1 - 1} q_2^{\alpha_2 - 1} \cdots q_k^{\alpha_k - 1} \mid n$, $q_1 - 1 < q_k \leq n$, одакле слиједи да су $q_k - 1 < n$ и $q_1 - 1 < q_2 - 1 < \ldots < q_k - 1$ различити природни бројеви мањи од n. Тако да $q_1 - 1 \cdot q_2 - 1 \cdots q_k - 1 \mid (n - 1)!$. То значи да $\varphi(n) \mid (n - 1)! \cdot n = n!$.

Ако је n непаран, онда на основу Ојлерове теореме слиједи $n \mid 2^{\varphi(n)-1} \mid 2^{n!}-1$ и тиме је доказ завршен.

$\square$

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

357

Наћи све бројеве облика $2^n-1, n \in \mathbb{N}$, тако да нису већи од 10^6 и да се могу записати као производ два проста броја и доказати да, ако је n паран број, мањи од 4, онда је 2^n-1 производ најмање 3 цијела броја, већа од 1.

Доказ. Имамо $2^2-1=3, 2^4-1=3\cdot5$ и $2^{2k}-1=(2^k-1)(2^k+1)$. Ако је за $n=2k>4$ број $2^{2k}-1$ једнак производу два проста броја, онда бројеви $2^k-1, 2^k+1$ морају бити прости. Како су ово узастопни, непарни бројеви, имамо да је $2^k-1 \leq 5$, па је $k \leq 2$. С обзиром на то да је $k>1$, мора бити $k=2$, супротно претпоставци да је $k>2$. Дакле, бројеви 2^n-1 су, за парно $n>4$, једнаки производу најмање три природна броја.

За непарно n, имамо $2^3-1=7, 2^5-1=31, 2^7-1=127, 2^9-1=7\cdot73, 2^{11}-1=23\cdot89, 2^{13}-1=8191$, који је прост, $2^{15}-1=7\cdot31\cdot151$; бројеви $2^{17}-1$ и $2^{19}-1$ су прости и $2^{21}-1=7\cdot127\cdot337$, док је $2^{23}-1>10^6$.

Тако да, сви природни бројеви облика 2^n-1, који су мањи од 10^6 и који се могу записати као производ два проста броја су $2^4-1=3\cdot5, 2^9-1=7\cdot73$ и $2^{11}-1=23\cdot89$.

$\square$

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.isinj.com/mt-aime/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

358

Нека је d било који позитиван цијели број различит од $2, 5$ и 13. Доказати да постоје различити a и b из скупа $\{2,5,13,d\}$ такви да $ab-1$ није потпун квадрат.

Доказ. Јасно је да ако су a и b из скупа $2, 5, 13$, израз $ab-1$ јесте потпун квадрат. Провјеримо то. Нека су $a, b \neq d$. Имамо:

$$\begin{aligned} 2\cdot5-1=10-1=9 &\quad (a=2, b=5 \text{ или } a=5, b=2\ ) \\ 2\cdot13-1=26-1=25 &\quad (a=2, b=13 \text{ или } a=13, b=2) \\ 5\cdot13-1=65-1=64 &\quad (a=5, b=13 \text{ или } a=13, b=5) \end{aligned}$$

Директном провјером смо закључили да у свим случајевима када су $a, b \neq d$, $ab - 1$ јесте потпун квадрат. Тако да остаје занимљив случај када је $a = d$ или $b = d$. Тај случај ћемо рјешавати тако што ћемо претпоставити да у свакој комбинацији за a и b из овог скупа, $ab - 1$ јесте потпун квадрат. Уколико добијемо контрадикцију то значи да постоји неки избор за a и b тако да $ab - 1$ не буде потпун квадрат.

Дакле, да докажемо тврђење показаћемо да $2d - 1, 5d - 1$ и $13d - 1$ не могу истовремено бити квадрати природних бројева. Квадрат непарног броја даје остатак 1, при дијељењу са 4 и 8. То је својство које се често користи, док је разматрање остатака при дијељењу са 5 мотивисано условом да је $5d - 1$ потпун квадрат. Дакле, од користи ће нам бити да размотримо остатке при дијељењу потпуних квадрата са $4, 5$ и 8, који су приказани у следећим табелама:

n	0	1	2	3
$n^2 \pmod 4$	0	1	0	1

n	0	1	2	3	4
$n^2 \pmod 5$	0	1	4	4	1

n	0	1	2	3	4	5	6	7
$n^2 \pmod 8$	0	1	4	1	0	1	4	1

Претпоставимо сада да је $a = d$, b ће тада бити из скупа $\{2, 5, 13\}$. Дакле, провјеравамо да ли може неки од $2d - 1, 5d - 1$ и $13d - 1$ да не буде потпун квадрат. Претпоставимо да су сва три потпуни квадрати. Посматрајмо остатке при дијељењу са 4.

$$\begin{aligned} 13d - 1 &= k^2 \qquad (1) \\ 5d - 1 &= l^2 \qquad (2) \\ 2d - 1 &= m^2 \qquad (3) \end{aligned}$$

$$(1) \implies 13d \equiv 1, 2 \pmod 4 \implies d \equiv 1, 2 \pmod 4$$

1.случај: $d \equiv 1 \pmod 4 \implies d = 4k + 1$, за неко $k \in \mathbb{Z}$.

$$(2) \implies 20k + 4 = 4(5k + 1) = l^2 \implies (\frac{l}{2})^2 \equiv 2 \pmod 5$$

Ту имамо контрадикцију са резултатима у другој табели са остацима, гдје видимо да су могући остаци потпуних квадрата при дијељењу са 5 само 0 или 4, али не и 2. Дакле, преостаје случај када је $d \equiv 2 \pmod 4$.

2.случај: $d \equiv 2 \pmod 4 \implies d = 4k + 2$, за неко $k \in \mathbb{Z}$

$$(3) \implies m^2 \equiv 3 \pmod 8$$

Сада и овдје имамо контрадикцију са резултатима у трећој табели, гдје видимо да су могући резултати потпуних квадрата при дијељењу са 8 само $0, 1$ или 4, али не и 3.

Закључујемо да $2d - 1, 5d - 1$ и $13d - 1$ не могу истовремено бити потпуни квадрати, што значи да постоји бар један који није и тиме је доказ завршен.

Оно што смо користили у задатку су остаци по модулу $4, 5$ и 8 квадрата природних бројева. Сви парни бројеви су облика $2k$, дакле парни број на квадрат ће бити облика $4k^2$, а то је $\equiv 0 \pmod 4$. Што се тиче непарних бројева, они су облика $2k+1$, па је сваки непаран број на квадрат облика $4k^2 + 4k + 1$, а то је $\equiv 1 \pmod 4$. Дакле, квадрати свих природних бројева дају остатке 0 или 1 при дијељењу са 4.

Остаци при дијељењу са 5 за природне бројеве су $0, 1, 2, 3$ или 4, па су остаци по модулу 5 за квадрате ових бројева $0, 1$ или 4. Слично за 8, остаци за природне бројеве су $0, 1, 2, 3, 4, 5, 6$ или 7, па су могућности за остатке квадрата $0, 1, 4$. Користећи се овим знањима и правилима конгруенција дошли смо до резултата.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

359

●●●●

Доказати да је број $A = 8888\cdots88$ ($2012 \cdot 2013$ осмица) дјељив бројевима $2, 3, 7, 11, 13, 37$. Провјерити да ли је он дјељив и са $4, 8, 16$.

Доказ. Користићемо растављање броја на чиниоце и на тај начин ћемо покушати да дођемо до рјешења. Примијетимо још да се број 888888 може записати у облику:

$$888888 = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37,$$

што значи да је овај број дјељив са $2, 3, 7, 11, 13$ и 37, као и са 4 и 8. То ћемо покушати да искористимо у растављању нашег броја.

Број A има $2012 \cdot 2013 = 4050156 = 6 \cdot 675026$ цифара, па се може записати у облику:

$$\begin{aligned} A &= 888888 + 10^6 \cdot 888888 + \ldots + 10^k \cdot 888888 = \\ &= 888888 \cdot (1 + 10^6 + \ldots + 10^k) = \\ &= 8 \cdot 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot (1 + 10^6 + \ldots + 10^k). \end{aligned}$$

Одавде је јасно да је број A дјељив са $2, 4, 8$ као и са $3, 7, 11, 13, 37$. Број у загради у претходној једнакости је непаран, па број није дјељив са 16.

Напомена: Сваки шестоцифрен број код којег су све цифре исте (облика $\overline{xxxxxx}$) је дјељив са цифрама $3, 7, 11, 13, 37$ и са бројем x. То доказујемо на сљедећи начин:

$$\begin{aligned}\overline{xxxxxx} &= 10^5 \cdot x + 10^4 \cdot x + 10^3 \cdot x + 10^2 \cdot x + 10 \cdot x + x = \\ &= (10^5 + 10^2) \cdot x + (10^4 + 10^1) \cdot x + (10^3 + 1) \cdot x = \\ &= 102 \cdot (10^3 + 1) \cdot x + 10^1 \cdot (10^3 + 1) \cdot x + (10^3 + 1) \cdot x = \\ &= (10^3 + 1) \cdot (10^2 + 10 + 1) \cdot x = \\ &= 1001 \cdot 111 \cdot x = \\ &= 3 \cdot 7 \cdot 11 \cdot 13 \cdot 37 \cdot x.\end{aligned}$$

Из посљедње једнакости очигледно слиједи наше тврђење.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`http://elibrary.matf.bg.ac.rs/bitstream/handle/123456789/4489/masSpasicTijana.pdf?sequence=1`

360
●●●●

(а) Доказати да постоје природни бројеви x, y, z чији је збир квадрата једнак $6^{2^{2014}}$.
(б) Одредити посљедње двије цифре броја 6^{2014}.
(в) Одредити природан број x, такав да важи једнакост

$$x^{2014} = x^{2013} + 2013.$$

Доказ. Индукцијом ћемо показати да се сваки број, облика 6^{2^n} може представити у облику збира три потпуна квадрата, тј. да за сваки природан број n постоје природни бројеви x_n, y_n, z_n, такви да је

$$x_n^2 + y_n^2 + z_n^2 = 6^{2^n}.$$

За $n = 1$ можемо узети $x_1 = 4, y_1 = 4, z_1 = 2$.

Претпоставимо да тврђење важи за неки природан број n и докажимо да тврђење важи и за природни број $n + 1$. Бројеве $x_{n+1}, y_{n+1}, z_{n+1}$ изабраћемо коришћењем бројева x_n, y_n, z_n на сљедећи начин:

$$x_{n+1}^2 = x_n^2 + y_n^2 - z_n^2, y_{n+1} = 2y_n z_n \text{ и } z_{n+1} = 2x_n z_n.$$

Сада добијамо:

$$\begin{aligned}x_{n+1}^2 + y_{n+1}^2 + z_{n+1}^2 &= (x_n^2 + y_n^2 - z_n^2)^2 + (2y_n z_n)^2 + (2x_n z_n)^2 = \\ &= (x_n^2 + y_n^2 + z_n^2)^2 = (6^{2^n})^2 = 6^{2^{n+1}},\end{aligned}$$

што је и требало показати.

(б) Непосредним израчунавањем утврђујемо да се бројеви $6^2, 6^3, 6^4, 6^5, 6^6, 6^7, \ldots$ завршавају редом цифрама $36, 16, 96, 76, 56, 36, \ldots$. Дакле, периодично се понављају посљедње цифре са периодом од 5 бројева. Како је $2014 = 4 + 5 \cdot 402$, то се 6^{2014} завршава истим цифрама као 6^4, дакле са 96.

(в) Из дате једнакости добијамо да је $x^{2014} - x^{2013} = 2013$. Ако је x паран број, онда су x^{2014} и x^{2013} парни бројеви, па њихова разлика, која је такође паран број, не може бити непаран број 2013.

Ако је x непаран број, онда су x^{2014} и x^{2013} непарни бројеви, па њихова разлика, која је паран број, не може бити 2013.

Закључујемо да не постоји природан број који задовољава дату једнакост.

$\square$

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://www.pmf.ni.ac.rs/mii-content/2014/Broj%202014%20u%20zanimljivim%20zadacima.pdf`

361 ●●●●

Нека огрлица А има 14 бисера, а огрлица Б 19 бисера. Доказати да за сваки непаран природан број n постоји начин да нумеришемо све бисере бројевима из скупа

$$\{n, n+1, \ldots, n+32\},$$

тако да је сваки број коришћен само једном и да су бројеви који одговарају сусједним бисерима узајамно прости.

Доказ. Основна идеја рјешења је да што је могуће више користимо узастопне природне бројеве за означавање сусједних бисера, пошто су они узајамно прости. Покушаћемо да из датог скупа на погодан начин издвојимо 14 узастопних бројева којима ћемо означити бисере огрлице А:

$$n+m, n+m+1, \ldots, n+m+13$$

(гдје ће број $m, 1 \leq m \leq 18$ бити накнадно одређен), док ће преостали бројеви чинити два низа узастопних бројева дужине m, односно $19 - m$. У питању су:

$$n, n+1, \ldots, n+m-1, n+m+14, \ldots, n+32,$$

и њима ћемо, не мијењајући им редослед, означити бисере огрлице Б.

Примијетимо најприје да је на огрлици Б испуњен услов $\text{нзд}(n, n+32) = \text{нзд}(n, 32) = 1$, јер је n непаран број. Према томе, услови из којих одређујемо m су:

$$\text{нзд}(n+m, n+m+13) = 1, \quad \text{нзд}(n+m-1, n+m+14) = 1.$$

Важе сљедеће једнакости:

$$\text{нзд}(n+m, n+m+13) = \text{нзд}(n+m, 13),$$
$$\text{нзд}(n+m-1, n+m+14) = \text{нзд}(n+m-1, 15),$$

па m тражимо из сљедећа три услова:

$$\begin{aligned} &(1) \quad m \not\equiv -n \pmod{13} \\ &(2) \quad m \not\equiv 1-n \pmod{3} \\ &(3) \quad m \not\equiv 1-n \pmod{5}. \end{aligned}$$

Међутим, од бројева $1, 2, \ldots, 18$ највише два не задовољавају први услов, тачно шест не задовољавају други и највише четири трећи услов. Према томе, међу њима постоји број m_0, који испуњава сва три услова. Ако сада ставимо $m = m_0$, онда нумерација обије огрлице има тражене особине.

$\square$

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

362

За дато $c \in \mathbb{N}$, нека је n_0 најмањи природан број такав да је $2^{n_0} > c$. Доказати да тада за све $n \geq n_0$ важи

$$a^n \mid cb^n \implies a \mid b,$$

гдје су $a, b \in \mathbb{N}$.

Доказ. Нека је p прост број и нека су α, β, γ редом највиши степени којим p дијели бројеве a, b, c, за које смо претпоставили да $a^n \mid cb^n$ $(n \geq n_0)$. Дакле, имамо

$$n\alpha \leq n\beta + \gamma.$$

С друге стране, како је $2^{n_0} > c$, то је $\gamma < n_0 \leq n$. Отуда је

$$n\alpha < n\beta + n = n(\beta + 1),$$

па добијамо $\alpha < \beta + 1$, тј. $\alpha \leq \beta$. Пошто је прост број p у овом разматрању био произвољан, слиједи $a \mid b$.

$\square$

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

363

Да ли једначина

$$x^2 + xy + y^2 = 2$$

има рационална рјешења?

Доказ. Крећемо од претпоставке да дата једначина има рационално рјешење (x, y). Тада можемо записати $x = \frac{a}{c}, y = \frac{b}{c}$, при чему ове разломке не можемо скратити истим природним бројем. Другим ријечима, нзд$(a, b, c) = 1$ (при чему су $a, b, c \in \mathbb{Z}$).
Добијамо:

$$a^2 + ab + b^2 = 2c^2.$$

Из горње једнакости слиједи да оба броја a, b морају бити парна (у супротном би лијева страна садржала један или три непарна сабирка). Због тога, c је непаран број (у супротном би било $2 \mid$ нзд(a, b, c)). Међутим, сада је лијева страна горње једнакости дјељива са 4, док је десна страна дјељива са 2, али не и са 4. Добијамо контрадикцију.

Дакле, одговор на постављено питање је негативан.

Коментар: Исти резултат слиједи и за једначину

$$x^2 + nxy + y^2 = 2,$$

гдје је n било који непаран цијели број.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://kupdf.net/download/igor-dolinka-elemetarna-teorija-brojeva-moji-omiljeni-zadaci_59f09e7be2b6f524242640a9_pdf`

364

(Математичка олимпијада у Русији, 1998.) Да ли постоје n-тоцифрени бројеви M и N, тако да су све цифре броја M парне, а све цифре броја N непарне и свака њихова цифра се појављује тачно једном у тим бројевима и $N \mid M$?

Доказ. Одговор је негативан. Претпоставимо да M и N постоје и да је $a = \frac{M}{N}$. Тада је $M \equiv 0 + 2 + 4 + 6 + 8 \equiv 2 \pmod 9$ и $N \equiv 1 + 3 + 5 + 7 + 9 \equiv 7 \pmod 9$. Оба су узајамно проста са бројем 9. Сада је $a \equiv \frac{M}{N} \equiv 8 \pmod 9$, па је $a \geq 8$. Али, $N \geq 13579$, па је $M = aN \geq 8(13579) > 99999$. Добили смо контрадикцију.

□

(**Јелена Јовановић 3/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

365

Низ природних бројева $(a_n)_{n \in \mathbb{N}}$ дефинисан је са $a_1 = 3$ и $a_{n+1} = 3^{a_n}$ за $n \geq 1$. Одредити последње двије цифре броја a_{2008}.

Доказ. Како је нзд$(3,4) = 1$ и нзд$(3,25) = 1$, према Ојлеровој теореми је $3^2 \equiv 1 \pmod 4$ и $3^{20} \equiv 1 \pmod{25}$, па је $3^{20} \equiv 1 \pmod{100}$. Из $a_1 = 3$ и $a_2 = 27$ слиједи

$$a_3 = 3^{a_2} = 3^{20} \cdot 3^7 \equiv 1 \cdot 3^7 \equiv 81 \cdot 27 \equiv 87 \pmod{100}.$$

Ако је $a_n \equiv 87 \pmod{100}$, тада је $a_n = 100k + 87 = 20(5k+4) + 7$, одакле је

$$a_{n+1} = 3^{a_n} = 3^{100k+87} = 3^{20^{5k+4}} \cdot 3^7 \equiv 3^7 \equiv 87 \pmod{100},$$

па слиједи $a_n \equiv 87 \pmod{100}$, односно индукцијом важи $a_n \equiv 87 \pmod{100}$ за све $n \geq 3$. Дакле, $a_{2008} \equiv 87 \pmod{100}$, тј. a_{2008} завршава цифрама 87. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

366

Доказати да постоји бесконачно много природних бројева n за које се скуп дјелилаца броја n може подијелити на дисјунктне скупове (бар два) такве да је збир елемената у сваком од тих скупова потпун квадрат.

Доказ. Потражимо такве бројеве у облику $n = p^k$ гдје је p прост број. Скуп дјелилаца броја n је тада $\{1, p, p^2, p^3, \ldots, p^k\}$. Подијелимо овај скуп на следеће двочлане подскупове: $\{1, p\}$, $\{p^2, p^3\}$,. . .,$\{p^{k-1}, p^k\}$, гдје смо поставили додатан захтјев да k буде непаран број и $k > 1$. Збир бројева у сваком оваквом подскупу је облика $p^{2i}(1+p)$, па да би ово било потпун квадрат, довољно је да $1 + p$ буде потпун квадрат. Ово је испуњено нпр. за $p = 3$. Дакле, услов из поставке испуњавају сви бројеви облика 3^k за $k > 1$, $2 \nmid k$. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

367

Колико постоји природних бројева $n > 1$ за које је број $a^{25} - a$ дјељив са n за призвољан природан број a?

Нека је n природан број са поменутим својством. Имамо да p^2, при чему је p прост број, не дијели n јер p^2 не дијели ни $p^{25} - p$.

На основу овога n једино можемо представити као производ различитих простих бројева.

С друге стране имамо:

$$2^{25} - 2 = 2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 241$$

Али n није дјељиво са 7 и 241 због тога што:

$$3^{25} \equiv -3 \mod 17$$

$$3^{25} \equiv 32 \mod 241$$

.

На основу Фермаове мале теореме имамо да је $a^{25} \equiv a \mod p$ када је $p = 2, 3, 5, 7, 13$. Због тога имамо да n треба бити једнако свим дјелиоцима броја $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$ који су различити од 1. Таквих бројева има $2^5 - 1 = 31$.

Доказ. □

(**Андрија Бошковић 14/19 Б**) задатак преузет са `https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

368

●●●●

Пронаћи све природне бројеве n такве да 7 дијели $2^n - 1$, а затим показати да за било који природан број n број $2^n + 1$ није дјељив са 7.

Доказ. На основу Фермаове мале тереме имамо:

$$2^6 \equiv 1 \pmod 7$$

.

Ово нам указује да

$$7 \mid (2^3 - 1)(2^3 + 1)$$

,

па онда знамо да

$$2^3 \equiv 1 \pmod 7$$

.

Стога сви бројеви n који су дјељиви са 3 одговарају услову задатка.

Нека је $n = 3k + r$ гдје је $r = 1$ или $r = 2$. Онда:

$$2^n = 2^{3k+r} = (2^3)^k \cdot 2^r \equiv 2 \pmod 7$$

или

$$2^n = 2^{3k+r} = (2^3)^k \cdot 2^r \equiv 4 \pmod 7$$

Стога не можемо пронаћи n такво да $2^n \equiv -1 \pmod 7$.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са `https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

369

●●●●

Доказати да важи:

$$\varphi(5186) = \varphi(5187) = \varphi(5188).$$

Доказ. Најприје ћемо да раставимо бројеве 5186, 5187 и 5188 на просте чиниоце. Провјеравање да ли је неки број прост може бити јако напорно, па је често корисно користити **табеле простих бројева**.
Добијамо:

$$5186 = 2 \cdot 2593$$

$$5187 = 3 \cdot 7 \cdot 13 \cdot 19$$

$$5188 = 2^2 \cdot 1297$$

Примијенићемо мултипликативност Ојлерове функције:

$$\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b),$$

гдје је нзд$(a, b) = 1$, што је у нашем случају испуњено јер смо раставили дате бројеве на просте чиниоце.
Тада имамо:

$$\varphi(5186) = \varphi(2 \cdot 2593) = \varphi(2) \cdot \varphi(2593) = (2^1 - 2^0) \cdot (2593^1 - 2593^0) = 1 \cdot 2592 = 2592$$

$$\varphi(5187) = \varphi(3 \cdot 7 \cdot 13 \cdot 19) = \varphi(3) \cdot \varphi(7) \cdot \varphi(13) \cdot \varphi(19)$$

$$= (3^1 - 3^0) \cdot (7^1 - 7^0) \cdot (13^1 - 13^0) \cdot (19^1 - 19^0) = 2 \cdot 6 \cdot 12 \cdot 18 = 2592$$

$$\varphi(5188) = \varphi(4 \cdot 1297) = (4 \cdot (1 - \frac{1}{2})) \cdot (1297^1 - 1297^0) = 2 \cdot 1296 = 2592.$$

$\square$

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`http://gauss.math.luc.edu/greicius/Math201/Fall2012/Exercises/euler-phi.pdf`

370
●●●●

Да ли једначина $x^4{}_1 + x^4{}_2 + ... + x^4{}_{14} = 1599$ има рјешења у скупу цијелих бројева?

Доказ. Ако је x природан број онда су могући остаци при дијељењу броја x са 16 из скупа $\{0, 1, 2, ..., 15\}$. Тада је:

$$x^2 \equiv k \pmod{16} k \in \{0, 1, 4, 9\}.$$

Из тога следи да је:

$$x^4 \equiv 0 \pmod{16}^4 \equiv 1 \pmod{16}$$

. Због тога збир $x^4{}_1 + x^4{}_2 + ... + x^4{}_{14}$ при дељењу са 16 може дати било који остатак из скупа $\{0, 1, 2, ..., 13, 14\}$, али не и број 15. Како је $1599 \equiv 15 \pmod{16}$, то дата једначина нема рјешења у скупу цијелих бројева. $\square$

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

371

Одредити све природне бројеве чија је вредност једнака збиру квадрата његових цифара у децималном запису.

Доказ. Разликују се следећи случајеви:
1) Ако је тражени број x једноцифрен, онда је $x = x^2$, па је $x = 1$.
2) Уколико је тражени број двоцифрен, онда је $10x + y = x^2 + y^2$, што је еквивалентно са $x(10-x) = y(y-1)$. Како је $y(y-1)$ паран број, то је и x парна цифра. За $x \in \{2, 4, 6, 8\}$ број $x(10-x)$ је једнак или 18 или 24, а они очигледно не представљају производ два узастопна природна броја.
3) Ако је тражени број троцифрен, онда је $100x+10y+z = x^2+y^2+z^2$. Како је $100x+10y+z = x^2 + y^2 + z^2 \leqslant 3 * 81 = 243$ то је $x = 1$ или $x = 2$.
• Ако је $x = 1$, онда је $100+10y+z = 1+y^2+z^2$ или после сређивања $99+10y+z = y^2+z^2$. Како је $99 > z^2$ и $10y > y^2$, то је лијева страна увек већа од десне па једначина нема рјешења.
•Ако је $x = 2$, онда је $200 + 10y + z = 4 + y^2 + z^2$. Лијева страна једнакости је увек већа од 200, а десна увек мања од 200, па једначина нема рјешења.
4) Уколико је број цифара већи од 3 и једнак k, онда је тражени број увек већи од $10k-1$, а збир квадрата његових цифара мањи од $100k$, па је једнакост могућа само ако је $10k - 1 \leqslant 100k$, или $10k - 3 \leqslant k$, што је немогуће, јер добијена неједнакост не важи ни за једно k веће од 3.

□

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

372

Постоје ли природни бројеви x и y такви да је $x^2 + 4y = 555\ldots555$ (декадни запис броја $555\ldots555$ садржи тачно n петица).

Доказ. Разликују се следећи случајеви:
1) Ако је $n = 1$, онда је $x^2 + 4y = 5$, тј. $x = 1, y = 1$.
2) Ако је $n \geq 2$, онда x може бити паран или непаран број :
2.1) Ако је $x = 2k, (k \in \mathbb{N})$, онда је $x^2 + 4y = 4k^2 + 4y = 4(k^2 + y) = 555\ldots555$, па једначина нема рјешења.
2.2) Ако је $x = 2k + 1, (k \in \mathbb{N})$, онда је $x^2 + 4y = 4k^2 + 4k + 1 + 4y = 555\ldots555$, или $4k^2 + 4k + 4y = 4(k^2 + k + y) = 555\ldots554$. Дакле, $2(k^2 + k + y) = 277\ldots77$. Како је лијева страна једначине паран, а десна непаран број, то једначина нема рјешења.
Према томе једино рјешење проблема је $x = y = n = 1$.

□

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

373

Нека су a и b прородни бројеви. Доказати да постоји бесконачно много природних бројева n таквих да је за сваки прост број p број $a \cdot p^n + b$ сложен.

Доказ. Нека је d највећи заједнички дјелилац бројева a и b. Ако је $d > 1$, онда је за сваки природан број n и прост број p, број $a \cdot p^n + b$ дјељив са d, те је као такав сложен и тврђење задатка је доказано. Дакле, довољно је размотрити случај $d = 1$. Нека је q прост дјелилац броја $a + b$ и r прост дјелилац броја $a \cdot q^{q-1} + b$. Тада је $r \neq q$. Заиста, ако је $r = q$, тада из $r \mid a \cdot q^{q-1} + b$ слиједи $r \mid b$, па из $q \mid a + b$ слиједи $q \mid a$, што је у супротности са $d = 1$. Посматрајмо бројеве n облика $(q-1)(1 + k(r-1))$, гдје је k произвољан природан број. Докажимо да су за овако одабране бројеве n, бројеви $a \cdot p^n + b$ сложени. Ако је $p \neq q$, онда на основу Мале Фермаове теореме имамо

$$a \cdot p^n + b \equiv a \cdot (p^{q-1})^{1+k(r-1)} + b \equiv a + b \equiv 0 \pmod{p}, \qquad (*)$$

док за $p = q$ (због $q \neq r$), на основу исте теореме важи

$$a \cdot p^n + b \equiv a \cdot (q^{r-1})^{k(q-1)} \cdot q^{q-1} + b \equiv a \cdot q^{q-1} + b \equiv 0 \pmod{r}. \qquad (**)$$

Из једнакости $(*)$ и $(**)$ се види, имајући на уму да је $a \cdot p^n + b > max\{q, r\}$, да је број $a \cdot p^n + b$ сложен за сваки прост број p и $n = (q-1) \cdot (1 + k(r-1))$, за $k \in \mathbb{N}$.

☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

374

Одредити све природне бројеве $n > 1$ који имају следеће својство: за сваке двије пермутације $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n)$ скупа $A = \{1, 2, \ldots, n\}$, постоје различити бројеви $i, j \in A$, такви да $n \mid (a_i + b_i) - (a_j + b_j)$.

Доказ. Ако је n непарно, узмимо пермутације $a_i = b_i = i$, за све $i \in A$. Важи: $n \mid (a_i + b_i) - (a_j + b_j) \Rightarrow n \mid 2i - 2j \Rightarrow n \mid i - j$. Међутим, $\mid i - j \mid < n$, па мора бити $i = j$. Према томе, непарни бројеви немају тражено својство. Размотримо сада случај парног n. Нека су $(a_1, a_2, \ldots, a_n)$, $(b_1, b_2, \ldots, b_n)$ произвољне пермутације скупа A. Ако n не дијели једну од разлика $(a_i + b_i) - (a_j + b_j)$, то значи да сви елементи n-торке $(a_1 + b_1, \ldots, a_n + b_n)$ дају различите остатке при дијељењу са n. Збир елемената те n-торке једнак је $n(n+1)$, па је дјељив са n. Са друге стране, $(a_1 + b_1) + \ldots + (a_n + b_n) \equiv 1 + 2 + \ldots + n \pmod{n}$, и $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$, што није дјељиво са n, јер је n парно, и нема заједничких дјелилаца са $n + 1$. Одавде добијамо да су природни бројеви са траженим својством парни. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

375

Доказати да за сваки природан број n постоји природан број x такав да је $2^x - x$ дјељиво са n.

Доказ. Доказујемо индукцијом по n да оваквих x-ева има бесконачно много. За $n = 1$ тврђење важи; претпоставимо да важи за све $n < n_0$, гдје је $n_0 \geq 2$ неки природан број. Узмимо $x = y^2$. Тада је по Ојлеровој теореми $2^x - x = 2^{2^y} - 2^y$ дјељиво са n_0 ако је $2^y - y$ дјељиво са $\phi(n_0)$ и y је довољно велико (нпр. $y \geq n_0$). Такви природни бројеви y постоје према индуктивној претпоставци, одакле слиједи постојање бесконачно много тражених бројева x. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

376

За природан број кажемо да је палиндром ако је једнак броју записаном истим цифрама у обрнутом редосљеду.
а) Наћи највећи петоцифрен палиндром који је дјељив са 101.
б) Наћи највећи број узастопних петоцифрених бројева међу којима нема палиндрома.

Доказ. а) Било који петоцифрени палиндром $abcba$ (a, b, c су цифре) може се приказати у облику

$$abcba = 10001a + 1010b + 100c = 101(99a + 10b + c) + 2a - c.$$

То значи да је тај палиндром дјељив са 101 ако и само ако је $2a - c = 0$ (јер је за било које цифре a и c испуњено $\mid 2a - c \mid < 101$). Једначина $2a = c$ имплицира да је $a \leq 4$. Пошто тражимо највећи број, узећемо да је $a = 4$. Тада је $c = 8$. Како за цифру b немамо никакве услове, то ћемо узети $b = 9$ да бисмо добили највећи могући број. Дакле, тражени број је 49 894.

б) Међу следећих 109 узастопних петоцифрених бројева

$$10\,902,\ 10\,903,\ \ldots,\ 10\,999,\ 11\,000,\ \ldots,\ 11\,009,\ 11010$$

нема палиндрома. Најмањи и највећи петоцифрени палиндроми су редом 10 001 и 99 999. Прије броја 10 001 је само један петоцифрени број, а иза броја 99 999 нема више петоцифрених бројева. Показаћемо да послије било ког петоцифреног палиндрома x, $x \neq 99\,999$, постоји други петоцифрени палиндром облика $x + 100$ или $x + 110$ или $x + 11$. Означимо $x = abcba$. Ако је $c \neq 9$, тада је број

$$x + 100 = ab(c+1)ba$$

палиндром. Ако је $c = 9 \neq b$, број

$$x + 110 = a(b+1)0(b+1)a$$

је палиндром, и коначно ако је $c = b = 9$ (наравно, $a \neq 9$) број

$$x + 11 = (a + 1)000(a + 1)$$

је палиндром. Према томе, највећи могући број узастопних петоцифрених бројева међу којима нема палиндрома је 109.

☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

377

Ради продаје, било је потребно неке од датих 555 парцела подијелити на мање. Притом се свака појединачна парцела могла подијелити или на 3 или на 4 дијела. Са дијељењем парцела се стало када је број парцела био 4 пута већи од броја извршених диоба. Колико је најмање диоба извршено?

Доказ. Дијељењем парцеле на 3 дијела укупан број парцела се повећава за 2, а при диоби на 4 дијела број парцела се повећава за 3. Ако са m означавамо број извршених диоба на 3 дијела, а са n означимо број извршених диоба на 4 дијела, проблем се своди на рјешавање Диафантове једначине $555 + 2m + 3n = 4(m + n)$, односно $2m + n = 555$. Из последње једначине закључујемо да је n непаран, односно $n \in \{1, 3, \ldots, 555\}$, што значи да дата једначина има више рјешења. Нама је потребно да нађемо минимални збир $m + n$, и он се добија за минимално n, јер када се n повећа за 2, m се смањи за 1, па се збир повећава. Дакле, морало је бити учињено бар $1 + 227 = 228$ диоба. ☐

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

378

Нека су $x_1, x_2, \ldots x_{2005}$ природни бројеви такви да је ${x_1}^2 + {x_2}^2 + \ldots + {x_{2005}}^2 = 2035$. Одредити $x_1, x_2, \ldots x_{2005}$.

Доказ. Очигледно је већина бројева x_i једнака 1, а само неки од њих већи од 1. Нека су $x_1, x_2, \ldots x_k \geq 2$, а сви остали $x_{k+1} = x_{k+2} = \ldots = x_{2005} = 1$. Тада је ${x_1}^2 + {x_2}^2 + \ldots + {x_k}^2 \geq 4k$, па је због тога $2035 = ({x_1}^2 + {x_2}^2 + \ldots + {x_k}^2) + ({x_{k+1}}^2 + {x_{k+2}}^2 + \ldots + {x_{2005}}^2) \geq 4k + (2005 - k) = 3k - 2005$. Из неједнакости $2035 \geq 3\breve{}2005$ следи да је $3k \leq 30$, па је $k \leq 10$. Дакле $_{11} = \ldots = _{2005} = 1$, па је ${x_{11}}^2 + {x_{12}}^2 + \ldots + {x_{2005}}^2 = 2005 - 10 = 1995$. Према томе ${x_1}^2 + {x_2}^2 + \ldots + {x_{10}}^2 = 2035 - 1995 = 40$.

Ако у скупу $\{x_1, x_2, \ldots, x_{10}\}$ има a јединица, b двојки, c тројки, d четворки, e петица и f шестица, онда је: $a+b+c+d+e+f = 10$ и $a+4b+9c+16d+25e+36f = 40$. Ако се од друге одузме прва једначина добије се линеарна Диофантова једначина $b+8c+15d+24e+35f = 30$. Одмах је јасно да је $f = 0$. Ако је $e = 1$, онда је $3b + 8 + 15d = 7$. У том случају би било $b = 2$, а сви остали би били 0, па би било $a + b + c + d + e + f = 3$, што је немогуће, јер тај збир износи 10. Дакле $e = 0$, па је $3b + 8 + 15d = 30$. Како су 3b, 15d и 30 дјељиви са 3, то мора бити и 8c, па се разликују два случаја $c = 3$ или $c = 0$.

1) Ако је $c = 3$, онда је $3b + 24 + 15d = 30$, па је $b + 5d = 2$ и има једно рјешење:

- $b = 2$ и $d = 0$, $c = 3$, $e = f = 0$, $= 5$, па је $3^2+3^2+3^2+2^2+2^2+1^2+\ldots+1^2 = 27+8+2000 = 2035$ (3 тројке, 2 двојке и 2000 јединица);

2) Ако је $= 0$, онда је $3b + 15d = 30$, па је $b + 5d = 10$ и има три решења:

- $b = 10$, $a = c = d = e = f = 0$, па је $2^2 + \ldots + 2^2 + 1^2 + \ldots + 1^2 = 40 + 1995 = 2035$(10 двојки и 1995 јединица);
- $b = 5$ и $d = 1$, $c = e = f = 0$, $a = 4$, па је $4^2+2^2++\ldots 2^2+1^2+\ldots+1^2 = 16+20+1999 = 2035$ (1 четворка, 5 двојки и 1999 јединица);
- $b = 0$ и $d = 2$, $c = e = f = 0$, $a = 8$, па је $4^2 + 4^2 + 1^2 + \ldots + 1^2 = 32 + 2003 = 2035$ (2 четворке и 2003 јединица);

□

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

379
●●●●

Опште рјешење једначине $x^2 + y^2 + z^2 = t^2$ у скупу природних бројева дефинисано је следећим релацијама:

$$x = 2, \qquad y = 2q, \qquad z = \frac{p^2 + q^2 - r^2}{r} \qquad t = \frac{p^2 + q^2 + r^2}{r}$$

где су p, q и r природни бројеви који испуњавају следеће услове:

$$(1) r \mid {}^2 + q^2, \qquad (2) p^2 + q^2 \geq r^2.$$

Доказати.

Доказ. Како број t^2 при дијељењу са 4 даје остатак 0 или 1, то и лијева страна једнакости мора имати исти остатак при дељењу са 4. Јасно је да ако је t паран онда и x, y и z морају бити парни, па се дијељењем једначине са 4 (једном, два, или више пута), опет на крају долази до случаја када је t непаран. Тада је очигледно да су два од три броја x, y и z парни, а један непаран.

Нека је $x = 2p$ и $y = 2q$. Нека је z непаран. Како је $t > z$ и како су оба непарна то је њихова разлика паран број, тј. $t - z = 2r$ или $t = 2r + z$. Како је $x^2 + y^2 + z^2 = t^2$, то је $x^2 + y^2 = 4p^2 + 4q^2 = t^2 - z^2 = (t - z)(t + z) = 2r(2r + z + z) = 4r^2 + 4rz$.

Из једнакости $4^2 + 4q^2 = 4r^2 + 4rz$ слиједи да је $p^2 + q^2 - r^2 = rz$. Тада је $z = \frac{p^2+q^2-r^2}{r}$ уз услове:

(1) збир $p^2 + q^2$ је дјељив са r;
(2) $p^2 + q^2 \geq r^2$.

□

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

380

●●●●

Доказати да је број $2^{2^n-1} - 2^n - 1$ сложен за све природне бројеве $n > 2$.

Доказ. За парно n важи $a_n = 2^{2^n-1} - 2^n - 1 \equiv 2 - 1 - 1 = 0 \pmod 3$. Даље, за $n \equiv 1 \pmod 4, (n > 1)$ је $2^{2^n-1} \equiv 2^3$ и $2^n \equiv 2 \pmod 5$, па је $5 \mid a_n$.
Нека је k природан број такав да $2^k \mid n+1$. Тврдимо да је тада a_n дјељиво са $2^{2^k}+1$.Заиста, $2^{2^k}+1 \mid 2^{n+1}+1$, па је $2a_n = 2^{2^n} - 2^{n+1} - 2 \equiv 1 + 1 - 2 = 0 \pmod{2^{2^k}+1}$. □

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://imomath.com/`

381

●●●●

Доказати да за сваки природан број s, постоји природан број n чији је збир цифара s и $s \mid n$.

Доказ. Нека је

$$n = 10^{s\varphi(s)} + 10^{(s-1)\varphi(s)} + \cdots + 10^{\varphi(s)}$$

.

Јасно је да је збир цифара броја n заиста s. Покажимо да је дати број дјељив са s.

$$n = (10^{s\varphi(s)} - 1) + (10^{(s-1)\varphi(s)} - 1) + \cdots + (10^{\varphi(s)} - 1) + s$$

је дјељив са s, на основу Ојлерове теореме.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

382

●●●●

Нека је $n > 3$ неки непаран природан број $n = {p_1}^{\alpha_1} \ldots {p_k}^{\alpha_k}$ гдје су $p_1 ... p_k$ прости бројеви. Ако важи

$$m = n \cdot (1 - \frac{1}{p_1}) \cdot ... \cdot (1 - \frac{1}{p_k})$$

доказати да постоји прост број p такав да p дијели $2^m - 1$, али не дијели m.

Доказ. Како је $m = \varphi(n)$ и n је непарно, на основу Олерове теореме знамо да n дијели $2^m - 1$. Имамо сада два случаја.

Први, нека је $n = p^r$ за неки прост број p. На основу поставке имамо да је $m = p^r - p^{r-1}$ паран број који је већи од 3.

Како p дијели

$$(2^m - 1) = (2^{\frac{m}{2}} - 1)(2^{\frac{m}{2}} + 1),$$

онда он дијели и неки од дата два чиниоца. Како је то случај можемо онда изабрати неки нови прост број који ће дијелити преостали чинилац. Јасно је да онда дати чинилац неће дијелити онај чинилац који дијели p. Како знамо да је $n = p^r$ онда знамо да нови прост број неће дијелити n, а самим тим ни m.

Нека у другом случају n буде сачињен од најмање два проста фактора. Знајући то закључујемо да ће m бити дјељиво са 4.

Такође за произвољан прост фактор p који је садржан у n имамо да $p-1$ дијели $\frac{m}{2}$. На основу Мале Фермаове теореме имамо да p такође дијели и $2^m - 1$.

Како дато тврђење важи за све просте чиниоце броја n, онда ниједан од њих неће дијелити $2^{\frac{m}{2}} + 1$. Нека је p_1 прост број који дијели $2^{\frac{m}{2}} + 1$. Јасно је да тај број самим тим дијели и $2^m - 1$. Али уочавамо да дати број не дијели n па самим тим ни m.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://matek.fazekas.hu/images/konyvek/andreescu-andrica-problems-on-number-theory.pdf`

383 ●●●●

Одредити природне бројеве x и y тако да је $x^y = y^x$.

Доказ. Примијетимо одмах двије чињенице:
Тривијално рјешење једначине је $x = y$ и једначина је симетрична. Зато се, не умањујући општост, може препоставити да је $x \leqslant y$. Тада постоји ненегативан цио број a, такав да је $y = x + a$. Слиједи да је $x^{x+a} = (x+a)^x$. Одавде је $x^a = (\frac{x+a}{x})^x$. Како је лијева страна једнакости природан број то мора бити и десна, па је $x + a = y$ дјељиво са x. Дакле $y = kx, (k \in \mathbb{N})$.
Тада је $x^{kx} = (kx)^x$, па је $x^k = kx$ па је $x^{k-1} = k$. Разликују се следећи случајеви:
1) Ако је $x = 1$, онда је $k = 1$, па је је $y = kx = x$. (тривијално рјешење)
2) Ако је $x > 1$ онда је и $k > 1$, па је:.
• За $k = 2$, слиједи $x = 2$, па је $y = kx = 4$.
• Ако је $k \geq 3$, онда је $x^{k-1} - 1 = (x-1)(x^{k-2} + x^{k-3} + \ldots + x + 1) \geq 2(k-1) = 2k - 2$. Како је $2k - 2 > k - 1$, то је $x^{k-1} - 1 > k - 1$, па је $x^{k-1} > k$ и једначина нема више рјешења у скупу природних бројева.
Водећи рачуна о симетричности једначине закључујемо да су сва рјешења једначине $(x, y) \in \{(2,4); (4,2); (1,1); (2,2), (3,3)\ldots\}$. То значи да једначина има бесконачно много рјешења.

□

(**Сања Лончар 7/19 Б**) задатак преузет са
Мала збирка Диофантових једначина-Војислав Илић

384

Ако су $p-1$ и $p+1$ прости бројеви, $p>4$, доказати да важи:

$$3\varphi(p) \leq p.$$

Доказ. Уочимо да за $p>4$, p је дјељив са 6. То је зато што су прости бројеви већи од 3 облика $6k+1$ или $6k-1$, што је раније доказано.
Зато је

$$p = 2^a 3^b m$$

гдје су $a, b \geq 1$, нзд$(m,6) = 1$.

$$\varphi(p) = \varphi(2^a 3^b m)$$

Користимо мултипликативност Ојлерове функције.

$$\varphi(p) \leq \varphi(2^a)\varphi(3^b)\varphi(m) \leq 2^{a-1} \cdot 2 \cdot 3^{b-1} \cdot m = 2^a 3^{b-1} m = \frac{p}{3}$$

Слиједи да је:

$$3 \cdot \varphi(p) = p$$

$\square$

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

385

Показати да за $n = 2(2p-1)$ важи да је $\phi(n) = \phi(n+2)$ када су и p и $2p-1$ непарни прости бројеви.

Доказ. Нека важи претпоставка да је $n = 2(2p-1)$ и да су p и $2p-1$ непарни прости бројеви.

Пошто су 2 и $2p-1$ узајамно прости, онда важи:

$$\phi(n) = \phi(2)\phi(2p-1) = 2p-2$$

$$\phi(n+2) = \phi(2(2p-1)+2) = \phi(4p) = \phi(4)\phi(p) = 2(p-1) = 2p-2$$

$\square$

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-m`
`pdf`

386

Показати да ако природан број n има r различитих непарних простих фактора, онда $2^r \mid \phi(n)$.

Доказ. Ако n има r различитих непарних простих фактора, можемо га представити као $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, гдје је $k_i \geqslant 1$. Сада је:

$$\phi(n) = \phi(p_1^{k_1})\phi(p_2^{k_2}) \cdots \phi(p_r^{k_r}) = p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1) \cdots p_r^{k_r-1}(p_r-1)$$

Како је p_j непарно, $\forall j \in \{1, 2, \ldots, r\}$ важи да је $p_j - 1$ парно, што значи да је и $\phi(p_j^{k_j})$ парно. Поошто је ових функција r, важи да $2^r \mid \phi(n)$, што је и требало доказати. □

(**Маријана Велетић 19/19 Ц**)задатак преузет са `https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-m` `pdf`

387

Доказати да важе следећа тврђења:

(а) Постоји бесконачно много природних бројева n за које је $\phi(n) = \frac{n}{3}$.

(б) Нема природних бројева n за које је $\phi(n) = \frac{n}{4}$.

Доказ. (а) Посматрајмо приподне бројеве $n = 2^k 3^j$, за $k, j > 0$. Примијетимо да је

$$\phi(n) = \phi(2^k 3^j) = 2^{k-1} \cdot 1 \cdot 3^{j-1} \cdot 2 = 2^k 3^{j-1} = \frac{2^k \cdot 3^j}{3} = \frac{n}{3}$$

Пошто су k и j произвољно одабрани, доказ важи у општем случају, па постоји бесконачно много природних бројева n за које је $\phi(n) = \frac{n}{3}$.

(б) Претпоставимо супротно - да постоји природан број n за који је $\phi(n) = \frac{n}{4}$. Како знамо да је $\phi(n)$ цио број, то значи да је n дјељиво са 4.

Претпоставимо да n има непаран прост дјелилац, и нека је p_r највећи такав број. Запишимо n у облику $n = 2^{k_0} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, k_i \geqslant 1$.

$$\phi(n) = 2^{k_0-1} p_1^{k_1-1}(p_1-1)p_2^{k_2-1}(p_2-1) \cdots p_r^{k_r-1}(p_r-1) = \frac{n}{4} = 2^{k_0-2} p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$$

Пошто p_r не дијели ниједан од бројева $p_i - 1$, за $i < r$ (јер је већи од њих), што ће рећи ниједно $\phi(p_i^{k_i})$, а експоненти броја p_r су такође различити, закључујемо да оваква једнакост није могућа.

Одавде закључујемо да n нема непарних простих дјелилаца, тј. да је n степен двојке.

Нека је $n = 2^k$. Тада је

$$\phi(n) = \phi(2^k) = 2^{k-1} \neq 2^{k-2} = \frac{n}{4}$$

Дакле, и овакво $\phi(n)$ је немогуће, па закључујемо да нема природних бројева n са својством да је $\phi(n) = \frac{n}{4}$. □

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-m`
`pdf`

388

(а) Ако сваки прост број који дијели n дијели и m, показати да је $\phi(nm) = n\phi(m)$.

(б) Ако је p прост број и $k \geqslant 2$, показати да је $\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2)$

Доказ. (а) Ако сваки прост број који дијели n дијели и m, онда је

$$\phi(nm) = nm \prod_{p|nm} (1 - \frac{1}{p})$$

Производ узима само вриједности простих бројева који дијеле mn. На основу услова задатка, ови прости бројеви дијеле и само m па важи и следеће:

$$\phi(nm) = nm \prod_{p|m} (1 - \frac{1}{p})$$

Али

$$n(m(\prod_{p|m}(1 - \frac{1}{p}))) = n\phi(m)$$

па смо овим показали да је $\phi(nm) = n\phi(m)$.

(б) Присјетимо се да је $\phi(p^k) = p^{k-1}(p-1)$ и примијетимо да су p^{k-1} и $p-1$ релативно прости бројеви. Видимо да је

$$\phi(\phi(p^k)) = \phi(p^{k-1}(p-1)) = \phi(p^{k-1})\phi(p-1) = p^{k-2}(p-1)\phi(p-1)$$

Користећи се тврђењем под (а), за $m = n$ (пошто m и n имају исте просте дјелиоце) добијамо да је

$$\phi(n^2) = \phi(nm) = n\phi(m) = n\phi(n)$$

Одатле је $\phi((p-1)^2) = (p-1)\phi(p-1)$ па закључујемо да је

$$\phi(\phi(p^k)) = p^{k-2}\phi((p-1)^2)$$

□

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-m`
`pdf`

389

●●●●

Наћи најмањи природан број $a > 2$ такав да $2 \mid a$, $3 \mid a+1$, $4 \mid a+2$, $5 \mid a+3$, $6 \mid a+4$.

Доказ. Вриједи:

$$2 \mid a \Rightarrow a \equiv 0 \pmod 2$$

$$3 \mid a+1 \Rightarrow a \equiv -1 \equiv 2 \pmod 3$$

$$4 \mid a+2 \Rightarrow a \equiv -2 \equiv 2 \pmod 4$$

$$5 \mid a+3 \Rightarrow a \equiv -3 \equiv 2 \pmod 5$$

$$6 \mid a+4 \Rightarrow a \equiv -4 \equiv 2 \pmod 6$$

Како је $a > 0$ и $2 \mid a$ видимо да $2 \mid (a-2)$. Дакле:

$2 \mid (a-2) \wedge 3 \mid (a-2) \wedge 4 \mid (a-2) \wedge 6 \mid (a-2)$

$\Rightarrow$ нзс$(2,3,4,6) \mid (a-2)$

$\Rightarrow 12 \mid (a-2)$

Ријешимо систем:

$a \equiv 2 \pmod{12}$
$a \equiv 2 \pmod 5$

нзд$(m_1, m_2) =$ нзд$(12,5) = 1$

$m = m_1 \cdot m_2 = 60$

$n_1 = \frac{m}{m_1} = 5$

$n_2 = \frac{m}{m_2} = 12$

- $5x \equiv 2 \pmod{12}$

  $\Rightarrow x_1 = 10$
- $12x \equiv 2 \pmod 5$

  $\Rightarrow x_2 = 6$

Решење $x_0 = n_1 \cdot x_1 + n_2 \cdot x_2 = 5 \cdot 10 + 12 \cdot 6 = 122 \equiv 2 \equiv 62 \pmod{60}$

Дакле, најмањи број $a > 2$ који задовољава наведене услове је $a = 62$ □

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-mo`
`pdf`

390

Да ли постоји низ од 21 узастопних природних бројева такав да је сваки од њих дјељив макар са једним простим бројем $p, 3 \leqslant p \leqslant 13$?

Доказ. У оваквом низу мора постојати 10 или 11 парних бројева. Не умањујући општост, претпоставићемо да се ради о низу који има 11 парних бројева. Сада наше питање постаје еквивалентно питању: "Да ли постоји низ од 10 узастопних *непарних* природних бројева такав да је сваки од њих дјељив макар са једним простим бројем $p, 3 \leqslant p \leqslant 13$?"

Међу 10 узастопних непарних природних бројева важи:

3 или 4 су дјељива са 3

2 су дјељива са 5

1 или 2 су дјељива са 7

0 или 1 су дјељиви са 11

0 или 1 су дјељиви са 13

Да би сваки од њих био дјељив макар са једним од наведених простих бројева, 4 морају бити садржаоци броја 3, 2 садржаоци броја 5, 2 садржаоци броја 7, 1 садржаоц броја 11 и 1 садржаоц броја 13. При томе, ниједан од ових бројева није садржаоц било која два наведена проста броја.

Да би у описаном низу од 10 бројева који можемо означити са $a_1 a_2 \ldots a_{10}$ постојала 4 дјељива са 3, то морају бити a_1, a_4, a_7 и a_{10}. Ови бројеви нису садржаоци бројева 5,7,11 и 13. Једина могућност која остаје за садржаоце броја 7 су чланови a_2 и a_9, па нам то оставља a_3 и a_8 као могућност за оне дјељиве са петицом. a_5 и a_6 су дјељиви са 11 и 13, у било ком редосљеду.

Дакле, постоји оваква секвенца бројева. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%`
`20Contests.pdf`

391

Доказати да једначина $x^2 - 2y^2 + 8z = 3$ нема решење у скупу позитивних цијелих бројева

Доказ. Решаваћемо ову једначину по $\pmod 8$.

Ако је y парно, тада једначина $x^2 = 2y^2 - 8z + 3$ даје остатак 3 при дијељењу са 8, што није могуће.

Ако је y непарно, тада је $y = 2k + 1, k \geqslant 0$, па је једначина облика $x^2 = 2 + 8k^2 - 8z + 3 = 8k^2 - 8z + 5$, што даје остатак 5 при дијељењу са 8. Како је x у овом случају непаран број, а за непарно x је $x^2 \equiv 1 \pmod 8$, и овај случај је немогућ. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://www.isinj.com/mt-usamo/250%20Problems%20in%20Elementary%20Number%20Theory%20-%20Sierpinski%20(1970).pdf`

392

Ако су a и b релативно прости природни бројеви, доказати да Диофантова једначина $ax - by = c$ има бесконачно много решења у скупу позитивних цијелих бројева.

Доказ. Како је нзд$(a, b) = 1$, а 1 дијели $c, \forall c$, закључујемо да једначина има решење. Покажимо да их има бесконачно много у скупу позитивних цијелих бројева.

Ако је пар (x_0, y_0) партикуларно решење ове једначине, онда је опште решење облика

$$x = x_0 - bt$$

$$y = y_0 - at$$

, $t \in Z$

Провјеримо:

$$a(x_0 - bt) - b(y_0 - at) = ax_0 - abt - by_0 + abt = ax_0 - by_0 = c$$

Сада треба показати да су за бесконачно много цијелих бројева t, x и y позитивни цијели бројеви.

Узмимо t тако да је $t < -\frac{|x_0|}{b}$ и $t < -\frac{|y_0|}{a}$. За овако одабрано t важи да су $x, y > 0$ и да је (x, y) решење једначине $ax - by = c$.

Постоји бесконачно много цјелобројних решења ове једначине јер постоји и бесконачно много бројева t који се могу конструисати како је наведено. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-m`
`pdf`

393

Показати да је

$$2903^n - 803^n - 464^n + 261^n$$

дјељив са 1897 за све природне бројеве n.

Доказ. Прво ћемо доказати да важи:

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots xy^{n-2} + y^{n-1})$$

тј. да $x - y$ дијели $x^n - y^n$, за свако n.
Претпоставићемо да је $x \neq y$, $xy \neq 0$. Без овакве претпоставке, теорема је безначајна. Под овом претпоставком, једнакост коју доказујемо слиједи директно из идентитета:

$$\sum_{k=0}^{n-1} a^k = \frac{a^n - 1}{a - 1}, a \neq 1,$$

постављајући да је $a = \frac{x}{y}$, а затим множећи читаву једнакост са y^n.
Користећи претходни доказ, знамо да је $2903^n - 803^n$ дјељиво са $2903 - 803 = 2100 = 7 \cdot 300$ и да је $261^n - 464^n$ дјељиво са $261 - 464 = -203 = 7 \cdot (-29)$. Закључујемо да је $2903^n - 803^n - 464^n + 261^n$ дјељиво са 7.
Такође, $2903^n - 464^n$ је дјељиво са $2903 - 464 = 9 \cdot 271$ и $261^n - 803^n$ је дјељиво са $-542 = (-2) \cdot 271$. Закључујемо да је израз $2903^n - 803^n - 464^n + 261^n$ дјељив и са 271.
Како бројеви 7 и 271 немају заједничких простих чинилаца, закључујемо да је израз $2903^n - 803^n - 464^n + 261^n$ дјељив са $7 \cdot 271 = 1897$, што је и требало доказати. □

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

394

Нека је p прост број. Доказати да важи:
а) $\binom{p-1}{n} \equiv (-1)^n \pmod{p}$, $1 \leq n \leq p-1$,
б) $\binom{p+1}{n} \equiv 0 \pmod{p}$, $2 \leq n \leq p-1$.

Доказ. а) $\binom{p-1}{n} = \frac{(p-1)!}{n! \cdot (p-n-1)!} = \frac{(p-1)(p-2)\ldots(p-n)}{n!}$
Треба да нађемо остатак при дијељењу овог производа са p. Посматраћемо које остатке сваки од чинилаца овог производа даје при дијељењу са p, па ће производ добијених остатака бити резултат који тражимо.
$(p-1)(p-2)\ldots(p-n) \equiv (-1)(-2)\ldots(-n) \equiv (-1)^n n! \pmod{p}$. Тврђење слиједи директно из претходног резултата.
б) На исти начин као под а) имамо:
$(p+1)p(p-1)\ldots(p-n+2) \equiv 1 \cdot 0 \cdot (-1) \cdots (-n+2) \equiv 0 \pmod{p}$. □

(**Лазар Шћекић 6/19 Б**) задатак са интернета
`https://www.fmf.uni-lj.si/~lavric/Santos%20-%20Number%20Theory%20for%20Mathematical%20Contests.pdf`

395

Одредити посљедње двије цифре броја 49^{19}.

Доказ. Како је нзд$(25, 4) = 1$ то, на основу Кинеске теореме о остацима, имамо да $x = 49^{19} \pmod{100}$ можемо записати у сљедећем облику конгруенција:

$$x = 49^{19} \pmod{25}$$
$$x = 49^{19} \pmod{4}.$$

$$49^{19} \equiv (-1)^{19} \equiv -1 \pmod{25}$$
$$49^{19} \equiv (-1)^{19} \equiv -1 \pmod{4}.$$

На основу теореме закључујемо да:

$$x = 49 \pmod{100}$$

Стога су посљедње двије цифре датог броја 49.

□

(**Андрија Бошковић 14/19 Б**) задатак преузет са
`https://brilliant.org/wiki/chinese-remainder-theorem/#solving-systems-of-congruences`

396

Дат је 25-цифрен број без деветки у децималном запису. Доказати да можемо да увећамо двије његове једнаке цифре за 1, тако да добијемо број који није дјељив са 7.

Доказ. Претпоставимо супротно. Означимо дати број са $n = \overline{a_{24}a_{23}\dots a_1 a_0}$. Ако је $a_i = a_j = a_k$ за неке различите i, j, k, онда је $10^i + 10^j \equiv 10^i + 10^k \equiv 10^j + 10^k \equiv -n \pmod{7}$, одакле је $10^i \equiv 10^j \equiv 10^k \equiv -\frac{n}{2} \pmod{7}$. Како је низ $1, 10, 10^2, \dots, 10^24$ периодичан са периодом 6, у њему се сваки остатак по модулу 7 (па тако и $-\frac{n}{2}$) појављује највише пет пута. Слиједи да се највише једна цифра може појавити више од двапут, а ни она не може више од пет пута. Али тада n може да има највише $8 \cdot 2 + 5 = 21$ цифара, контрадикција.

□

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://imomath.com/`

397

Ријешити једначину $2x^2 + 1 = y^2$ у скупу рационалних бројева

Доказ. Пођимо од решења дате једначине $(x_1,y_1)=(0,1)$:
Сва друга решења су дата са $(x, y) = (pt, 1 + qt)$, гдје су p,q цијели и t рационалан. Ако фиксирамо p и q једначина $2x^2 + 1 = y^2$ даје једначину по t: $2p^2t^2 = 2qt + q^2t^2$, одакле је t=0 или $t = \frac{2q}{2p^2-q^2}$. Сада добијамо:

$$x = \frac{2pq}{2p^2-q^2}$$
$$y = \frac{2p^2+q^2}{2p^2-q^2}$$

$\square$

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/UTB4.pdf`

398

За неки природан број n, $n > 3$, нека је S збир цифара броја $1+2+\ldots+n$. Ако у декадном запису броја S учествују све исте цифре, која цифра то може бити?

Доказ. Нека је тражена цифра једнака a. Како је $1 + 2 + \ldots + n = \frac{n(n+1)}{2}$, тада би важило да је $\frac{n(n+1)}{2} = a \cdot \underbrace{11\ldots1}_{k}$, $k > 1$, односно

$$(2n + 1)^2 = 8 \cdot \frac{n(n+1)}{2} + 1 = 8 \cdot a \cdot \underbrace{11\ldots1}_{k}+1.$$

Ако је $a \in \{2, 4, 7, 9\}$ број на десној страни претходне једнакости завршава се са 3 или 7, а то није могуће пошто је он потпун квадрат. Ако је пак $a \in \{3, 8\}$ онда је двоцифрени завршетак броја $8 \cdot a \cdot \underbrace{11\ldots1}_{k}+1$ једнак 65 или 05. Међутим ово није могуће јер би се тада број $2n + 1$ завршавао цифром 5, а његов квадрат са 25 (због $(10l + 5)^2 = 100(l^2 + l) + 25$). Дакле, остају нам могућности $a = 1$, $a = 5$ и $a = 6$. Докажимо да није могуће $a = 1$. Претпоставимо да је $\frac{n(n+1)}{2} = \frac{10^k-1}{9}$ за неко $k > 1$. Отуда је

$$2 \cdot 10^k = 9n^2 + 9n + 2 = (3n + 1)(3n + 2).$$

Како су бројеви $3n + 1$ и $3n + 2$ узајамно прости, то један од њих мора бити степен двојке, а други степен петице. Међутим, како је

$$5^k - 2^{k+1} > 2^{2k} - 2^{k+1} \geq 2^{k+2} - 2^{k+1} = 2^{k+1} \geq 8,$$

то бројеви 5^k и 2^{k+1} не могу бити узастопни, те тражена цифра није једнака 1.
Очигледно, могуће је $a = 5$, јер је $\frac{10\cdot11}{2} = 55$, као и $a = 6$, пошто је $\frac{11\cdot12}{2} = 66$. Из свега наведеног закључујемо да је тражена цифра 5 или 6.

$\square$

(**Александар Вујовић 4/19 Б**) задатак преузет са
`https://imomath.com/srb`

399

Низ бројева формира се на следећи начин:
први члан низа је број 3^{1996}; сваки следећи, почев од другог, једнак је збиру цифара претходног.
Наћи број који се налази на 1996. мјесту.

Доказ. Јасно да сваки члан тога низа мора бити дјељив са 9. Нека јеa_n означен n-ти члан тога низа. Како $3^2 < 10$ имамо да је $3^{1996} < 10^{998}$, па a_1 има највише 998 цифара. Значи његова сума цифара није већа од $998 \cdot 9 = 8929 > a_2$. Сада је јасно да је $a_3 \leqslant 8+8+9+9 = 34$, па је $a_4 \leqslant 9$. Јасно да је $a_n \leqslant 9$, за свако $n \geq 4$, па како је $9 \mid a_{1996}$, то је $a_{1996} = 9$. ☐

(**Сања Лончар 7/19 Б**) задатак преузет са
`https://imomath.com/srb/dodatne/uvodkongr_mr.pdf`

400

Наћи остатак при дијељењу броја 2^{40} са 77.

Доказ. Задатак ћемо ријешити користећи Кинеску теорему о остацима.

Примијетимо да је $77 = 7 \cdot 11$. Формираћемо двије једначине да бисмо добили одговарајуће остатке.

$$2^{40} \equiv a \pmod 7$$

$$2^{40} \equiv b \pmod{11}$$

Примијетимо да је $\phi(7) = 6$ а $\phi(11) = 10$.

$2^{40} = 2^{36} \cdot 2^4$. Примијетимо да је 36 степен броја 6 ($6 = \phi(7)$), а како су 2 и 7 можемо примијенити Фермаову теорему. Закључујемо да је $2^6 \equiv 1 \pmod 7$. Лако се види да је $2^4 \equiv 2 \pmod 7$. Користећи својства конгруенције видимо да је остатак $dot2 = 2$.

Сличним резоновањем закључујемо да је остатак при дијељењу 2^{40} са 11 једнак 1 јер је $2^{10} \equiv 1 \pmod{11}$.

Сада, на основу Кинеске теореме о остацима, коначно решење је облика $7x+2$ или $11y+1$.

$7x + 2 = 11y + 1 \Rightarrow 7x + 1 = 11y \Rightarrow x = 2, y = 3$.

Коначно решење је: $7x + 2 = 7 \cdot 3 + 2 = \mathbf{23}$. ☐

(**Маријана Велетић 19/19 Ц**)задатак преузет са

401

Ако је $x \equiv a \pmod{n}$ доказати да је или $x \equiv a \pmod{2n}$ или $x \equiv a + n \pmod{n}$.

Доказ. Како је $x \equiv a \pmod{n}$ слиједи да је $x = a + tn, t \in Z$.

- Ако је t парно, онда је $t = 2r, r \in Z$.

  Тада је $x = a + 2rn = a + r(2n) \Rightarrow x \equiv a \pmod{2n}$

- Ако је t непарно, онда је $t = 2r + 1, r \in Z$.

  Тада је $x = a + (2r + 1)n = a + n + r(2n) \Rightarrow x \equiv a + n \pmod{n}$

□

(**Маријана Велетић 19/19 Ц**)задатак преузет са
`https://cdchester.co.uk/wp-content/uploads/2018/02/david-m-burton-elementary-number-theory-mo`
`pdf`

402

(Мултипликативност Ојлерове функције) Нека су m и n узајамно прости природни бројеви. Доказати

$$\phi(mn) = \phi(m)\phi(n).$$

Доказ. Прво се подсјетимо дефиниције групе R_k и дефиниције Ојлерове функције

$$R_k = \{a \in \mathbb{Z}_k \mid \text{нзд}(a, k) = 1\}$$
$$\phi(k) = |R_k|$$

Нека су $R_m = \{r_1, r_2, \ldots, r_{\phi(m)}\}$ и $R_n = \{s_1, s_2, \ldots, s_{\phi(n)}\}$. Посматрајмо скуп

$$T = \{nr + ms \mid r \in R_m, \; s \in R_n\}$$

и примјетимо да је $|T| = \phi(m)\phi(n)$. Доказаћемо да је $T = R_{mn}$. Доказ изводимо у 3 корака

1. Сваки елемент скупа T је узајамно прост са mn
2. Не постоје два различита елемента из T која су конгруентна по модулу mn
3. Сваки цио број који је узајамно прост са mn је конгруентан неком елементу скупа T

Нека је p прост дјелилац броја нзд$(nr + ms, mn)$ гдје су $r \in R_m,\ s \in R_n$. Како $p \mid mn$ и нзд$(m, n) = 1$ закључујемо да или $p \mid m$ или $p \mid n$. Без губљења општости претпоставимо $p \mid m$. Одатле даље добијамо

$$p \mid nr + ms \implies p \mid nr \overset{\text{нзд}(p,n)=1}{\implies} p \mid r$$

Дакле,

$$p \mid r,\ p \mid m \implies p \mid \text{нзд}(m, r) = 1$$

што је контрадикција. Тиме смо доказали (1).

Нека је $nr + ms \equiv nr' + ms' \pmod{mn}$ гдје су $r, r' \in R_m, s, s' \in R_n$. Даље,

$$n(r - r') + m(s - s') = k(mn),\ k \in \mathbb{Z}$$

Одавде лако добијамо да

$$m \mid n(r - r')$$

и како важи нзд$(m, n) = 1$ онда

$$m \mid r - r' \iff r \equiv r' \pmod{m}.$$

Међутим како $r, r' \in R_m$ онда је $r = r'$. Слично за n добијамо $s = s'$. Дакле тиме смо доказали и (2).

Сада доказујемо (3). Нека је $k \in \mathbb{Z}$, нзд$(k, mn) = 1$. Из Безуовог идентитета добијамо

$$k = nr' + ms'$$

Докажимо да је нзд$(r', m) = 1$ и нзд$(s', n) = 1$. Претпоставимо супротно постоји прост фактор p такав да $p \mid r'$ и $p \mid m$. Одатле добијамо $p \mid k$ и $p \mid mn$. Контрадикција са нзд$(k, mn) = 1$. Дакле, нзд$(r', m) = 1$.

Истим аргументом доказујемо нзд$(s', n) = 1$. Даље бројеве r' и s' можемо записати на сљедећи начин

$$r' = r + am,\ s' = s + bn,\ \ r \in R_m, s \in R_n$$

па одатле

$$k = nr' + ms' = nr + ms + mn(a + b) \equiv nr + ms \pmod{mn}.$$

Тиме смо комплетирали доказ. □

(**Велимир Ђоровић 5/19 Б**) задатак преузет из материјала за предавања