Марија Станић • Небојша Икодиновић

ТЕОРИЈА БРОЈЕВА
Збирка задатака

2004

Садржај

Предговор

Невероватна комбинација тешко схватљиве природе и опште познате, бар елементарне, примене једног апстрактног појма већ хиљадама година чини број увек интересантном темом за проучавање. Остављајући по страни покушаје дефинисања појма броја, који су прича за себе, само проучавање његових особина је комплексна игра чији се крај не види. У њој равноправно могу учествовати скоро сви којима су познате основне особине и операције, а ако при томе имају и идеју, онда су добри резултати увек могући. Оно што је најинтересантније јесте да већина решења проблема који се тичу бројева изгледају једноставно, али до њих најчешће није лако стићи.

Ова књига има за циљ да представи велики број идеја које ће бити од помоћи свима који се често, са намером или не, сусрећу са задацима за чије је решавање потребно детаљније познавање особина бројева и њихових међусобних односа.

Књига је пре свега намењена надареним ученицима средњих школа, који воле математику и припремају се за национална и међународна такмичења. Међутим, она садржи и основне појмове, тврђења и једноставније задатке, тако да могу да је користе и читаоци који се први пут срећу са теоријом бројева. Сматрамо да може бити од велике користи и професорима који припремају ученике како средњих, тако и основних школа за математичка такмичења. Велики број задатака је преузет са разних националних и међународних такмичења. Код задатака са националних такмичења наведена је земља (ако није реч о нашој), степен такмичења, разред и година када је такмичење одржано, а код међународних такмичења коришћене су уобичајене скраћенице: ЈБМО (Јуниорска балканска математичка олимпијада), БМО (Балканска математичка олимпијада), ММО (Медитеранска математичка олимпијада) и ИМО (Интернационална математичка олимпијада).

Имајући у виду да су бројеви главни извор настанка многих математичких (нарочито алгебарских) теорија верујемо да ова књига може бити корисна студентима у разним курсевима, на пример у заснивању математичке анализе, затим у рачунарству и дискретној математици, наравно у алгебри итд.

Захваљујемо се рецензентима, др Радосаву Ђорђевићу и др Дејану Бојовићу, који су пажљиво прочитали рукопис и дали низ корисних примедби и сугестија које су допринеле квалитету књиге. Такође, захвалност дугујемо члановима Математичке радионице младих и колегама др Браниславу Поповићу, мр Бојани Боровићанин, мр Ани Капларевић–Малишић и Слађани Димитријевић на помоћи.

Посебно се захваљујемо свим ученицима са којима смо последњих година радили и који су главна инспирација за писање ове књиге.

У Крагујевцу, *Аутори*
августа 2004.

1. Функција цео део

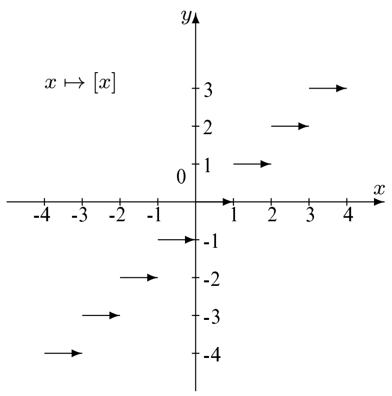
Дефиниција 1.1. *За реалан број x са $[x]$ означавамо* ***цео део*** *броја x, тј. највећи цео број који није већи од x.*

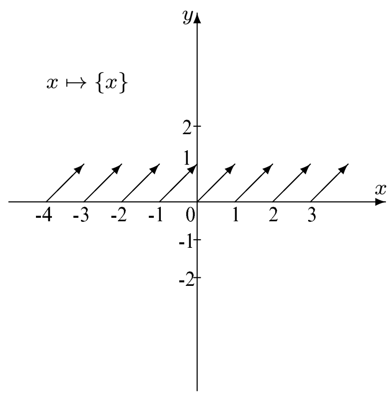
Пример 1.1. $[3] = 3$, $[4,5] = 4$, $\left[-\sqrt{3}\right] = -2$, $[\pi] = 3$.

Дефиниција 1.2. *За реални број x са $\{x\}$ означавамо* ***разломљени део*** *броја x, тј. узимамо да је $\{x\} = x - [x]$.*

Пример 1.2. $\{3\} = 3$, $\{2,178\} = 0,178$,
$\left\{-\sqrt{3}\right\} = -\sqrt{3} - \left[\sqrt{3}\right] = -\sqrt{3} - (-2) = 2 - \sqrt{3}$,
$\{-1,253\} = -1,253 - [-1,253] = -1,253 + 2 = 0,747$.

На следећим сликама дати су графици функција $x \mapsto [x]$ и $x \mapsto \{x\}$.





Теорема 1.1. *За произвољне реалне бројеве x и y важи:*

(1) $x - 1 < [x] \leqslant x < [x] + 1$;

(2) $0 \leqslant \{x\} < 1$*;*

(3) $[x+n] = [x] + n$*, за сваки цео број* n*;*

(4) $\left[\dfrac{[x]}{n}\right] = \left[\dfrac{x}{n}\right]$, *при чему је* $x > 0$ *и* n *произвољан природан број;*

(5) $[x] + [y] \leqslant [x+y] \leqslant [x] + [y] + 1$*;*

(6) $[nx] \geqslant n[x]$, *за сваки природан број* n*;*

(7) $[x-y] \leqslant [x] - [y]$*;*

(8) $[xy] \geqslant [x] \cdot [y]$, *ако је* $x > 0$ *и* $y > 0$*;*

(9) $\left[x + \dfrac{1}{2}\right] = [2x] - [x]$*;*

(10) $[2x+2y] \geqslant [x] + [y] + [x+y]$.

ДОКАЗ. (1) Доказ следи директно из дефиниције функције $x \mapsto [x]$.

(2) Из (1) следи

$$\{x\} = x - [x] \geqslant x - x = 0 \quad \text{и} \quad \{x\} = x - [x] < x - (x-1) = 1.$$

(3) Нека је $n \in \mathbb{N}$ и $x \in \mathbb{R}$. Из (1) имамо да је $[x] \leqslant x < [x] + 1$ па је

$$[x] + n \leqslant x + n < [x] + n + 1,$$

одакле је $[x+n] = [x] + n$.

(4) Нека је $n \in \mathbb{N}$ и $x \in \mathbb{R}$, $x \geqslant 0$. Ако је $\left[\dfrac{x}{n}\right] = k$, тада је $k \leqslant \dfrac{x}{n} < k+1$, тј. $kn \leqslant x < kn + n$, па и $kn \leqslant [x] < kn + n$. Ако последњу једнакост поделимо са n добијамо $k \leqslant \dfrac{[x]}{n} < k+1$, тј. $\left[\dfrac{[x]}{n}\right] = k$.

(5) Важи:

$$[x+y] = [[x]+\{x\}+[y]+\{y\}] \overset{(3)}{=} [x]+[y]+[\{x\}+\{y\}] \geqslant [x]+[y],$$

јер је $[\{x\}+\{y\}] \geqslant 0$. Како је $\{x\}+\{y\} < 2$, то је $[\{x\}+\{y\}] \leqslant 1$, па је

$$[x+y] = [x]+[y]+[\{x\}+\{y\}] \leqslant [x]+[y]+1.$$

(6) Нека је n произвољан природан број. Тада је

$$[nx] = [n[x]+n\{x\}] = n[x]+[n\{x\}] \geqslant n[x].$$

(7) Важи:

$$[x-y] = [[x]+\{x\}-[y]-\{y\}] = [x]-[y]+[\{x\}-\{y\}] \leqslant [x]-[y],$$

јер је $0 \leqslant \{x\}, \{y\} < 1$, па је

$$[\{x\}-\{y\}] = \begin{cases} 0, & \{x\} \geqslant \{y\} \\ -1, & \{x\} < \{y\} \end{cases}.$$

(8)

$$\begin{aligned} [xy] &= [([x]+\{x\})([y]+\{y\})] \\ &= [x]\cdot[y] + [[x]\cdot\{y\}+\{x\}\cdot[y]+\{x\}\cdot\{y\}] \\ &\geqslant\ [x]\cdot[y]. \end{aligned}$$

(9) Разликујемо два случаја:

1. Ако је $0 \leqslant \{x\} < \dfrac{1}{2}$, тада је

$$\left[x+\frac{1}{2}\right] = \left[[x]+\{x\}+\frac{1}{2}\right] = [x]$$

и

$$[2x] = [2([x]+\{x\})] = [2[x]+2\{x\}] = 2[x],$$

па је $\left[x+\dfrac{1}{2}\right]=[2x]-[x]$;

2. Ако је $\dfrac{1}{2}\leqslant\{x\}<1$, тада је $[x]=\left[[x]+\alpha+\dfrac{1}{2}\right]$, где је $\alpha=\{x\}-\dfrac{1}{2}$ и $0\leqslant\alpha<\dfrac{1}{2}$, па је

$$\left[x+\frac{1}{2}\right]=\left[[x]+\alpha+\frac{1}{2}+\frac{1}{2}\right]=[[x]+1+\alpha]=[x]+1$$

и

$$[2x]=\left[2\left([x]+\alpha+\frac{1}{2}\right)\right]=[2[x]+1+2\alpha]=2[x]+1,$$

одакле следи да је $\left[x+\dfrac{1}{2}\right]=[2x]-[x]$.

(10) Доказ препуштамо читаоцу. ■

1.1. Задаци

1. Нека су x,y,z произвољни реални бројеви. Доказати да је

$$x+[y+z]=y+[x+z]=z+[x+y]$$

ако и само ако је $\{x\}=\{y\}=\{z\}$.

Решење. Није тешко доказати да једнакости

$$x+[y+z]=y+[x+z]=z+[x+y]$$

важе ако и само ако је испуњено

$$(*)\qquad \{x\}+[\{y\}+\{z\}]=\{y\}+[\{x\}+\{z\}]=\{z\}+[\{x\}+\{y\}].$$

Очигледно, ако је $\{x\} = \{y\} = \{z\}$, важи и $(*)$. Поред тога, ако важи $(*)$, имамо да је, на пример,

$$\{x\} - \{y\} = [\{x\} + \{z\}] - [\{y\} - \{z\}] \in \mathbb{Z},$$

па пошто $\{x\}, \{y\} \in [0,1)$, биће $\{x\} = \{y\}$. Слично се доказује да је $\{y\} = \{z\}$, па је тиме доказано да је $\{x\} = \{y\} = \{z\}$.

2. Доказати да ако за неки реалан број x важи $\{8x\} = \{15x\}$, онда је и $\{26x\} = \{75x\}$.

Решење. Приметимо да за произвољне бројеве $a = [a] + \{a\}$ и $b = [b] + \{b\}$ важи: $\{a\} = \{b\}$ ако и само ако $a - b = [a] - [b]$ ако и само ако $a - b \in \mathbb{Z}$. Дакле, $\{8x\} = \{15x\}$ даје $7x \in \mathbb{Z}$, одакле имамо и $49x \in \mathbb{Z}$ и $\{26x\} = \{75x\}$.

3. Решити једначину $\{x\} + \{2x\} + \{3x\} = x$.

Решење. Нека је x решење дате једначине, $k = [x]$ и $\alpha = \{x\}$. Постоје следеће могућности:

1. Ако је $\alpha \in \left[0, \frac{1}{3}\right)$, тада је $6\alpha = k + \alpha$, тј. $5\alpha = k$, а како је $0 \leqslant \alpha < \frac{1}{3}$, биће $0 \leqslant k < \frac{5}{3}$, тј. $k = 0$ или $k = 1$, па је, у овом случају, $x = k + \alpha = 0$ или $x = k + \alpha = 1 + \frac{1}{5} = 1\frac{1}{5}$;

2. Ако је $\alpha \in \left[\frac{1}{3}, \frac{1}{2}\right)$, тада је $\alpha + 2\alpha + 3\alpha - 1 = k + \alpha$, тј. $5\alpha = k + 1$, а како је $\frac{1}{3} \leqslant \alpha < \frac{1}{2}$, биће $\frac{2}{3} \leqslant k < \frac{3}{2}$, тј. $k = 1$, па је $x = k + \alpha = 1 + \frac{2}{5} = 1\frac{2}{5}$;

3. Ако је $\alpha \in \left[\frac{1}{2}, \frac{2}{3}\right)$, тада је $\alpha + 2\alpha - 1 + 3\alpha - 1 = k + \alpha$, тј. $5\alpha = k + 2$, а како је $\frac{1}{2} \leqslant \alpha < \frac{2}{3}$, биће $\frac{1}{2} \leqslant k < \frac{4}{3}$, тј. $k = 1$, па је

$x = k + \alpha = 1 + \frac{3}{5} = 1\frac{3}{5}$;

4. Ако је $\alpha \in \left[\frac{2}{3}, 1\right)$, тада је $\alpha + 2\alpha - 1 + 3\alpha - 2 = k + \alpha$, тј. $5\alpha = k + 3$, а како је $\frac{2}{3} \leqslant \alpha < 1$, биће $\frac{1}{3} \leqslant k < 2$, тј. $k = 1$, па је $x = k + \alpha = 1 + \frac{4}{5} = 1\frac{4}{5}$.

Дакле, решења дате једначине су $0,\ 1\frac{1}{5},\ 1\frac{2}{5},\ 1\frac{3}{5},\ 1\frac{4}{5}$.

4. Решити једначину $\left[\frac{5+6x}{8}\right] = \frac{15x-7}{5}$.

Решење. Ако ставимо да је $\left[\frac{5+6x}{8}\right] = m,\ \ m \in \mathbb{Z}$, имамо да је $\frac{15x-7}{5} = m$, одакле је $x = \frac{5m+7}{15}$. Дата једначина се може записати у облику

$$\left[\frac{5 + 6\frac{5m+7}{15}}{8}\right] = m, \quad \text{тј.} \quad \left[\frac{m}{4} + \frac{39}{40}\right] = m.$$

Значи, $m \leqslant \frac{m}{4} + \frac{39}{40} < m + 1$. Решавањем последњих неједначина добијамо да $m \in \left(-\frac{1}{30}, \frac{13}{10}\right]$, одакле је $m = 0$ или $m = 1$, јер $m \in \mathbb{Z}$.

За $m = 0$ добија се $x = \frac{7}{15}$, а за $m = 1$, $x = \frac{4}{5}$. Лако се проверава да обе ове вредности представљају решење полазне једначине.

5. Решити систем једначина:

$$\begin{aligned} x + [y] + \{z\} &= 1,1 \\ y + [z] + \{x\} &= 2,2 \\ z + [x] + \{y\} &= 3,3. \end{aligned}$$

Решење. Сабирањем датих једначина добијамо да је

$$x + y + z = 3,3.$$

Како је $x + y + z = z + [x] + \{y\}$, имамо да је $x + y = [x] + \{y\} = [x] + y - [y]$, односно $x = [x] - [y]$, одакле следи да је x цео број. Значи $x = [x]$, па је $[y] = 0$, као и $\{x\} = 0$ и $y = \{y\}$. Сада, из прве једначине система је $x + \{z\} = 1,1$ одакле је $x = 1$ и $\{z\} = 0,1$. Из друге једначине система је $y + [z] = 2,2$ па је $y = 0,2$ и $[z] = 2$.

Дакле, $x = 1$, $y = 0,2$ и $z = 2,1$ је решење система.

6. Решити систем једначина:

$$\begin{aligned} &x - y = 2\,001 \\ &[x] + [y] = 2\,003. \end{aligned}$$

Решење. Нека је пар (x, y) решење датог система. Прву једначину датог система можемо записати и у облику

$$[x] + \{x\} - [y] - \{y\} = 2\,001,$$

одакле следи да $\{x\} - \{y\} \in \mathbb{Z}$, тј. $\{x\} = \{y\}$, због $0 \leqslant \{x\}, \{y\} < 1$, па је:

$$\begin{aligned} &[x] - [y] = 2\,001 \\ &[x] + [y] = 2\,003, \end{aligned}$$

тј. $[x] = 2\,002$ и $[y] = 1$. Дакле, дати систем једначина има бесконачно много решења.

Скуп решења је $\mathcal{R} = \{(2\,002 + \omega, 1 + \omega) \mid 0 \leqslant \omega < 1\}$.

7. Решити једначину $x^2 - 2[x] + \{x\} = 0$.

Решење. Ако претпоставимо да дата једначина има решења и да је x једно њено решење, пошто је $\{x\} \geqslant 0$ и $x^2 \geqslant 0$, имамо да је

$[x] \geqslant 0$. Нека је $[x] = k$ и $\{x\} = \alpha$. Тада је $(k+\alpha)^2 - 2k + \alpha = 0$, тј.

$$(*) \qquad \alpha^2 + (2k+1)\alpha + k^2 - 2k = 0.$$

Из последње једначине и чињенице да је $\alpha \geqslant 0$ добијамо да је

$$\alpha = \frac{-(2k+1) + \sqrt{(2k+1)^2 - 4(k^2-2k)}}{2},$$

тј.

$$\alpha = \frac{-(2k+1) + \sqrt{12k+1}}{2} \quad \text{и} \quad 12k+1 \geqslant (2k+1)^2.$$

У скупу целих бројева ($k \in \mathbb{Z}$) неједначина $12k+1 \geqslant (2k+1)^2$, тј. $4k(k-2) \leqslant 0$, има три решења: $k \in \{0, 1, 2\}$.

Ако је $k = 0$, једначина $(*)$ постаје $\alpha^2 + \alpha = 0$, па је, због $\alpha \in [0, 1)$, $\alpha = 0$. Дакле, $x = k + \alpha = 0$.

Ако је $k = 1$, једначина $(*)$ постаје $\alpha^2 + 3\alpha - 1 = 0$, па је, опет због $\alpha \in [0,1)$, $\alpha = \dfrac{-3+\sqrt{13}}{2}$. Дакле, $x = 1 + \dfrac{-3+\sqrt{13}}{2} = \dfrac{\sqrt{13}-1}{2}$.

Најзад, ако је $k = 2$, из $\alpha^2 + 5\alpha = 0$ и $\alpha \in [0, 1)$, добијамо да је $\alpha = 0$, па је $x = 2$.

Дакле, решења дате једначине су 0, $\dfrac{\sqrt{13}-1}{2}$, 2.

8. (Савезно такмичење 1987, I разред) Дат је природан број n. Одредити број решења једначине

$$x^2 - [x^2] = (x - [x])^2,$$

за које је $1 \leqslant x \leqslant n$.

Решење. Ако ставимо да је $x = m + \alpha$, $m \in \{1, 2, \ldots, n-1\}$, $0 \leqslant \alpha < 1$, дата једначина постаје

$$m^2 + 2m\alpha = \left[m^2 + 2m\alpha + \alpha^2\right].$$

Дакле, број $m+\alpha$, је решење дате једначине ако и само ако је $2m\alpha$ цео број, тј. ако и само ако је

$$\alpha \in \left\{0, \frac{1}{2m}, \frac{2}{2m}, \dots, \frac{2m-1}{2m}\right\},$$

па у интервалу $[m, m+1)$ дата једначина има $2m$ решења. Како $x=n$ јесте решење, то је тражени број једнак

$$1+2\,(1+2+\cdots+(n-1)) = 1+(n-1)n = n^2-n+1.$$

9. (XX Московска олимпијада) Решити једначину $x^3-[x]=4$.

Решење. Из $x^3-4=[x]\leqslant x$ следи да је $x^3-x\leqslant 4$, одакле је $x<2$, јер за $x\geqslant 2$ имамо да је $x(x^2-1)\geqslant 2\cdot 3>4$. Такође, из $x^3-4=[x]\geqslant x-1$, тј. $x^3-x>3$ закључујемо да је $x\geqslant -1$, јер за $x<-1$ имамо да је $x^3-x=x(x^2-1)<0$.

Дакле, $x\in[-1,2)$, па је $[x]\in\{-1,0,1\}$.

За $[x]=-1$ дата једначина се своди на $x^3+1=4$, одакле је $x=\sqrt[3]{3}$, што је немогуће јер је $\left[\sqrt[3]{3}\right]=1\neq -1$.

За $[x]=0$ добијамо $x^3=4$, тј. $x=\sqrt[3]{4}$, што је такође немогуће због $\left[\sqrt[3]{4}\right]=1\neq 0$.

За $[x]=1$ добијамо једино решење дате једначине $x=\sqrt[3]{5}$.

10. (Савезно такмичење 1989, I разред) Одредити све природне бројеве n за које важи једнакост

$$[\sqrt[3]{1}]+[\sqrt[3]{2}]+\cdots+[\sqrt[3]{n}]=2n.$$

Решење. Нека је $a_m=[\sqrt[3]{m}]-2$, $m\in\mathbb{N}$. Треба одредити све природне бројеве n за које важи

$$a_1+a_2+\cdots+a_n=0.$$

Како је

$$\begin{array}{lll} a_m = -1 & \text{за} & 1 \leqslant m \leqslant 7 \\ a_m = 0 & \text{за} & 8 \leqslant m \leqslant 26 \\ a_m = 1 & \text{за} & 27 \leqslant m \leqslant 63 \\ a_m \geqslant 2 & \text{за} & m \geqslant 64 \end{array}$$

збир $a_1+a_2+\cdots+a_n$ једнак је нули ако и само ако је $n = 26+7 = 33$.

11. (Пролећно математичко такмичење, Бугарска 2002, 8. разред) Наћи све природне бројеве n за које је $n - [n\{\sqrt{n}\}] = 2$.

Решење. Ако је $n = p^2$ тада је $\sqrt{n} = p$ и $\{\sqrt{n}\} = 0$, па је $n = 2$. Контрадикција са $n = p^2$. Дакле, постоји природан број t такав да је $(t-1)^2 < n < t^2$. Тада је $[\sqrt{n}] = t - 1$, па важи (коришћењем чињенице да ако је a цео број важи $[a+b] = a + [b]$):

$$\begin{aligned} n - \left[n\left\{\sqrt{n}\right\}\right] &= n - \left[n\left(\sqrt{n} - \left[\sqrt{n}\right]\right)\right] = n - \left[n\left(\sqrt{n} - t + 1\right)\right] \\ &= n - \left[n\sqrt{n}\right] + nt - n = nt - \left[n\sqrt{n}\right]. \end{aligned}$$

Према томе, $nt = 2 + [n\sqrt{n}]$.

Нека је $n = t^2 - k$ и претпоставимо да је $k \geqslant 2$. Тада је

$$n\sqrt{n+2} \leqslant nt$$

и пошто је

$$2 + \left[n\sqrt{n}\right] \leqslant 2 + n\sqrt{n},$$

добијамо да је $n\sqrt{n+2} \leqslant 2 + n\sqrt{n}$. Записујући ову неједнакост у облику $n\left(\sqrt{n+2} - \sqrt{n}\right) \leqslant 2$ и множећи је са $\sqrt{n+2} + \sqrt{n}$ добијамо

$$(*) \qquad n \leqslant \sqrt{n+2} + \sqrt{n}.$$

Пошто је $\sqrt{n(n+2)} < n + 1$, после квадрирања неједнакости $(*)$ добијамо $n^2 < 3(n+1)$. Ова неједнакост је тачна само за $n = 1, 2$ или 3 и непосредном провером можемо видети да ниједна од ових вредности није решење.

Према томе, $k = 1$ и после сличних трансформација добијамо $n \leqslant 2\left(\sqrt{n+1}+\sqrt{n}\right)$. Из

$$2\left(\sqrt{n+1}+\sqrt{n}\right) < 4\sqrt{n+1}$$

следи $n < 4\sqrt{n+1}$. Пошто је $n = t^2 - 1$ добијамо $t^2 - 1 < 4t$, што је тачно само за $t \leqslant 4$. Према томе, све могуће вредности за n су $n = 3, n = 8$ и $n = 15$. Провером утврђујемо да само $n = 8$ и $n = 15$ задовољавају услове задатка.

12. (Национална математичка олимпијада–прва рунда, Румунија 2003, 9. разред) Наћи цео део броја

$$a_n = \sqrt[3]{24 + \sqrt[3]{24 + \cdots + \sqrt[3]{24}}} \qquad (n \text{ корена}),$$

где је $n \geqslant 1$.

Решење. Очигледно је

$$a_{n+1} = \sqrt[3]{24 + a_n} \quad \text{и} \quad 2 \leqslant \sqrt[3]{24} = a_1 < 3.$$

Претпоставимо да је за неко $n \in \mathbb{N}$ испуњено $2 \leqslant a_n < 3$. Тада је

$$a_{n+1} = \sqrt[3]{24 + a_n} < \sqrt[3]{24 + 3} = 3 \quad \text{и} \quad a_{n+1} > \sqrt[3]{24} > 2.$$

Дакле, важи $2 \leqslant a_n < 3$, за све $n \geqslant 1$, па је $[a_n] = 2$ за све $n \geqslant 1$.

13. (Национална математичка олимпијада–прва рунда, Румунија 2003, 10. разред) Нека су n и p позитивни цели бројеви за које важи $p > 2^n$. Доказати да је цео део броја $\displaystyle\sum_{k=0}^{n} \sqrt[p]{1 + \binom{n}{k}}$ једнак $n + 1$.

Решење. Треба показати да је

$$n + 1 \leqslant \sum_{k=0}^{n} \sqrt[p]{1 + \binom{n}{k}} < n + 2.$$

Лева неједнакост је очигледна јер је $\sqrt[p]{1+\binom{n}{k}} > 1$. За десну неједнакост искористићемо Бернулијеву неједнакост:

$$\left(1+\frac{1}{p}\binom{n}{k}\right)^p \geqslant 1+p\cdot\frac{1}{p}\binom{n}{k} = 1+\binom{n}{k},$$

одакле је

$$1+\frac{1}{p}\binom{n}{k} \geqslant \sqrt[p]{1+\binom{n}{k}} \quad \text{за све } \ k=0,1,\ldots,n.$$

Сабирањем претходних неједнакости добијамо

$$\sum_{k=0}^{n}\sqrt[p]{1+\binom{n}{k}} \leqslant n+1+\frac{1}{p}\sum_{k=0}^{n}\binom{n}{k} = n+1+\frac{2^n}{p} < n+2.$$

14. (Хермит) Ако је x реалан број а n природан број, онда важи:

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx].$$

Решење. Пошто је

$$\begin{aligned}&[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]\\ =\ & n[x]+[\{x\}]+\left[\{x\}+\frac{1}{n}\right]+\left[\{x\}+\frac{2}{n}\right]+\cdots+\left[\{x\}+\frac{n-1}{n}\right]\end{aligned}$$

и $[nx]=n[x]+[n\{x\}]$, довољно је доказати да дата једнакост важи за све реалне бројеве x из $[0,1)$.

Нека $x \in [0,1)$ и нека је k број из $\{0,1,\ldots,n-1\}$ такав да је $\frac{k}{n} \leqslant x < \frac{k+1}{n}$. Тада је

$$[x] = \left[x+\frac{1}{n}\right] = \left[x+\frac{2}{n}\right] = \cdots = \left[x+\frac{n-k-1}{n}\right] = 0,$$

јер је $x + \frac{n-k-1}{n} < \frac{k+1}{n} + \frac{n-k-1}{n} = 1$. Такође је

$$\left[x+\frac{n-k}{n}\right] = \left[x+\frac{n-k+1}{n}\right] = \cdots = \left[x+\frac{n-1}{n}\right] = 1,$$

јер је $x + \frac{n-k}{n} \geqslant \frac{k}{n} + \frac{n-k}{n} = 1$ и $x + \frac{n-1}{n} < \frac{k+1}{n} + \frac{n-1}{n} \leqslant \frac{n}{n} + \frac{n-1}{n} < 2$. Значи

$$\begin{aligned}
&[x] + \left[x+\frac{1}{n}\right] + \left[x+\frac{2}{n}\right] + \cdots + \left[x+\frac{n-k-1}{n}\right] \\
&+ \left[x+\frac{n-k}{n}\right] + \left[x+\frac{n-k+1}{n}\right] + \cdots + \left[x+\frac{n-1}{n}\right] \\
&= \underbrace{0+\cdots+0}_{n-k \text{ пута}} + \underbrace{1+\cdots+1}_{k \text{ пута}} = k.
\end{aligned}$$

Из $\frac{k}{n} \leqslant x < \frac{k+1}{n}$ следи да је $k \leqslant nx < k+1$, тј. да је $[nx] = k$, чиме је тврђење доказано.

15. (Словеначка математичка олимпијада 1999, IV разред) Нека је m природан број и $r_1, r_2, \ldots, r_m$ позитивни рационални бројеви такви да је $r_1+r_2+\cdots+r_m = 1$. Дефинисана је функција $f : \mathbb{N} \to \mathbb{Z}$

$$f(n) = n - [r_1 n] - [r_2 n] - \cdots - [r_m n].$$

Наћи минимум и максимум функције f.

Решење. За сваки r_i, $i = 1, 2, \ldots, m$, и сваки природан број n важи неједнакост $0 \leqslant r_i n - [r_i n] < 1$.

Нека је s најмањи заједнички садржалац именилаца рационалних бројева r_i, $i = 1, 2, \ldots, m$. Тада је

$$f(n) = \sum_{i=1}^{m} (r_i n - [r_i n]) \geqslant 0, \quad \text{за сваки природан број } n,$$

и $f(s) = 0$, па је 0 минимум функције f. Даље, због

$$f(n) = \sum_{i=1}^{m} (r_i n - [r_i n]) < m, \quad \text{за сваки природан број } n,$$

и

$$\begin{aligned} f(s-1) &= s - 1 - \sum_{i=1}^{m} [r_i s - r_i] \\ &= s - 1 - \sum_{i=1}^{m} (r_i s - 1) \\ &= s - 1 - s + m = m - 1 \end{aligned}$$

максимум функције f је $m - 1$.

16. (Савезно такмичење 1985, II разред) Нека је функција $f : \mathbb{N} \to \mathbb{N}$ задата формулом $f(m) = m + [\sqrt{m}]$. Доказати да за свако $m \in \mathbb{N}$ постоји $k \in \mathbb{N}$, тако да је $f^k(m) = f(f \ldots (f(m)) \ldots)$ потпун квадрат.

Решење. Приметимо да за сваки природан број m постоји природан број n такав да важи

$$n^2 \leqslant m \leqslant n^2 + 2n = (n+1)^2 - 1.$$

Ако је $m = n^2$, онда је:

$$\begin{aligned}
&f(m) = f(n^2) = n^2 + n,\\
&f^2(n^2) = n^2 + 2n,\\
&f^3(n^2) = n^2 + 3n = (n+1)^2 + n - 1,\\
&f^5(n^2) = (n+1)^2 + n - 1 + 2(n+1) = (n+2)^2 + n - 2,\\
&f^7(n^2) = (n+2)^2 + n - 2 + 2(n+2) = (n+2)^2 + n - 3,\\
&\quad\vdots\\
&f^{2n-1}(n^2) = (n + n - 1)^2 + 1,\\
&f^{2n+1}(n^2) = (2n-1)^2 + 1 + 2(2n-1) = (2n)^2.
\end{aligned}$$

Слично се за $m = n^2 + \alpha n + \beta,\ \alpha \in \{0, 1\},\ \beta \in \{1, 2, \ldots, n\}$ добија

$$f^{2\beta-\alpha}(m) = f^{2\beta-\alpha}(n^2 + \alpha n + \beta) = (m + \beta)^2.$$

2. Дељивост целих бројева

Дефиниција 2.1. *Цео број a* ***дељив је*** *целим бројем b, различитим од нуле, ако и само ако постоји цео број q такав да је $a = bq$. Ако је број a дељив бројем b, пишемо $b \mid a$ (b дели a). Кажемо да је број b* ***делилац*** *броја a, односно да је број a* ***садржалац*** *броја b.*

Ако број a није дељив бројем b писаћемо $b \nmid a$ (b не дели a).

Очигледно је из претходне дефиниције да за сваки цео број a важи $a \mid a$. Ако важи $a \mid b$ и $a \neq b$, тада кажемо да је a ***прави делилац*** од b.

Теорема 2.1.
1. $b \mid a \Rightarrow b \mid ac$ *за свако* $c \in \mathbb{Z}$.
2. $a \mid b \wedge b \mid c \Rightarrow a \mid c$.
3. $a \mid b \wedge a \mid c \Rightarrow a \mid bx + cy$ *за све* $x, y \in \mathbb{Z}$.
4. $a \mid b \wedge b \mid a \Rightarrow a = b \vee a = -b$.
5. *Ако за позитивне бројеве a, b важи $a \mid b$, онда је $a \leqslant b$.*

Доказ. 1. Како $b \mid a$ тада постоји цео број m такав да је $a = mb$. Тада за све $c \in \mathbb{Z}$ важи $ac = (mc)b = nb$, где је $n = mc \in \mathbb{Z}$, одакле следи да $b \mid ac$.

2. Ако $a \mid b$ и $b \mid c$ тада постоје цели бројеви m и n такви да је $b = ma$ и $c = nb$, па је $c = nma$, а како је $nm \in \mathbb{Z}$ следи да $a \mid c$.

3. Ако $a \mid b$ и $a \mid c$ тада постоје цели бројеви m и n такви да је $b = ma$ и $c = na$. Тада је за произвољне целе бројеве x и y

$$bx + cy = max + nay = a(mx + ny),$$

па како је $mx + ny \in \mathbb{Z}$ то важи $a \mid bx + cy$.

4. Ако је $b = 0$, тада је и $a = 0$, па је $a = b$. Нека је $b \neq 0$. Тада из $a \mid b$ и $b \mid a$ следи да постоје цели бројеви m и n такви да је $b = ma$ и $a = nb$, одакле је $a = nma$, па је $nm = 1$. Како су n и m цели бројеви то је или $n = m = 1$ или $n = m = -1$, односно $a = b$ или $a = -b$.

5. Из $a \mid b$ следи да постоји $q \in \mathbb{Z}$ такав да је $b = aq$, а како је $b > 0$ и $a > 0$, то је и $q > 0$, односно, због $q \in \mathbb{Z}$, $q \geqslant 1$, па важи $b = aq \geqslant a \cdot 1 = a$. ∎

ТЕОРЕМА 2.2. *Ако се у једнакости $a_1 + a_2 + \cdots + a_k = 0$ за све сабирке сем једног зна да су дељиви целим бројем b, онда је и тај сабирак дељив са b.*

ДОКАЗ. Нека је a_i сабирак за који се не зна да ли је дељив са b. Тада је

$$a_1 = bq_1,\ a_2 = bq_2,\ \ldots,\ a_{i-1} = bq_{i-1},\ a_{i+1} = bq_{i+1},\ \ldots,\ a_k = bq_k,$$

за неке целе бројеве $q_1, q_2, \ldots, q_{i-1}, q_{i+1}, \ldots, q_k$. Тада из дате једнакости добијамо

$$a_i = -b(q_1 + q_2 + \cdots + q_{i-1} + q_{i+1} + \cdots + q_k) = bq_i,$$

где је $q_i = -(q_1 + q_2 + \cdots + q_{i-1} + q_{i+1} + \cdots + q_k) \in \mathbb{Z}$, тј. $b \mid a$. ∎

ТЕОРЕМА 2.3. (***Теорема о остатку***) *Нека је $a \in \mathbb{Z}$ и $b \in \mathbb{N}$. Тада постоје јединствени бројеви $q, r \in \mathbb{Z}$ такви да је*

$$a = bq + r, \qquad 0 \leqslant r < b.$$

*Број q назива се **количник**, а број r **остатак** при дељењу броја a бројем b.*

ДОКАЗ. Посматрајмо све бројеве облика $a - kb$, где је $k \in \mathbb{Z}$. Изаберимо међу тим бројевима најмањи број који припада скупу $\mathbb{N} \cup \{0\}$

(такав број сигурно постоји јер је скуп природних бројева добро уређен). Нека је тај изабрани број $a - qb$. Обележићемо га са r. Тада је

$$(1) \qquad a = bq + r, \qquad 0 \leqslant r < b,$$

јер би у случају $r \geqslant b$ и број $a - (q+1)b < a - qb$ био из скупа $\mathbb{N} \cup \{0\}$, што је у контрадикцији са избором броја $a - bq$. Према томе, доказали смо егзистенцију бројева q и r. Остаје још да докажемо и њихову јединственост. Претпоставимо да постоје и бројеви q_1 и r_1 такви да је

$$(2) \qquad a = bq_1 + r_1, \qquad 0 \leqslant r_1 < b.$$

Тада из (1) и (2) следи

$$0 = b(q - q_1) + (r - r_1),$$

одакле следи да $b \mid r - r_1$. Како је $|r - r_1| < b$, то је $r - r_1 = 0$, тј. $r = r_1$, па је и $q = q_1$. ■

Претходном теоремом је омогућено представљање бројева у позиционој нотацији у датој бројевној бази. Ако је $b > 1$ дати природан број, тада за сваки природан број a постоје јединствени природни бројеви $n, a_0, a_1, \ldots, a_n$ такви да је:

$$(*) \qquad \begin{cases} a = a_n b^n + \cdots + a_1 b + a_0 \\ 0 \leqslant a_0, a_1, \ldots, a_{n-1} < b,\ 1 \leqslant a_n < b \end{cases}$$

Нека су природни бројеви $0, 1, \ldots, b-1$ означени посебним знацима, које називамо цифрама у бројевној бази b. Ако су $c_0, c_1, \ldots, c_n$ цифре које одговарају бројевима $a_0, a_1, \ldots, a_n$ у представљању $(*)$, тада пишемо

$$a = (c_n \ldots c_1 c_0)_b.$$

У декадном систему, који користимо за записивање природних бројева, цифре су $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$ и пишемо $a = c_n \dots c_1 c_0$, уместо $a = (c_n \dots c_1 c_0)_{10}$.

Пример 2.1. *База бинарног система је број* 2*, док су цифре* 0 *и* 1*. На пример, ако је* $a = 1101101_2$*, онда је* $a = 2^6 + 2^5 + 2^3 + 2^2 + 2^0 = 109$.

Пример 2.2. *Хексадецимални систем за базу има* $b = 16$*, а цифре овог система су* $0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F$*. Дакле, овде симболи* A, B, C, D, E, F *стоје редом за* $10, 11, 12, 13, 14, 15$*. На пример,* $E07A_{16} = 14 \cdot 16^3 + 7 \cdot 16^1 + 10 \cdot 16^0 = 57466$.

Пример 2.3. *Представимо број* $a = 973$ *у бројевном систему са базом* $b = 7$*. Како је*

$$\begin{aligned} 973 &= 139 \cdot 7 + \underline{0} \\ 139 &= 19 \cdot 7 + \underline{6} \\ 19 &= 2 \cdot 7 + \underline{5} \\ 2 &= 0 \cdot 7 + \underline{2} \end{aligned}$$

имамо да је $a = 2560_7$.

Напомена. Ако су b и B бројевне базе такве да је $B = b^k$ за неки природан број k, тада постоји „брз“ алгоритам за прелаз из бројевног система са базом b у базу B, односно из базе B у базу b, који је специјално важан за прелаз из бинарне базе у хексадецималну, и обрнуто. Читаоцу препуштамо да самостално дође до алгоритма, на основу наредног примера.

Пример 2.4. *За* $b = 2$*,* $B = 2^4 = 16$ *и* $a = A70F_{16}$ *имамо*

$$a = \underbrace{1010}_{A}\,\underbrace{0111}_{7}\,\underbrace{0000}_{0}\,\underbrace{1111}_{F} = 1010011100001111_2.$$

Ако је $a = 10101010001100_2$*, онда је*

$$a = 0010\,1010\,1000\,1100 = 2A8C_{16}.$$

ДЕФИНИЦИЈА 2.2. *Цео број d је* ***заједнички делилац бројева*** *a и b ако $d \mid a$ и $d \mid b$.*

ДЕФИНИЦИЈА 2.3. *Највећи међу заједничким делиоцима бројева a и b је* ***највећи заједнички делилац*** *бројева a и b. Обележава се са (a, b) или* НЗД (a, b).

Пошто сваки цео број различит од 0 има коначно много делилаца, то је скуп заједничких делилаца два цела броја коначан и у њему постоји највећи број. Према томе, највећи заједнички делилац два цела броја увек постоји. Ми ћемо за највећи заједнички делилац бројева a и b у овој књизи користити ознаку (a, b), осим у случајевима када би та ознака довела до забуне (јер се иста ознака користи и за уређени пар), када ћемо користити ознаку НЗД (a, b).

ДЕФИНИЦИЈА 2.4. *За бројеве a и b кажемо да су* ***узајамно (релативно) прости*** *ако је $(a, b) = 1$.*

ТЕОРЕМА 2.4. *Највећи заједнички делилац два цела броја, од којих је бар један различит од 0, је јединствен.*

ДОКАЗ. Нека је $d = (a, b)$ и $d_1 = (a, b)$. Тада важи $d \mid d_1$ и $d_1 \mid d$, одакле следи да је $d = d_1$. ■

На основу дефиниција 2.2. и 2.3. следи да ако је d заједнички делилац бројева a и b, онда $d \mid (a, b)$.

ТЕОРЕМА 2.5. *Ако је $a = bq$ и $b \geqslant 0$, онда је $(a, b) = b$.*

ДОКАЗ. Како $b \mid a$ и $b \mid b$, то је b заједнички делилац бројева a и b. Ниједан цео број $c > b$ не може бити делилац броја b, (због $b \geqslant 0$), па је $(a, b) = b$. ■

ТЕОРЕМА 2.6. *Ако је* $d = (a, b)$ *онда постоје бројеви* $\alpha, \beta \in \mathbb{Z}$ *такви да је* $\alpha a + \beta b = d$. *Највећи заједнички делилац бројева* a *и* b *је најмањи позитиван број облика* $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$.

ДОКАЗ. У скупу целих бројева облика $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$ изаберимо најмањи позитиван број. Нека је то број $c = \alpha a + \beta b$. Доказаћемо да је c заједнички делилац бројева a и b. Ако $c \nmid a$ онда постоје цели бројеви q и r, $0 < r < c$, такви да је $a = cq + r$. Тада је

$$r = a - cq = a - q(\alpha a + \beta b) = (1 - \alpha q)a - \beta qb.$$

Из претходне једнакости следи да је r позитиван број мањи од c, а припада скупу бројева облика $\alpha a + \beta b$, што је контрадикција са претпоставком да је c најмањи такав број. Дакле, $c \mid a$. Аналогно се доказује да $c \mid b$.

Треба доказати још да је $d = c$. Како $d \mid a$ и $d \mid b$, то је $a = md$ и $b = nd$, за неке целе бројеве m и n. Тада је $c = \alpha md + \beta nd = d(\alpha m + \beta n)$, па $d \mid c$, а то значи да је $d \leqslant c$. Како је d највећи заједнички делилац бројева a и b, а c заједнички делилац бројева a и b то мора бити $d \geqslant c$, па је $d = c$, односно $d = \alpha a + \beta b$.■

ТЕОРЕМА 2.7. *Ако је* $k > 0$, *онда је* $(ka, kb) = k(a, b)$.

ДОКАЗ. Према претходној теореми највећи заједнички делилац бројева a и b је најмањи позитиван број облика $\alpha a + \beta b$, $\alpha, \beta \in \mathbb{Z}$, а највећи заједнички делилац бројева ka и kb је најмањи позитиван број облика $\alpha ka + \beta kb$, $\alpha, \beta \in \mathbb{Z}$, одакле због услова $k > 0$ директно следи тврђење. ■

ТЕОРЕМА 2.8. *Ако* $c \mid ab$ *и ако је* $(c, a) = 1$, *тада* $c \mid b$.

ДОКАЗ. Из претпоставке $(c, a) = 1$ следи да постоје $\alpha, \gamma \in \mathbb{Z}$ такви да је $\alpha a + \gamma c = 1$, па је и $\alpha ab + \gamma cb = b$. Из претпоставке $c \mid ab$ и чињенице да $c \mid cb$, следи да $c \mid b$. ■

У претходној теореми претпоставка да су a и c узајамно прости је веома битна, јер без тог услова не следи да $c \mid b$. На пример, $10 \mid 5 \cdot 8$, али $10 \nmid 5$ и $10 \nmid 8$.

Како дељивост целих бројева не зависи од знака, можемо се ограничити на дељивост природних бројева. Сада ћемо дати један алгоритам за одређивање највећег заједничког делиоца два природна броја, који се заснива на теореми о остатку.

Еуклидов алгоритам. На основу теореме 2.3. можемо исписати следећи низ једнакости:

$$\begin{aligned}
a &= bq_1 + r_1, && 0 \leqslant r_1 < b,\\
b &= r_1q_2 + r_2, && 0 \leqslant r_2 < r_1,\\
r_1 &= r_2q_3 + r_3, && 0 \leqslant r_3 < r_2,\\
&\vdots && \vdots\\
r_{n-2} &= r_{n-1}q_n + r_n, && 0 \leqslant r_n < r_{n-1},\\
r_{n-1} &= r_nq_{n+1}.
\end{aligned}$$

Како бројеви r_n чине строго опадајући низ природних бројева мањих од b, то ћемо након коначног броја корака доћи до $r_{n+1} = 0$, тј. до једнакости $r_{n-1} = r_nq_{n+1}$, која говори о дељивости два узастопна остатка.

ТЕОРЕМА 2.9. 1. *Ако је $a = bq + r$, онда је $(a, b) = (b, r)$.*
2. *Последњи остатак r_n који је различит од нуле у Еуклидовом алгоритму представља највећи заједнички делилац бројева a и b.*

ДОКАЗ. 1. Нека је d заједнички делилац бројева a и b. Тада из $a = bq + r$ следи да $d \mid r$, односно да је d заједнички делилац бројева b и r. Ако је c заједнички делилац бројева b и r, тада, опет из једнакости $a = bq + r$, следи да $c \mid a$, па је c заједнички делилац бројева a и b. Према томе, скуп заједничких делилаца бројева a и b поклапа се са

скупом заједничких делилаца бројева b и r, па су међусобно једнаки и њихови највећи елементи, тј. $(a,b)=(b,r)$.
2. На основу 1. важе следеће једнакости:

$$(a,b)=(b,r_1)=(r_1,r_2)=\cdots=(r_{n-2},r_{n-1})=(r_{n-1},r_n).$$

Пошто $r_n \mid r_{n-1}$ то је $(r_{n-1},r_n)=r_n$, па је $(a,b)=r_n$. ■

ПРИМЕР 2.5. *Одредимо* $(942,444)$. *Применом Еуклидовог алгоритма добијамо*

$$\begin{aligned} 942 &= 2\cdot 444+54\\ 444 &= 8\cdot 54+12\\ 54 &= 4\cdot 12+6\\ 12 &= 2\cdot 6 \end{aligned}$$

одакле следи да је $(942,444)=6$.

Теорема 2.6. тврди да за свака два цела броја a и b постоје цели бројеви α и β такви да је $\alpha a+\beta b=(a,b)$. Знајући Еуклидов алгоритам није тешко наћи поступак како за задате a и b ефективно одредити α и β. Тај поступак нећемо детаљно описивати, већ ћемо га илустровати на следећем примеру.

ПРИМЕР 2.6. *Одредимо целе бројеве α и β такве да је*

$$\alpha\cdot 942+\beta\cdot 444=(942,444).$$

На основу примера 2.5. *имамо да је* $(942,444)=6$*, као и*

$$\begin{aligned} 54 &= 942+(-2)\cdot 444\\ 12 &= 444+(-8)\cdot(942+(-2)\cdot 444)=(-8)\cdot 942+17\cdot 444\\ 6 &= 54+(-4)\cdot 12=33\cdot 942+(-70)\cdot 444. \end{aligned}$$

ДЕФИНИЦИЈА 2.5. *Највећим заједничким делиоцем* n *целих бројева* $a_1, a_2, \ldots, a_n$ *зовемо највећи од заједничких делилаца ових бројева и обележавамо га са* $(a_1, a_2, \ldots, a_n)$ *или* НЗД$(a_1, a_2, \ldots, a_n)$. *Ако је* $(a_1, a_2, \ldots, a_n) = 1$, *бројеви* $a_1, a_2, \ldots, a_n$ *су* ***узајамно (релативно) прости***. *Бројеви* $a_1, a_2, \ldots, a_n$ *су* ***узајамно (релативно) прости у паровима*** *ако је* $(a_i, a_j) = 1$ *за* $i = 1, 2, \ldots, n,\ j = 1, 2, \ldots, n,\ i \neq j$.

Слично као и код највећег заједничког делиоца два броја, за највећи заједнички делилац бројева $a_1, a_2, \ldots, a_n$ користићемо ознаку $(a_1, a_2, \ldots, a_n)$, осим у случајевима када та ознака може довести до забуне и тада ћемо писати НЗД $(a_1, a_2, \ldots, a_n)$.

Приметимо да бројеви $a_1, a_2, \ldots, a_n$, $(n > 2)$ могу бити узајамно прости, а да притом не морају бити узајамно прости по паровима.

ПРИМЕР 2.7. $(55, 100, 205) = 5$; $(3, 7, 12) = 1$, *тј. бројеви* $3, 7$ *и* 12 *су узајамно прости, међутим, они нису узајамно прости у паровима јер је* $(3, 12) = 3$.

Највећи заједнички делилац бројева $a_1, a_2, \ldots, a_n$ може се добити вишеструком применом Еуклидовог алгоритма, о чему говори следећа теорема.

ТЕОРЕМА 2.10. *За природне бројеве* $a_1, a_2, \ldots, a_n$ $(n \geqslant 3)$ *важи*

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

ДОКАЗ. Нека је

$$d = (a_1, a_2, \ldots, a_n) \quad \text{и} \quad d' = ((a_1, a_2, \ldots, a_{n-1}), a_n).$$

Како $d \mid a_i$ за $i = 1, 2, \ldots, n$, то $d \mid (a_1, a_2, \ldots, a_{n-1})$ и $d \mid a_n$, па према томе $d \mid d'$. Слично, због $d' \mid (a_1, a_2, \ldots, a_{n-1})$ и $d' \mid a_n$, важи $d' \mid a_i$ за $i = 1, 2, \ldots, n$, па $d' \mid d$. Према томе, $d = d'$. ■

ДЕФИНИЦИЈА 2.6. *Заједничким садржаоцем* n *целих бројева* $a_1, a_2, \ldots, a_n$*, различитих од нуле, називамо сваки број који је дељив сваким од бројева* $a_1, a_2, \ldots, a_n$*. Најмањи међу позитивним заједничким садржаоцима бројева* $a_1, a_2, \ldots, a_n$ *зове се* ***најмањи заједнички садржалац*** *тих бројева и обележава се са* $[a_1, a_2, \ldots, a_n]$ *или са* НЗС $(a_1, a_2, \ldots, a_n)$.

На основу дефиниције 2.6. следи да ако је $s = [a_1, a_2, \ldots, a_n]$ и S ма који заједнички садржалац бројева $a_1, a_2, \ldots, a_n$, онда $s \mid S$.

У овој књизи ћемо за најмањи заједнички садржалац бројева $a_1, a_2, \ldots, a_n$ увек користити ознаку $[a_1, a_2, \ldots, a_n]$.

ТЕОРЕМА 2.11. $(a, b) \cdot [a, b] = |\,ab|$.

ДОКАЗ. Доказаћемо тврђење за природне бројеве (лако се прелази на целе бројеве).

Нека је S заједнички садржалац бројева a и b. Тада је $S = ak$, за неки природан број k. Како $b \mid S$, то је $\dfrac{ak}{b} \in \mathbb{N}$. Нека је $d = (a, b)$. Тада постоје узајамно прости природни бројеви m и n такви да је $a = md$ и $b = nd$, па је

$$\frac{ak}{b} = \frac{mdk}{nd} = \frac{mk}{n} \in \mathbb{N}.$$

Како $n \mid mk$ и $(n, m) = 1$, то $n \mid k$, односно постоји природан број t, такав да је $k = nt = \dfrac{b}{d}t$. Дакле, $S = \dfrac{ab}{d}t$.

С друге стране, сваки број облика $\dfrac{ab}{d}t$ је садржалац бројева a и b. Према томе, S је заједнички садржалац бројева a и b ако и само ако је $S = \dfrac{ab}{d}t,\ t \in \mathbb{N}$. Најмањи такав број добија се за $t = 1$. Дакле, ако је $s = [a, b]$, тада је $s = \dfrac{ab}{d}$. ∎

2.1. Задаци

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

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

18. Доказати да:

(1) су сви бројеви облика $1\,007, 10\,017, 100\,117, 1\,001\,117, \dots$ (између цифара 0 и 7 умеће се произвољно много пута цифра 1) дељиви са 53;

(2) за свако $n \in \mathbb{N}$, $133 \mid 11^{n+2} + 12^{2n+1}$;

(3) за свако $n \in \mathbb{N}$, $3^n \mid \underbrace{aa...a}_{3^n}$ за ма коју цифру a.

Решење. (1) Једноставно, дељењем, можемо се уверити да су дати бројеви сложени: $1\,007 : 53 = 19$, $10\,017 : 53 = 189, \dots,$

$$\begin{array}{l}
\;\;10011\dots17 : 53 = 188\dots89 \\
\underline{-53} \\
\;\;\;\;471 \\
\;\;\underline{-424} \\
\;\;\;\;\;\;471 \\
\;\;\;\;\;\;\;\;\;\;\vdots \\
\;\;\;\;\;\;\;\;\;\;471 \\
\;\;\;\;\;\;\;\;\underline{-424} \\
\;\;\;\;\;\;\;\;\;\;\;\;477 \\
\;\;\;\;\;\;\;\;\underline{-\;\;477} \\
\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;\;0
\end{array}$$

Иначе, тврђење следи на основу принципа математичке индукције, из чињенице да је дати низ бројева задат рекурентним формулама

$$a_1 = 1\,007, \quad a_{n+1} = (a_n - 6) \cdot 10 + 7 = 10a_n - 53,$$

а сам доказ препуштамо читаоцу.

(2) Тврђење доказујемо индукцијом по n.
За $n = 1$, $133 \mid 11^{1+2} + 12^{2\cdot 1+1} = 1\,331 + 1\,728 = 3\,059 = 23 \cdot 133$.
Претпоставимо да тврђење важи за неко $n \in \mathbb{N}$.
Тада је

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

па на основу индукцијске претпоставке $133 \mid 11^{n+3} + 12^{2n+3}$. Дакле, за свако $n \in \mathbb{N}$, $133 \mid 11^{n+2} + 12^{2n+1}$.

(3) Тврђење такође доказујемо индукцијом по n.
За $n = 1$, $3 \mid \overline{aaa}$.
Претпоставимо да $3^n \mid \overline{\underbrace{aa\ldots a}_{3^n}}$.

$$\begin{aligned} \overline{\underbrace{aa\ldots a}_{3^{n+1}}} &= \overline{\underbrace{aa\ldots a}_{3^n}\underbrace{aa\ldots a}_{3^n}\underbrace{aa\ldots a}_{3^n}} \\ &= 10^{2\cdot 3^n}\overline{\underbrace{aa\ldots a}_{3^n}} + 10^{3^n}\overline{\underbrace{aa\ldots a}_{3^n}} + \overline{\underbrace{aa\ldots a}_{3^n}} \\ &= (1\underbrace{00\ldots0}_{3^n-1}1\underbrace{00\ldots0}_{3^n-1}1) \cdot \overline{\underbrace{aa\ldots a}_{3^n}}\,. \end{aligned}$$

Како $3 \mid 1\underbrace{00\ldots0}_{3^n-1}1\underbrace{00\ldots0}_{3^n-1}1$ и по индукцијској претпоставци $3^n \mid \overline{\underbrace{aa\ldots a}_{3^n}}$, то $3^{n+1} \mid \overline{\underbrace{aa\ldots a}_{3^{n+1}}}$.

19. Одредити остатак дељења броја $6^{83} + 8^{83}$ са 49.

Решење:

$$\begin{aligned} 6^{83} + 8^{83} &= (7-1)^{83} + (7+1)^{83} \\ &= 7^{83} - \binom{83}{1}7^{82} + \cdots + \binom{83}{82}7 - 1 + \end{aligned}$$

$$
\begin{aligned}
&+ 7^{83} + \binom{83}{1} 7^{82} + \cdots + \binom{83}{82} 7 + 1 \\
&= N \cdot 49 + 2 \cdot \binom{83}{82} \cdot 7 = N \cdot 49 + 2 \cdot 83 \cdot 7 \\
&= N \cdot 49 + 2 \cdot (11 \cdot 7 + 6) \cdot 7 \\
&= N \cdot 49 + 2 \cdot 11 \cdot 49 + 49 + 35.
\end{aligned}
$$

Дакле, остатак дељења броја $6^{83} + 8^{83}$ са 49 је 35.

20. Доказати да за сваки природан број n важи:
(1) $6 \mid n^3 + 5n$; (2) $30 \mid n^5 - n$; (3) $120 \mid n^5 - 5n^3 + 4n$.

Решење. Ова тврђења се доказују применом принципа математичке индукције, али да она важе може се „видети“ из одговарајућих једнакости.

(1) $n^3 + 5n = n^3 - n + 6n = (n-1)n(n+1) + 6n$.

Како $2 \mid (n-1)n(n+1)$, $3 \mid (n-1)n(n+1)$ и $(2,3) = 1$, то важи $2 \cdot 3 = 6 \mid (n-1)n(n+1)$.

(2) $n^5 - n = n(n^4 - 1) = (n-1)n(n+1)(n^2+1)$.

Према (1) $6 \mid (n-1)n(n+1)$. Могуће је да наступе следећи случајеви:

(i) $n = 5k,$ за неки $k \in \mathbb{Z}$;
(ii) $n = 5k+1,$ за неки $k \in \mathbb{Z},$ тада је $n - 1 = 5k$;
(iii) $n = 5k+2,$ за неки $k \in \mathbb{Z},$ тада је $n^2 + 1 = 5(5k^2 + 2k + 1)$;
(iv) $n = 5k+3,$ за неки $k \in \mathbb{Z},$ тада је $n^2 + 1 = 5(5k^2 + 6k + 2)$;
(v) $n = 5k+4,$ за неки $k \in \mathbb{Z},$ тада је $n + 1 = 5(k+1)$.

(3) $n^5 - 5n^3 + 4n = n(n^4 - 5n^2 + 4) = n(n^2-4)(n^2-1)$
$= (n-2)(n-1)n(n+1)(n+2)$.

Производ пет узастопних бројева дељив је са $5! = 120$.

21. Ако је збир $2\,004$ природна броја дељив са 6, онда је и збир њихових кубова дељив са 6. Доказати.

Решење. Како је за сваки природан број a број

$$a^3 - a = (a-1)a(a+1)$$

дељив са 6, то је и број

$$\begin{aligned} a_1^3 - a_1 + a_2^3 - a_2 \ &+ \cdots + a_{2004}^3 - a_{2004} \\ &= (a_1^3 + a_2^3 + \cdots + a_{2004}^3) - (a_1 + a_2 + \cdots + a_{2004}) \end{aligned}$$

дељив са 6, па како је број $a_1 + a_2 + \cdots + a_{2004}$ дељив са 6, то је и број $a_1^3 + a_2^3 + \cdots + a_{2004}^3$ дељив са 6.

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

Решење. Доказ оба тврђења изводимо индукцијом по n.

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

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

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

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

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

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

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

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

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

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

23. Нека је n природан број. Доказати да је број

$$(n+1)(n+2)\cdots(n+n)$$

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

Решење. Доказаћемо индукцијом да се број 2 појављује тачно n пута као чинилац броја $(n+1)(n+2)\cdots(n+n)$.

За $n=1$ тврђење је очигледно тачно, јер је тада дати производ једнак 2.

Претпоставимо да се, за неки природан број n, број 2 у производу $(n+1)(n+2)\cdots(n+n)$ појављује као чинилац тачно n пута.

Тада је

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

па пошто се, према индукцијској претпоставци, 2 појављује тачно n пута као чинилац у производу $(n+1)(n+2)\cdots(n+n)$, а чинилац $2n+1$ је непаран те он није дељив са 2, следи да се у производу $(n+1+1)(n+1+1)\cdots(n+1+n-1)(n+1+n)(n+1+n+1)$ број 2 као чинилац појављује тачно $n+1$ пута.

24. Колико има природних бројева који нису већи од $2\,004$ за које важи $[\sqrt{n}] \mid n$?

Решење. Нека је $[\sqrt{n}]=k$. Тада је

$$k \leqslant \sqrt{n} < k+1, \quad \text{тј.} \quad k^2 \leqslant n < k^2+2k+1.$$

Између узастопних квадрата k^2 и $(k+1)^2$ само су бројеви k^2, k^2+k и k^2+2k дељиви са k. Према томе, у сваком од интервала $[1^2,2^2)$,

$[2^2, 3^2)$, $\ldots$, $[43^2, 44^2)$ постоје три природна броја који задовољавају дати услов. Како је $44^2 = 1\,936$, $44^2+44 = 1\,980$ и $44^2+2\cdot 44 = 2\,024$, бројева са траженом особином има $3 \cdot 43 + 2 = 131$.

25. Доказати да је збир $2n + 1$ узастопних природних бројева дељив са $2n + 1$.

Решење. Тврђење следи на основу једнакости

$$k + (k + 1) + (k + 2) + \cdots + (k + 2n) = (k + n)(2n + 1).$$

26. Доказати да ни за један природан број n број

$$1^{2005} + 2^{2005} + \cdots + n^{2005}$$

није дељив са $n + 2$.

Решење. Тврђење задатка следи на основу једнакости

$$\begin{aligned} 2\left(1 + 2^{2005} + \cdots + n^{2005}\right) &= 2 + \left(2^{2005} + n^{2005}\right) + \left(3^{2005} + (n-1)^{2005}\right) \\ &\quad + \cdots + \left(n^{2005} + 2^{2005}\right) = 2 + (n + 2)M, \end{aligned}$$

где је M цео број.

27. Ако су у троцифреном броју дељивом са 7 последње две цифре једнаке, доказати да је збир цифара тог броја дељив са 7.

Решење. Нека су $a, b \in \{0, 1, 2, \ldots, 9\}$, $a \neq 0$ такви да

$$7 \mid \overline{abb} = 100a + 10b + b = 100a + 11b = 98a + 7b + 2(a + b + b).$$

Тада $7 \mid a + b + b$, тј. збир цифара троцифреног броја $\overline{abb}$ дељив је са 7.

28. Нека су M и N два деветоцифрена броја са особином да ако се било која цифра броја M замени цифром са одговарајућег места у броју N (на пример, цифра десетица у M замени се цифром десетица из N), добија се број дељив са 7. Доказати да је сваки број, који се добије кад се нека цифра броја N замени одговарајућом цифром из M, дељив са 7.

Решење. Нека је

$$M = \overline{m_8m_7m_6m_5m_4m_3m_2m_1m_0} = \sum_{i=0}^{8} 10^i m_i$$

и

$$N = \overline{n_8n_7n_6n_5n_4n_3n_2n_1n_0} = \sum_{i=0}^{8} 10^i n_i\,.$$

Када се у M уместо цифре m_i напише одговарајућа цифра n_i из N, добије се број $M + 10^i(n_i - m_i)$. Како је тај број дељив са 7, за $i = 0, 1, \ldots, 8$, можемо писати $M + 10^i(n_i - m_i) = 7M_i$. Означимо са $N_i = N + 10^i(m_i - n_i)$, $i = 0, 1, \ldots, 8$, број који се добија када се у N цифра n_i замени одговарајућом цифром m_i из M. Треба доказати да је сваки N_i дељив са 7.

Сабирањем добијамо

$$7\sum_{i=0}^{8} M_i = 9M + \sum_{i=0}^{8} 10^i(n_i - m_i) = 9M + (N - M) = 8M + N,$$

па је

$$\begin{aligned} N_i &= N + 10^i(m_i - n_i) = \left(7\sum_{i=0}^{8} M_i - 8M\right) + (M - 7M_i) \\ &= 7\left(\left(\sum_{i=0}^{8} M_i\right) - M - M_i\right) \end{aligned}$$

дељив са 7, што је и требало доказати.

29. (ИМО 1998) Одредити све парове (a, b) природних бројева, такве да је број $a^2b + a + b$ дељив са $ab^2 + b + 7$.

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

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

Размотримо најпре 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 две могућности $a = 11$ и $a = 49$. Провером 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 $8(2a^2 + a + 2) = (4a + 9)(4a - 7) + 79$ следи да $4a + 9 \mid 79$, што је очигледно немогуће, па у овом случају нема решења.

Нека је сада $b \geqslant 3$. Како је

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

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

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

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

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

30. Ако су a, b, c цели бројеви, $m, n \in \mathbb{N}$, доказати да важи:

(1) $(a, c) = 1,\ (b, c) = 1 \Rightarrow (ab, c) = 1$;

(2) $(a, b) = 1 \Rightarrow (a^m, b^n) = 1$;

(3) $a \mid c,\ b \mid c,\ (a, b) = 1 \Rightarrow ab \mid c$.

Решење. (1) Како је $(a,c)=1$, то постоје бројеви $\alpha,\gamma_1\in\mathbb{Z}$ такви да је $\alpha a+\gamma_1 c=1$. Слично из $(b,c)=1$ следи да постоје бројеви $\beta,\gamma_2\in\mathbb{Z}$ такви да је $\beta b+\gamma_2 c=1$. Тада је $\alpha a\beta b=(1-\gamma_1 c)(1-\gamma_2 c)$, односно $\alpha\beta ab+(\gamma_1+\gamma_2-\gamma_1\gamma_2 c)c=1$, одакле следи да је $(ab,c)=1$.

(2) Према (1) имамо :

$$\begin{aligned}(a,b)=1\ &\Rightarrow (a^2,b)=1\Rightarrow\cdots\Rightarrow(a^m,b)=1\\ &\Rightarrow (a^m,b^2)=1\Rightarrow\cdots\Rightarrow(a^m,b^n)=1.\end{aligned}$$

(3) Због $(a,b)=1$ је $[a,b]=ab$. Како $a\mid c$ и $b\mid c$ то и $[a,b]\mid c$, односно $ab\mid c$.

31. Разлика два непарна броја једнака је 2^n. Доказати да су они узајамно прости.

Решење. Нека су a и b непарни бројеви. Тада је $d=(a,b)$ непаран број. Међутим, по услову задатка $d\mid 2^n$, одакле је $d=1$.

32. Ако је $(a,b)=1$, онда је $(a+b,a-b)$ једнак 1 или 2. Доказати.

Решење. Ако је $(a+b,a-b)=d$, тада је $a+b=dx$ и $a-b=dy$, одакле добијамо $2a=d(x+y)$ и $2b=d(x-y)$. То значи да је d заједнички делилац бројева $2a$ и $2b$. Како су a и b узајамно прости бројеви, то је $(2a,2b)=2$, па $d\mid 2$, тј. $d=1$ или $d=2$.

33. (ИМО 1959) Доказати да се за $n\in\mathbb{N}$ разломак $\dfrac{21n+4}{14n+3}$ не може скратити.

Решење. Тврђење следи из следећег низа једнакости:

$$(21n+4,14n+3)=(14n+3,7n+1)=(7n+1,1)=1.$$

34. Ако су a и b решења једначине $x^2+px-1=0$, где је p непаран број, тада су, за сваки ненегативан цео број n, бројеви a^n+b^n и $a^{n+1}+b^{n+1}$ цели и узајамно прости. Доказати.

Решење. Према Виетовим формулама је $a+b=-p$ и $ab=-1$. Доказаћемо тврђење задатка индукцијом.

За $n=0$ имамо: $a^0+b^0=2$ и $a^1+b^1=-p$ су узајамно прости.

Нека су a^n+b^n и $a^{n+1}+b^{n+1}$ цели и узајамно прости бројеви.

Број

$$\begin{aligned} a^{n+2}+b^{n+2} &= (a+b)\left(a^{n+1}+b^{n+1}\right)-ab\left(a^n+b^n\right) \\ &= -p\left(a^{n+1}+b^{n+1}\right)+\left(a^n+b^n\right) \end{aligned}$$

је такође цео. Ако бројеви $a^{n+2}+b^{n+2}$ и $a^{n+1}+b^{n+1}$ не би били узајамно прости, тада не би били узајамно прости ни бројеви $a^{n+1}+b^{n+1}$ и a^n+b^n. Одатле следи тврђење задатка.

35. Збир 49 природних бројева једнак је 999. Наћи највећу могућу вредност њиховог највећег заједничког делиоца.

Решење. Нека је збир природних бројева $a_1, a_2, \ldots, a_{49}$ једнак 999 и нека је $d=(a_1, a_2, \ldots, a_{49})$. Јасно, $d \mid 999 = 3^3 \cdot 37$. Такође, $d \mid a_i$ (и $d \leqslant a_i$), $i=1,2,\ldots,49$. Дакле, $999 = a_1+a_2+\cdots+a_{49} \geqslant 49d$, одакле следи да је $d \leqslant \dfrac{999}{49} < 21$. Једини делиоци броја 999, мањи од 21 су: 1, 3 и 9. Вредност $d=9$, може бити „достигнута“ на следећи начин

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

36. За природан број кажемо да је *палиндром* (или да је *симетричан*) ако је једнак броју записаном истим цифрама у обрнутом редоследу. (На пример бројеви 121, $1\,331$, $56\,788\,765$, $45\,699\,654$ су палиндроми.)

Наћи највећи заједнички делилац свих десетоцифрених палиндрома.

Решење. Сваки десетоцифрени палиндром је дељив са 11. Поред тога, како је

$$9\,999\,999\,999 = 11 \cdot 909\,090\,909$$

и

$$1\,000\,000\,001 = 11 \cdot 90\,909\,091,$$

а $90\,909\,091$ и $909\,090\,909$ су узајамно прости бројеви ($90\,909\,091 \cdot 10 - 909\,090\,909 = 1$), следи да је највећи заједнички делилац једнак 11.

37. (Чешко–словачка математичка олимпијада – друга рунда, 2003) Наћи највећи петоцифрени палиндром који је дељив са 101.

Решење. Било који петоцифрени палиндром $\overline{abcba}$ може се приказати у облику

$$\overline{abcba} = 10\,001a + 1\,010b + 100c = 101(99a + 10b + c) + 2a - c.$$

То значи да је тај палиндром дељив са 101 ако и само ако је $2a - c = 0$ (јер је за било које цифре a и c испуњено $|2a - c| < 101$). Једначина $2a = c$ имплицира да је $a \leqslant 4$. 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 $49\,894$.

38. Одредити најмањи природан број који при дељењу са $4, 6, 8$, 10 и 12 даје остатке редом $2, 4, 6, 8$ и 10.

Решење. Нека је n природан број такав да је $n = 4q_1 + 2$, за неко q_1, $n = 6q_2 + 4$, за неко q_2, $n = 8q_3 + 6$, за неко q_3, $n = 10q_4 + 8$, за неко q_4, $n = 12q_5 + 10$, за неко q_5.

Тада $4 \mid n + 2$, $6 \mid n + 2$, $8 \mid n + 2$, $10 \mid n + 2$, $12 \,|\, n + 2$, па $[4, 6, 8, 10, 12] \mid n + 2$. Најмањи природан број такав да $120 \mid n + 2$ ($[4, 6, 8, 10, 12] = 120$) је 118.

39. Наћи најмањи број који при дељењу са $n, n+1, \ldots, n+m$ даје редом остатке $r, r + 1, \ldots, r + m$.

Решење. То је број $[n, n+1, \ldots, n+m] - n + r$.

40. Природан број n подељен са 6 даје остатак 4, а подељен са 15 даје остатак 7. Колики је остатак при дељењу броја n са 30?

41. Ако су a и b природни бројеви, доказати да је

$$a^n + b^n \leqslant (a,b)^n + [a,b]^n \quad \text{за } n \in \mathbb{N}.$$

Решење. Нека је $d = (a,b)$ и $s = [a,b]$. Тада је $s \geqslant a$, $s \geqslant b$ и $ab = ds$. Из

$$d^n + s^n - a^n - b^n = \frac{(ds)^n + s^{2n} - a^n s^n - b^n s^n}{s^n} = \frac{(s^n - a^n)(s^n - b^n)}{s^n} \geqslant 0$$

следи тврђење задатка.

42. (Мала олимпијада 1969) 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 дељив са ab.

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

Претпоставимо сада да је $i = j$. Означимо са d највећи заједнички делилац 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 дељиви 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 следило $2d > x_b - x_1 + 1 = b$. 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 $x_i(x_i + d)$ дељив са $ds = ab$, а у супротном је $x_i(x_i - d)$ дељиво са ab.

43. Ако је $1!+2!+\cdots+n!=m!$, тада је $1!+2!+\cdots+m!=n!$. Доказати.

Решење. Претпоставимо да је $n>1$. Сви сабирци, осим првог, у збиру $1!+2!+\cdots+n!$ су парни. Стога је збир непаран, па је и $m!$ непаран број. То је могуће само за $m=1$. Међутим, за $n>1$ је $m>1$. Отуда је $m=n=1$ и једнакости тривијално важе.

44. Ако су a,b,m,n природни бројеви, $(a,b)=1$ и $a>1$, доказати импликацију

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

Решење. Нека су a,b,m,n природни бројеви, $(a,b)=1$, $a>1$ и $a^m+b^m \mid a^n+b^n$. Претпоставимо да $m \nmid n$. Тада је $n=qm+r$, $0<r<m$.

⌜ *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;

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

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

2. случај: q је паран; $q = s + 1$, s је непаран.

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

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

45. (Савезно такмичење 1969, II разред) Доказати да је за сваки природан број n бар један од бројева $3^{3n} + 2^{3n}$ и $3^{3n} - 2^{3n}$ дељив са 35.

Решење. Ако је n непаран број, онда је $3^{3n} + 2^{3n} = 27^n + 8^n$, па $27 + 8 = 35 \mid 27^n + 8^n$.

Ако је $n = 2k$, за неки $k \in \mathbb{N}$, онда је

$$3^{3n} - 2^{3n} = 3^{6k} - 2^{6k} = 729^k - 64^k = (729 - 64)\sum_{i=0}^{k-1} 729^{k-1-i}64^i,$$

па тврђење следи, јер је $729 - 64 = 19 \cdot 35$.

46. Нека су a, b и c цели бројеви такви да важи $a+b+c \mid a^2+b^2+c^2$. Доказати да постоји бесконачно много природних бројева n за које

$$a + b + c \mid a^n + b^n + c^n.$$

Решење. Докажимо индукцијом по броју k да је за све природне бројеве облика $n = 2^k$ испуњено:

$$a + b + c \mid a^n + b^n + c^n, \quad a + b + c \mid 2(a^n b^n + b^n c^n + c^n a^n).$$

За $k=1$ прво тврђење је очигледно, а друго следи из

$$2(ab+bc+ca)=(a+b+c)^2-(a^2+b^2+c^2).$$

Нека тврђење важи за неко k. Из

$$a^{2^{k+1}}+b^{2^{k+1}}+c^{2^{k+1}}=\left(a^{2^k}+b^{2^k}+c^{2^k}\right)^2-2\left(a^{2^k}b^{2^k}+b^{2^k}c^{2^k}+c^{2^k}a^{2^k}\right)$$

добијамо прво тврђење и за $k+1$, а из

$$\begin{aligned}&a^{2^{k+1}}b^{2^{k+1}}+b^{2^{k+1}}c^{2^{k+1}}+c^{2^{k+1}}a^{2^{k+1}}\\ =&\left(a^{2^k}b^{2^k}+b^{2^k}c^{2^k}+c^{2^k}a^{2^k}\right)^2-2\left(a^{2^k}+b^{2^k}+c^{2^k}\right)a^{2^k}b^{2^k}c^{2^k}\end{aligned}$$

и друго.

47. Наћи све природне бројеве који се завршавају двема истим цифрама којима се завршавају и њихови квадрати.

Решење. Нека је a природан број који се завршава са две исте цифре као и његов квадрат. Тада $100 \mid a^2-a=a(a-1)$, тј.

$$a(a-1)=100k=4\cdot 25\cdot k \quad \text{за неки } k.$$

Пошто је $(a-1,a)=1$, имамо да:

$$(25 \mid a \text{ и } 4 \mid a-1) \text{ или } (25 \mid a-1 \text{ и } 4 \mid a) \text{ или } 100 \mid a \text{ или } 100 \mid a-1.$$

У првом случају, када $25 \mid a$ и $4 \mid a-1$, број a се завршава цифрама 00, 25, 50 или 75, тј.

$$a=\overline{\ldots 00} \text{ или } a=\overline{\ldots 25} \text{ или } a=\overline{\ldots 50} \text{ или } a=\overline{\ldots 75}$$

па је

$$a-1=\overline{\ldots 99} \text{ или } a-1=\overline{\ldots 24} \text{ или } a-1=\overline{\ldots 49} \text{ или } a-1=\overline{\ldots 74}.$$

Једино у случају када се a завршава цифрама 25, број $a-1$ је дељив са 4, па $100 \mid a^2-a$.

У другом случају, када $25 \mid a-1$ и $4 \mid a$, број $a-1$ се завршава цифрама 00, 25, 50 или 75, тј.

$$a-1=\overline{\ldots 00} \text{ или } a-1=\overline{\ldots 25} \text{ или } a-1=\overline{\ldots 50} \text{ или } a-1=\overline{\ldots 75},$$

па је

$$a=\overline{\ldots 01} \text{ или } a=\overline{\ldots 26} \text{ или } a=\overline{\ldots 51} \text{ или } a=\overline{\ldots 76}.$$

Једино у случају када се $a-1$ завршава цифрама 75, тј. a се завршава цифрама 76, број a је дељив са 4, па $100 \mid a^2-a$.

Ако $100 \mid a$, тада су 00 последње две цифре броја a, па $100 \mid a^2-a$.

Најзад, ако $100 \mid a-1$, последње две цифре броја a су 01, и $100 \mid a^2-a$.

Дакле, тражени бројеви су сви бројеви које се завршавају цифрама 25, 76, 00 или 01.

48. (ММО 2002) Наћи све природне бројеве x, y такве да $y \mid x^2+1$ и $x^2 \mid y^3+1$.

Решење. Ако је $x=y$, тада је $x=y=1$ једно решење. Такође, ако је $y=2$, тада је $x=1$ или $x=3$. Дакле, нашли смо три решења: $(1,1)$, $(1,2)$, $(3,2)$.

Нека је сада (x,y) решење такво да је $x \neq y$ и $y>2$. Тада су бројеви $\dfrac{x^2+1}{y}$ и $\dfrac{y^3+1}{x^2}$ природни и њихов производ је такође природан број. Како је

$$\frac{x^2+1}{y} \cdot \frac{y^3+1}{x^2} = y^2 + \frac{x^2+y^3+1}{x^2 y}$$

и број $\dfrac{x^2+y^3+1}{x^2y}$ је такође природан. Међутим, тада је

$$\begin{aligned} x^2+y^3+1 \geqslant x^2y &\Leftrightarrow x^2(y-1) \leqslant y^3+1 \\ &\Leftrightarrow x^2 \leqslant \frac{y^3+1}{y-1} = y^2+y+1+\frac{2}{y-1} \\ &\Rightarrow x^2 \leqslant y^2+y+1+1 \\ &\Rightarrow x^2 < (y+1)^2 \\ &\Rightarrow x < y+1 \end{aligned}$$

Дакле, ако је (x,y) решење такво да је $x \neq y$ и $y > 2$, тада је $x < y$. Даље, из $y \mid x^2+1$ следи да је $x^2+1 = yy_1$, за неки природан број y_1. Очигледно је $x > 1$. Ако би било $y_1 \geqslant x$, имали бисмо

$$yy_1 \geqslant (x+1)x = x^2+x > x^2+1,$$

што је немогуће. Дакле, $y_1 < x$. Из једнакости $x^2+1 = yy_1$ следи да $y_1 \mid x^2+1$, као и да је $y = \dfrac{x^2+1}{y_1}$ и

$$y^3+1 = \frac{(x^2+1)^3}{y_1^3}+1 = \frac{(x^2+1)^3+y_1^3}{y_1^3},$$

па $x^2 \mid \dfrac{(x^2+1)^3+y_1^3}{y_1^3}$, одакле следи да $x^2 \mid (x^2+1)^3+y_1^3$, тј. да $x^2 \mid y_1^3+1$.

На крају имамо да $y_1 \mid x^2+1$, $x^2 \mid y_1^3+1$ и $y_1 < x$, па мора бити $y_1 \leqslant 2$. Дакле, проблем се своди на следеће случајеве:

(1) $y_1 = 1$: тада је $y = x^2+1$, тј. $x^2 = y-1$ и $(y-1) \mid y^3+1$. Међутим,

$$y^3+1 = y^3-1+2 = (y-1)(y^2+y+1)+2,$$

па $y-1 \mid 2$, одакле је $y=3$, а директном провером видимо да ово није решење.

(2) $y_1 = 2$: тада је $2y = x^2+1$, тј. $x^2 = 2y-1$ и $2y-1 \mid y^3+1$, па и $2y-1 \mid 8y^3+8$. Међутим, из

$$8y^3+8 = (2y-1)(4y^2+4y+1)+9$$

добијамо да $2y-1 \mid 9$. Тада из $y>2$, тј. $2y-1>3$, добијамо $y=5$, одакле директно налазимо да је $x=3$.

Дакле, решења су: $(1,1)$, $(1,2)$, $(3,2)$, $(3,5)$.

3. Прости бројеви

Дефиниција 3.1. *Цео број $p > 1$ је* ***прост*** *ако нема ниједан делилац d, $1 < d < p$. Цео број $m > 1$ који није прост је* ***сложен*** *број.*

Теорема 3.1. *Природан број $n > 1$ је сложен ако и само ако има прост фактор p, такав да је $p \leqslant \sqrt{n}$.*

Доказ. Ако n има прост фактор $p \leqslant \sqrt{n}$, онда је он очигледно сложен број. Обрнуто, ако је p најмањи прост фактор сложеног броја n, тада постоји природан број q такав да је $n = pq$, и при том је $q \geqslant p$. Одатле следи да је $p \leqslant \sqrt{n}$. ■

Теорема 3.2. (***Еуклид***) *Постоји бесконачно много простих бројева, тј. од сваког простог броја постоји већи прост број.*

Доказ. Претпоставимо супротно, тј. да постоји коначно много простих бројева. Нека су то бројеви $p_1, p_2, \ldots, p_k$, и нека су сви остали природни бројеви (већи од 1) сложени. Посматрајмо број $n = p_1 p_2 \cdots p_k + 1$. Према нашој претпоставци он мора бити сложен, па мора бити дељив неким простим бројем. Међутим, то је немогуће јер при дељењу било којим од бројева $p_1, p_2, \ldots, p_k$ даје остатак 1. Контрадикција. ■

Теорема 3.3. *Ако је дат произвољан природан број k, увек се може наћи k узастопних сложених бројева.*

Доказ. Посматрајмо следећих k узастопних природних бројева:

$$\begin{aligned}
A_1 &= (k+1)k(k-1)\cdots 3\cdot 2\cdot 1 + 2\\
A_2 &= (k+1)k(k-1)\cdots 3\cdot 2\cdot 1 + 3\\
&\ \vdots\\
A_k &= (k+1)k(k-1)\cdots 3\cdot 2\cdot 1 + k + 1.
\end{aligned}$$

Пошто је број A_1 дељив са 2, A_2 са 3, $\dots$, A_k са $k+1$, свих k бројева су сложени. ∎

Теорема 3.4. (***Еуклидова лема***) *Ако је p прост број и $p \mid ab$, онда $p \mid a$ или $p \mid b$.*

Доказ. Претпоставимо да $p \nmid a$. Тада је $(p,a)=1$, па $p \mid b$ (теорема 2.8.). ∎

Теорема 3.5. (***Основни став аритметике***) *Сваки природан број N већи од 1 може се једнозначно представити у облику производа простих чинилаца (са тачношћу до њиховог поретка). Прецизније, за сваки природан број $N>1$ постоје јединствени прости бројеви $p_1,p_2,\dots,p_k$, такви да је $p_1<p_2<\dots<p_k$, и јединствени природни бројеви $\alpha_1,\alpha_2,\dots,\alpha_k$ тако да је*

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \qquad (\textbf{\textit{Канонска факторизација}}\ \textit{броја}\ N.)$$

Доказ. Ако је N прост број тврђење очигледно важи. Претпоставимо да тврђење важи за сваки сложен број мањи од N. Ако је N сложен број, тада постоји природан број d такав да је $1<d<N$ и $d \mid N$. Означимо најмањи такав број са p_1. Тада p_1 мора бити прост број (ако би био сложен тада би постојао прост број $p<p_1$, такав да $p \mid p_1$, али тада $p \mid N$, што је у супротности са избором броја p_1 као најмањег природног броја већег од 1 који дели N). Тада је $N=p_1n_1$, где је $1<n_1<N$. По индукцијској претпоставци број n_1 се може представити као производ простих фактора, па према томе може и N. Групишући једнаке просте факторе броја N, закључујемо да се сваки природан број $N>1$ може представити у облику

$$N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

где су $p_1<p_2<\dots<p_k$ прости бројеви и $\alpha_1,\alpha_2,\dots,\alpha_k \in \mathbb{N}$.

Докажимо сада да је представљање броја N у облику производа простих чинилаца јединствено. Претпоставимо супротно, тј. да природан број N има две такве факторизације:

$$\begin{array}{lll} N = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, & p_1 < p_2 < \cdots < p_k, & \alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{N} \\ N = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}, & q_1 < q_2 < \cdots < q_\ell, & \beta_1, \beta_2, \ldots, \beta_\ell \in \mathbb{N}. \end{array}$$

С обзиром на то да $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$, $1 \leqslant i \leqslant k$, то постоји индекс j такав да је $p_i = q_j$, $1 \leqslant j \leqslant \ell$. Дакле, $\{p_1, p_2, \ldots, p_k\} \subseteq \{q_1, q_2, \ldots, q_\ell\}$ и симетрично $\{q_1, q_2, \ldots, q_\ell\} \subseteq \{p_1, p_2, \ldots, p_k\}$. Према томе, $k = \ell$ и с обзиром на то да су низови $p_1, p_2, \ldots, p_k$ и $q_1, q_2, \ldots, q_\ell$ растући, следи да је $p_1 = q_1$, $p_2 = q_2, \ldots, p_k = q_k$.

Претпоставимо да је $\alpha_1 \neq \beta_1$, на пример $\alpha_1 = \beta_1 + \gamma$, $\gamma > 0$. Тада

$$p_1^{\gamma} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = p_2^{\beta_1} \cdots p_k^{\beta_k},$$

па p_1 дели леву и не дели десну претходне једнакости, што је контрадикција, па је $\alpha_1 = \beta_1$. Слично $\alpha_2 = \beta_2, \ldots, \alpha_k = \beta_k$, одакле следи јединственост факторизације. ■

Користећи основни став аритметике лако се одређује највећи заједнички делилац и најмањи заједнички садржалац задатих природних бројева. Наиме, ако је

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

(неки од бројева α_i, β_i могу бити и једнаки нули), имамо да је:

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \cdots p_k^{\min\{\alpha_k, \beta_k\}},$$

$$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} p_2^{\max\{\alpha_2, \beta_2\}} \cdots p_k^{\max\{\alpha_k, \beta_k\}}.$$

Одавде, због једнакости

$$\min\{\alpha, \beta\} + \max\{\alpha, \beta\} = \alpha + \beta$$

добијамо елегантан доказ теореме 2.11.

ТЕОРЕМА 3.6. *Ако је производ два узајамно проста природна броја квадрат целог броја, тј. ако је* $ab = c^2$, $(a, b) = 1$, *тада су и* a *и* b *квадрати целих бројева:* $a = a_1^2$, $b = b_1^2$.

ДОКАЗ. Да би број био квадрат целог броја, неопходно је и довољно да су му сви експоненти у канонској факторизацији парни. Како су a и b узајамно прости, то они немају заједничких делилаца, па је сваки прост делилац броја c^2 или делилац броја a или делилац броја b, али не и делилац оба ова броја. Зато сви прости фактори бројева a и b у канонској факторизацији морају имати парне експоненте, тј. a и b су квадрати целих бројева. ■

ТЕОРЕМА 3.7. *Нека је* $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *канонска факторизација броја* a. *Тада су сви позитивни делиоци броја* a *облика*

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad 0 \leqslant \beta_i \leqslant \alpha_i \ \ (i = \overline{1, k}).$$

Специјално, ако укупан број позитивних делилаца броја a (*укључујући* 1 *и само* a) *означимо са* $\tau(a)$, *тада је*

$$\tau(a) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1).$$

Ако збир свих позитивних делилаца броја a *означимо са* $\sigma(a)$, *тада је*

$$\sigma(a) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

ДОКАЗ. Важи да $d \mid a$ јер је $a = md$, где је $m = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$, где је $\gamma_i = \alpha_i - \beta_i$, за $i = 1, 2, \ldots, k$. Очигледно је да делиоци броја a не могу садржати у својој канонској факторизацији просте бројеве који нису у канонској факторизацији броја a, нити може неко β_i бити веће од одговарајућег α_i.

Из првог дела теореме видимо да се код произвољног делиоца d броја a, експонент β_i, са којим се прост број p_i појављује у канонској факторизацији броја d, може изабрати на α_i+1 начина, одакле следи да је

$$\tau(a)=(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_k+1).$$

Остаје још да докажемо да важи дата формула за збир делилаца броја a. То ћемо доказати индукцијом по броју (различитих) простих делилаца броја a.

Ако је $a=p^\alpha$, за неки прост број p и неко $\alpha\in\mathbb{N}$, тада су $1,p,p^2,\dots,p^\alpha$ сви позитивни делиоци броја a, и важи

$$1+p+p^2+\cdots+p^\alpha=\frac{p^{\alpha+1}-1}{p-1}.$$

Претпоставимо да једнакост важи за све природне бројеве који имају k (различитих) простих делилаца.

Нека је $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}\cdot p_{k+1}^{\alpha_{k+1}}$. Ако је $a_0=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, тада имамо да су:

$$\begin{array}{llll} d_1, & d_1\cdot p_{k+1}, & \dots, & d_1\cdot p_{k+1}^{\alpha_{k+1}} \\ d_2, & d_2\cdot p_{k+1}, & \dots, & d_2\cdot p_{k+1}^{\alpha_{k+1}} \\ \vdots & & & \end{array}$$

сви делиоци броја a, где су $d_1,d_2,\dots$ сви делиоци броја a_0, па је

$$\begin{aligned}\sigma(a)=\sum_{d|a}d&=\sum_{d|a_0}\left(d+d\cdot p_{k+1}+\cdots+d\cdot p_{k+1}^{\alpha_{k+1}}\right)\\ &=\left(1+p_{k+1}+\cdots+p_{k+1}^{\alpha_{k+1}}\right)\sum_{d|a_0}d\\ &=\frac{p_{k+1}^{\alpha_{k+1}+1}-1}{p_{k+1}-1}\cdot\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1}-1}{p_k-1}.\end{aligned}$$ ■

ДЕФИНИЦИЈА 3.2. *Функција $f:\mathbb{N}\to\mathbb{Z}$ је мултипликативна ако:*

(1) *за неко $n_0\in\mathbb{N}$ је $f(n_0)\neq 0$;*

(2) *ако је $(m,n)=1$, онда је $f(mn)=f(m)f(n)$.*

ТЕОРЕМА 3.8. *Функције τ и σ су мултипликативне.*

ДОКАЗ. Ако су m и n узајамно прости бројеви, тада је

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{и} \quad n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell},$$

при чему се ниједан од бројева p_i не поклапа ни са једним од бројева q_j. Тада је

$$mn = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} q_1^{\beta_1} q_2^{\beta_2} \cdots q_\ell^{\beta_\ell}$$

канонска факторизација броја mn, па на основу теореме 3.7. следи

$$\tau(mn) = (\alpha_1 + 1) \cdots (\alpha_k + 1)(\beta_1 + 1) \cdots (\beta_\ell + 1) = \tau(m)\tau(n)$$

и

$$\sigma(mn) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_k^{\alpha_k+1} - 1}{p_k - 1} \frac{q_1^{\beta_1+1} - 1}{q_1 - 1} \cdots \frac{q_\ell^{\beta_\ell+1} - 1}{q_\ell - 1} = \sigma(m)\sigma(n).$$

Дакле, функције τ и σ су мултипликативне. ∎

На крају ћемо дати елегантнији, али теже читљив, запис доказа формуле за збир делилаца броја a (теорема 3.7.). Збир свих делилаца броја a је

$$\begin{aligned}
\sigma(a) &= \sum_{\beta_1=0}^{\alpha_1} \sum_{\beta_2=0}^{\alpha_2} \cdots \sum_{\beta_k=0}^{\alpha_k} p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} \\
&= \prod_{i=1}^{k} \left(1 + p_i + p_i^2 + \cdots + p_i^{\alpha_i}\right) \\
&= \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.
\end{aligned}$$

3.1. Фермаови бројеви

Велики број математичара је безуспешно покушавао да нађе општу формулу за просте бројеве, тј. полином $P(x)$ чије би вредности за све ненегативне целе бројеве биле прости бројеви. Интересантан је полином $P(n) = n^2 - 79n + 1\,601$ који за $0 \leqslant n \leqslant 79, n \in \mathbb{Z}$, даје просте бројеве, али за $n = 80$ је $f(80) = 80^2 - 79 \cdot 80 + 1\,601 = 1\,681 = 41^2$.

Лема 3.1. *За сваки полином $P(x)$, степена већег од 1, са целобројним коефицијентима, постоји природан број n такав да $P(n)$ није прост број.*

Доказ. За сваки природан број a постоји полином $A(x)$ са целобројним коефицијентима такав да је

$$P(x) = (x - a)A(x) + P(a).$$

Ако полином $P(x)$ има корен који је природан број, тј. постоји природан број a_0 такав да је $P(a_0) = 0$, тада је $P(x) = (x - a_0)A_0(x)$, за $x \in \mathbb{N}$, при чему је A_0 неки полином са целобројним коефицијентима, одакле није тешко закључити да постоји природан број n такав да је $P(n)$ сложен.

Ако полином $P(x)$ нема корен који је природан број, тада постоји природан број a такав да је $P(a) > 1$ (или $P(a) < -1$), а такође и, довољно велики, природан број m такав да је за $n_0 = a + mP(a)$, $n_0 \in \mathbb{N}$, $A(n_0) \neq 0$ (полином $A(x)$ има највише коначно много корена) и $1 + mA(n_0) \notin \{-1, 0, 1\}$. Тада је

$$P(n_0) = P(a)(mA(n_0) + 1),$$

тј. $P(n_0)$ је сложен број. ■

НАПОМЕНА. Скуп простих бројева је скуп свих позитивних вредности полинома (има 26 променљивих и 25-ог је степена):

$$(k+2)(1-(wz+h+j-q)^2-((gk+2g+k+1)(h+j)+h-z)^2-$$
$$(2n+p+q+z-e)^2-(16(k+1)^3(k+2)(n+1)^2+1-f^2)^2-$$
$$(e^3(e+2)(a+1)^2+1-o^2)^2-((a^2-1)y^2+1-x^2)^2-$$
$$(16r^2y^4(a^2-1)+1-u^2)^2-$$
$$(((a+u^2(u^2-a))^2-1)(n+4dy)^2+1-(x+cu)^2)^2-$$
$$(n+L+v-y)^2-((a^2-1)L^2+1-m^2)^2-(ai+k+1-L-i)^2-$$
$$(p+L(a-n-1)+b(2an+2a-n^2-2n-2)-m)^2-$$
$$(q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x)^2-$$
$$(z+pL(a-p)+t(2ap-p^2-1)-pm)^2)$$

У вези са тражењем формула које дају просте бројеве поменућемо погрешну *Фермаову хипотезу*. Ферма је изучавао бројеве облика

$$f_n = 2^{2^n}+1 \qquad (n \in \mathbb{N} \cup \{0\}),$$

који се по њему називају ***Фермаови бројеви***. За првих 5 вредности од n Ферма је добио редом бројеве

$$f_0 = 3,\ f_1 = 5,\ f_2 = 17,\ f_3 = 257,\ f_4 = 65\,537.$$

Провером је утврдио да су сви они прости. Он је изрекао хипотезу да је и за све $n \geqslant 5$ број f_n прост. Међутим, Ојлер је показао да је број

$$f_5 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417$$

сложен.

Напоменимо још да до данас није пронађен ни један прост Фермаов број већи од f_4.

Показано је да је питање да ли је неки Ферамов број прост или сложен повезано са проблемом конструкције правилних многоуглова помоћу лењира и шестара.

ТЕОРЕМА 3.9. (***Гаус***) *Правилан многоугао са n страница може се конструисати шестаром и лењиром ако и само ако је n природан број облика $n = 2^s p_1 p_2 \dots p_k$, где је s ненегативан цео број, а $p_1, p_2, \dots, p_k$ различити Фермаови прости бројеви или је $n = 2^s$, где је $s > 1$ цео број.*

Напоменимо да је Гаус био „одушевљен“ доказом да се правилни 17-тоугао може конструисати лењиром и шестаром и да је његова жеља била да му на надгробном споменику буде урезан баш правилан 17-тоугао.

3.2. Мерсенови бројеви

ТЕОРЕМА 3.10. *Ако је n природан број и $2^n - 1$ прост број, онда је и n прост број.*

ДОКАЗ. Доказаћемо еквивалентно тврђење, тј. да је $2^n - 1$ сложен број ако је n сложен број. Нека је $n = rs$, $r > 1, s > 1$. Тада је

$$\begin{aligned} 2^n - 1 = 2^{rs} - 1 &= (2^r)^s - 1 \\ &= (2^r - 1)\left((2^r)^{s-1} + (2^r)^{s-2} + \cdots + 1\right), \end{aligned}$$

тј. број $2^n - 1$ је сложен. ■

Обрат претходне теореме не важи што показује следећи пример

$$2^{11} - 1 = 2\,047 = 23 \cdot 89.$$

Бројеви облика $M_n = 2^n - 1$, $n \in \mathbb{N}$ називају се Мерсенови бројеви. Видели смо (теорема 3.10.) да они могу бити прости само ако је n прост број.

За просте бројеве p, бројеви $M_p = 2^p - 1$, који су и сами прости, називају се ***прости Мерсенови бројеви***.

Иначе, Мерсен је ове бројеве изучавао у вези са савршеним бројевима.

ДЕФИНИЦИЈА 3.3. *Природан број n је* ***савршен број*** *ако је једнак збиру свих својих позитивних делилаца (искључујући сам број n), тј. ако је $\sigma(n) = 2n$.*

Прва три савршена броја су $6 = 1+2+3$, $28 = 1+2+4+7+14$, $496 = 1+2+4+8+16+31+62+124+248$, и то су једини савршени бројеви мањи од $1\,000$. Четврти савршен број је $8\,128$. Приметимо да важи:

$$6 = 2 \cdot 3, \quad 28 = 4 \cdot 7, \quad 496 = 16 \cdot 31, \quad 8\,128 = 64 \cdot 127.$$

ТЕОРЕМА 3.11. *Ако је $2^p - 1$ прост број онда је $2^{p-1}\left(2^p - 1\right)$ савршен број и сваки паран савршен број је тог облика.*

ДОКАЗ. Нека је $k = 2^p - 1$ прост број и $n = 2^{p-1}\left(2^p - 1\right)$. 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

$$\begin{aligned}\sigma(n) &= \sigma\left(2^{p-1}\right) \cdot \sigma(k) \\ &= \left(1 + 2 + 2^2 + \cdots + 2^{p-1}\right) \cdot 2^p \\ &= \left(2^p - 1\right) \cdot 2 \cdot 2^{p-1} = 2n,\end{aligned}$$

одакле следи да је број n савршен.

Обрнуто, нека је n произвољан паран савршен број. Запишимо га у облику $n = 2^{p-1}m$, где је m непаран број и $p \geqslant 2$. Из мултипликативности функције σ следи:

$$\sigma\left(2^{p-1}m\right) = \sigma\left(2^{p-1}\right)\sigma(m) = \left(2^p - 1\right) \cdot \sigma(m).$$

Пошто је n савршен број то је

$$\sigma(n) = 2n = 2^p m.$$

Из претходне две једнакости следи

$$2^p m = (2^p - 1) \cdot \sigma(m),$$

па закључујемо да $2^p - 1 \mid 2^p m$, тј. да $2^p - 1 \mid m$. Према томе, $m = (2^p - 1)\,M$. Замењујући то у претходну једнакост добијамо

$$2^p\,(2^p - 1)\,M = (2^p - 1) \cdot \sigma(m), \text{ тј. } \quad 2^p M = \sigma(m).$$

Како су и m и M делиоци од m то је

$$2^p M = \sigma(m) \geqslant m + M = 2^p M,$$

па је $\sigma(m) = m + M$. То значи да је број m прост и једина његова два делиоца су m и $1 = M$. Према томе, $m = 2^p - 1$ је прост број, што је и требало доказати. ∎

Напоменимо да није познато да ли постоје непарни савршени бројеви. Ово је један од најстаријих нерешених проблема у математици. Познато је једино да би такав број, ако постоји, морао имати најмање 300 цифара у декадном запису и да би морао имати прост делилац већи од 10^{20}. Иначе, парни савршени бројеви се могу завршавати једино цифрама 6 и 8, што се лако може показати коришћењем претходне теореме.

Налажење што већег простог броја је велики изазов за многе математичаре. Данас се то углавном своди на налажење што већег Мерсеновог простог броја.

Џорџ Волтман је 1996. године основао међународно удружење GIMPS (the **G**reat **I**nternet **M**ersenne **P**rime **S**earch) које има више од $100\,000$ чланова који трагају за што већим Мерсеновим простим бројем. При том користе интернет и заједнички централни рачунар (GIMPS) за тестирање и проверу. До оснивања овог удружења била су позната 34 Мерсенова броја, а до сада је откривено још 6.

38. Мерсенов прост број $2^{6972593} - 1$ је откривен 1999. (Clarkson, Woltman, Kurowski), и то је био први откривени прост број са више од $1\,000\,000$ цифара. У његовом декадном запису има $2\,098\,960$ цифара.

После тога су откривена још два Мерсенова проста броја, и то $2^{13466917} - 1$ (Cameron, Woltman, Kurowski 2001. године, $4\,053\,946$ цифара) и

$$2^{20996011} - 1$$

(Shafer, Woltman, Kurowski 17. новембра 2003. године), али још траје провера да ли је до сада највећи откривени прост број (у чијем декадном запису учествује $6\,320\,430$ цифара) 40. Мерсенов прост број или можда има још неки мањи од њега који није познат. Можда ће то бити познато када ви будете читали ову књигу. Можда ће до тада бити откривен још неки Мерсенов прост број. Зато посетите сајт

`http://www.mersenne.org/status.htm`

где се резултати ажурирају на сваких сат времена.

Тренутно је актуелна награда од $100\,000$ америчких долара за прву особа која пронађе прост број са више од $10\,000\,000$ цифара.

3.3. Дистрибуција простих бројева

ТЕОРЕМА 3.12. (**Теорема о простим бројевима**) *Обележимо са $\pi(n)$ број простих бројева не већих од n. Тада важи*

$$\pi(n) \sim \frac{n}{\ln n}.$$

(*Чита се:* $\pi(n)$ *је асимптотски једнако са* $\dfrac{n}{\ln n}$.)

Доказ претходне теореме захтева сложен математички апарат, па ћемо га изоставити. Теорема о простим бројевима заправо тврди да за сваки реалан број $\varepsilon > 0$ (ма колико он био мали) постоји неки природан број n_0 (који зависи од ε), такав да је за све природне бројеве $n > n_0$ испуњено

$$1 - \varepsilon < \frac{\pi(n)}{\dfrac{n}{\ln n}} < 1 + \varepsilon.$$

Напоменимо само да је ово тврђење изнео као хипотезу Гаус 1840. године, а доказали су је независно Вале-Пусен и Адамар 1896. Пре њих, тачније 1850. године, Чебишев је доказао да за сваки природан број $n > 1$ важи

$$\frac{7}{8} \cdot \frac{n}{\ln n} \leqslant \pi(n) \leqslant \frac{9}{8} \cdot \frac{n}{\ln n}.$$

Навешћемо без доказа још једну теорему која говори о дистрибуцији простих бројева:

ТЕОРЕМА 3.13. (***Дирихле***) *Нека су a и m узајамно прости природни бројеви. Тада сваки аритметички низ $(a + km)$, $k = 0, 1, 2 \ldots$ садржи бесконачно много простих бројева.*

3.4. Задаци

49. Доказати да је сваки прост број $p > 3$ облика $6k + 1$ или $6k + 5$ $(k \in \mathbb{N} \cup \{0\})$.

Решење. Сви ненегативни цели бројеви су облика $6k$, $6k+1$, $6k+2$, $6k+3$, $6k+4$ или $6k+5$ ($k \in \mathbb{N} \cup \{0\}$). Пошто бројеви $6k$, $6k+2$, $6k+3$ и $6k+4$ не могу бити прости, сваки прост број већи од 3 је облика $6k+1$ или $6k+5$.

$\ulcorner$ *Напомена.* Еквивалентна формулација тврђења претходног задатка је да је сваки прост број $p > 3$ облика $6k+1$ или $6k-1$ ($k \in \mathbb{N}$), што се често краће записује $p = 6k \pm 1$ ($k \in \mathbb{N}$). $\lrcorner$

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

(2) Ако су p и q прости бројеви већи од 3, доказати да важи $24 \mid p^2 - q^2$.

Решење. (1) Пошто је $p^2 - 1 = (p-1)(p+1)$ и како је p непаран број, то су $p-1$ и $p+1$ два узастопна парна броја и њихов производ је дељив са 8. Даље, $p-1, p, p+1$ су 3 узастопна природна броја, па је један од њих дељив са 3. То сигурно није p јер је p прост број већи од 3, па је један од бројева $p-1$ и $p+1$ дељив са 3, а онда је и њихов производ, тј. p^2-1, дељив са 3.

Дакле, $3 \mid p^2 - 1$ и $8 \mid p^2 - 1$, па како је $(3,8) = 1$, то следи да $24 = 3 \cdot 8 \mid p^2 - 1$.

(2) Тврђење (2) следи из тврђења (1) због

$$p^2 - q^2 = (p^2 - 1) - (q^2 - 1).$$

51. Наћи све просте бројеве p такве да су и бројеви

(а) $8p^2 + 1$; (б) $p + 10$ и $p + 14$; (в) $p^2 + 4$ и $p^2 + 6$

прости.

Решење. (а) 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

$$8(6k+1)^2+1=8(36k^2+12k+1)+1=3\cdot(96k^2+32k+3)$$

сложен број. Ако је $p=6k+5$, тада је

$$8(6k+5)^2+1=8(36k^2+60k+25)+1=3\cdot(96k^2+160k+67)$$

сложен број.

Дакле, једино решење је $p=3$.

(б) (*Прво решење*) За $p=2$ број $p+10=12$ није прост.

За $p=3$ бројеви $p+10=13$ и $p+14=17$ су прости.

Ако је $p=5$, тада опет број $p+10=15$ није прост.

Нека је p прост број већи од 5. Могућа су два случаја:

$p=6k+1$ за неки k – тада је $p+14=6k+15=3(2k+5)$ сложен број;

$p=6k+5$ за неки k – тада је $p+10=6k+15=3(2k+5)$ сложен број.

(*Друго решење*) Сваки природан број је облика $3k$, $3k+1$ или $3k+2$. 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 решење.

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.

(в) Ако је $p=2$, тада је $p^2+4=8$ сложен број.

За $p=3$ је $p^2+6=15$ сложен број.

За $p=5$ су бројеви $p^2+4=29$ и $p^2+6=31$ 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 решење је $p = 5$.

52. Ако су бројеви p и $2p^2 + 1$ прости, доказати да је и $3p^2 + 2$ такође прост.

Решење. Ако је p прост број већи од 3, тада је p облика $6k + 1$ или $6k+5$ за неко k. Ако је $p = 6k+1$, тада је број $2p^2+1 = 2(6k+1)^2+1 = 2(36k^2 + 12k + 1) + 1 = 3(24k^2 + 8k + 1)$ сложен. Ако је $p = 6k + 5$, тада је опет број $2p^2 + 1 = 2(6k+5)^2 + 1 = 2(36k^2 + 60k + 25) + 1 = 3(24k^2 + 40k + 17)$ сложен.

Дакле, p је прост број мањи од 5, тј. $p = 2$ или $p = 3$.

Ако је $p = 2$, тада је $2p^2 + 1 = 9$ сложен број.

За $p = 3$, $2p^2 + 1 = 19$ је прост број, а прост је и $3p^2 + 2 = 29$.

53. (а) Ако су p и $8p - 1$ прости бројеви, доказати да је $8p + 1$ сложен број.

(б) Ако су p и $2p + 1$ прости бројеви $(p > 3)$, доказати да је $4p + 1$ сложен број.

Решење. (а) Важно је приметити да је тврђење овог дела задатка еквивалентно са:

ако је p прост број, тада је $8p - 1$ сложен или је $8p + 1$ сложен.

Заиста, ако је $q =$ "број p је прост", $r =$ "број $8p - 1$ је прост", $s =$ "број $8p + 1$ је прост", тврђење под (а) је

$$q \wedge r \Rightarrow \neg s,$$

па пошто је формула $(q \wedge r \Rightarrow \neg s) \Leftrightarrow (q \Rightarrow \neg r \vee \neg s)$ таутологија, тврђење под (а) може се формулисати и на следећи начин:

(∗) ако је p прост број, тада је бар један од бројева
$8p-1$ или $8p+1$ сложен.

За $p=2$ број $8p-1$ није прост. За $p=3$ тврђење очигледно важи. Сваки прост број $p>3$ је облика $3k-1$ или $3k+1$, за неки природан број k.

Ако је p прост број облика $3k-1$, за неки k, тада је $8p-1=24k-9=3(8k-3)$ сложен јер је $8k-3>1$ за $k\geqslant 1$.

Ако је p прост број облика $3k+1$, за неки k, тада је $8p+1=24k+9=3(8k+3)$ сложен јер је $8k+3>1$ за $k\geqslant 1$.

(б) Слично као у делу (а), довољно је доказати да важи:

ако је p прост број већи од 3, тада је бар један
од бројева $2p+1$ или $4p+1$ сложен.

54. 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?

Решење:

$$\begin{aligned}(a+b+c+d)^2 &= a^2+b^2+c^2+d^2+2ab+2ac\\ &\qquad +2ad+2bc+2bd+2cd\\ &= 2(a^2+b^2+ab+ac+ad+bc+bd+cd).\end{aligned}$$

Значи, $(a+b+c+d)^2$ је паран број, па је и $a+b+c+d$ паран, дакле сложен.

55. Доказати да су сви бројеви

(1) $10\,001, 100\,010\,001, 1\,000\,100\,010\,001, \ldots$

(2) n^4+4^n, за свако $n\in\mathbb{N}$

сложени.

Решење. (1) Број $10\,001 = 73 \cdot 137$ је сложен.
За $k > 1$, $k-$ти елемент низа се може представити у облику

$$1 + 10^4 + \cdots + 10^{4k}$$

и важи:

$$\begin{aligned} 1 + 10^4 + \cdots + 10^{4k} &= \frac{10^{4k+4} - 1}{10^4 - 1} = \frac{10^{2k+2} - 1}{10^2 - 1} \cdot \frac{10^{2k+2} + 1}{10^2 + 1} \\ &= \frac{(10^{2k} + \cdots + 1)(10^{2k+2} + 1)}{101}. \end{aligned}$$

Број 101 је прост, па он дели бар један од бројева $10^{2k} + \cdots + 1$ и $10^{2k+2} + 1$, који су за $k > 1$ сигурно већи од 101, па је број

$$\frac{(10^{2k} + \cdots + 1)(10^{2k+2} + 1)}{101}$$

сложен.

(2) Разликујемо следеће случајеве:

1. Ако је n паран, тада је $n^4 + 4^n$ такође паран број већи од 2, па је сложен.

2. Ако је $n = 2k + 1$, за неки $k \in \mathbb{Z}$, онда је

$$n^4 + 4^n = n^4 + 4 \cdot 4^{2k} = n^4 + 4 \cdot (2^k)^4,$$

што је на основу идентитета Софи Жермен сложен број.

56. Сваки број облика $3n - 1$ дељив је неким простим бројем облика $3k - 1$. Доказати.

Решење. Сваки прост број осим броја 3 је или облика $3k - 1$ или облика $3k + 1$. Ако дати број облика $3n - 1$ нема ни један прост чинилац облика $3k - 1$, онда су сви његови прости чиниоци облика $3k + 1$. Тада је, због $(3k + 1)(3j + 1) = 3(3kj + k + j) + 1$, производ свих простих чинилаца тог облика такође облика $3m+1$, што није могуће. Дакле, дати број има прост чинилац облика $3k-1$.

57. Доказати да међу 30 узастопних природних бројева, где је најмањи већи од 5, има највише 8 простих.

Решење. Од тих 30 узастопних бројева 15 је парних, 5 оних који су дељиви са 3, а нису дељиви са 2 и још 2 који су дељиви са 5, а нису ни са 2 ни са 3. Према томе, бар $15+5+2=22$ броја су сложена, па простих не може бити више од 8.

58. Дато је 15 природних бројева $1 < n_1, n_2, \ldots, n_{15} \leqslant 2\,003$. Ако је за све $i, j \in \{1, 2, \ldots, 15\}$, $i \neq j$, $(n_i, n_j) = 1$, доказати да је бар један од датих бројева прост.

Решење. Нека је p_i најмањи прост број који дели n_i. Тврђење задатка следи из чињенице да су $p_1, p_2, \ldots, p_{15}$ међусобно различити прости бројеви и да је 15−ти прост број (у низу простих бројева) 47 ($47^2 = 2\,209 > 2\,003$).

59. Доказати да има бесконачно много простих бројева облика $4k-1$, $k \in \mathbb{N}$.

Решење. Претпоставимо да таквих бројева има коначно много; нека су то $3, 7, 11, \ldots, p_n$. Посматрајмо број $P = 4 \cdot (3 \cdot 7 \cdots p_n) - 1$. Број P већи је од свих наведених простих бројева и има облик $4k-1$; дакле, сложен је. Пошто је

$$P + 1 = 4 \cdot (3 \cdot 7 \cdots p_n)$$

и $(P, P+1) = 1$, то је P узајамно прост са свим простим бројевима $3, 7, \ldots, p_n$, а како је P и непаран број, сви његови прости фактори су облика $4k+1$. Но, то је немогуће јер производ два броја облика $4k+1$ има облик

$$(4k_1+1)(4k_2+1) = 4 \cdot (4k_1k_2 + k_1 + k_2) + 1,$$

а P је облика $4k-1$. Контрадикција.

60. Ако су $p_1, p_2, \ldots, p_n$ међусобно различити прости бројеви, доказати да $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n}$ није цео број.

Решење. Број

$$\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_n} = \frac{p_2p_3\cdots p_n + p_1p_3\cdots p_n + \cdots + p_1p_2\cdots p_{n-1}}{p_1p_2\cdots p_n}$$

није цео, јер бројилац последњег разломка није дељив са p_1 (први сабирак у том бројиоцу није дељив са p_1, а сви остали сабирци су дељиви са p_1), а именилац јесте.

61. Наћи све природне бројеве n за које је $\left[\frac{n^3+8n^2+1}{3n}\right]$ прост број.

Решење. Ако је $n = 3k$, онда је

$$\left[\frac{n^3+8n^2+1}{3n}\right] = 3k^2 + 8k = k(3k+8),$$

што је прост број само ако је $k = 1$. Тада је $n = 3$.

Ако је $n = 3k+1$, онда је

$$\left[\frac{n^3+8n^2+1}{3n}\right] = (3k+1)(k+3),$$

што је прост број само за $k = 0$. Тада је $n = 1$.

Коначно, ако је $n = 3k+2$, тада је број

$$\left[\frac{n^3+8n^2+1}{3n}\right] = 3k^2 + 12k + 6 = 3(k^2+4k+2)$$

сложен.

62. Збир два природна броја једнак је $30\,030$. Доказати да њихов производ није дељив са $30\,030$.

Решење. Претпоставимо да је производ природних бројева x и $30\,030 - x$ $(x < 30\,030)$ дељив са $30\,030$, тј. да је $x(30\,030 - x) = 30\,030k$. Тада је $x^2 = 30\,030(x - k)$, тј. број x^2 је дељив са $30\,030$. Тада је x дељиво сваким простим фактором броја $30\,030$. Како је $30\,030 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13$, то је x дељиво са $30\,030$, па је $x \geqslant 30\,030$, што је контрадикција.

63. Одредити најмањи природан број чија је половина потпун квадрат, трећина потпун куб и петина потпун пети степен.

Решење. Тражени број n мора бити дељив са $2, 3$ и 5 и, због минималности, нема других простих фактора. Нека је $n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$. Из услова задатка следи да је:

$$\frac{n}{2} = 2^{\alpha-1} \cdot 3^\beta \cdot 5^\gamma = a^2,$$
$$\frac{n}{3} = 2^{\alpha} \cdot 3^{\beta-1} \cdot 5^\gamma = b^3,$$
$$\frac{n}{5} = 2^{\alpha} \cdot 3^\beta \cdot 5^{\gamma-1} = c^5,$$

где су a, b и c природни бројеви. Тада је α најмањи непаран природан број дељив са 3 и 5, β најмањи природан број дељив са 2 и 5 који при дељењу са 3 даје остатак 1 и γ најмањи природан број дељив са 2 и 3 који при дељењу са 5 даје остатак 1. Према томе, $\alpha = 15$, $\beta = 10$ и $\gamma = 6$. Тада је $n = 2^{15} \cdot 3^{10} \cdot 5^6 = 30\,233\,088\,000\,000$.

64. Доказати да за сваки природан број n постоји скуп од n сложених бројева који образују аритметичку прогресију, при чему су ти бројеви по паровима узајамно прости.

Решење. Ако је $2 \leqslant k \leqslant N$, број $N! + k$ је сложен. За дати природан број n изаберимо прост број p такав да је $p > n$ и цео број

$N \geqslant p + (p-1)n!$. Тада сложени бројеви

$$N! + p,\ N! + p + n!,\ \ldots,\ N! + p + (n-1)n!$$

образују аритметичку прогресију. Ако је q заједнички прост делилац нека два броја горњег низа, онда је и разлика та два броја $jn!$ $(0 < j < n)$ дељива са q. Одатле следи да је $q \leqslant n$. Тада је и $N!$ дељив са q, па према томе и p, што је немогуће. Добијена контрадикција показује да су свака два члана низа узајамно прости бројеви.

65. Ако су $f : \mathbb{N} \to \mathbb{Z}$ и $g : \mathbb{N} \to \mathbb{Z}$ мултипликативне функције, доказати да је и функција $h : \mathbb{N} \to \mathbb{Z}$, дефинисана са $h(n) = f(n) \cdot g(n)$, $n \in \mathbb{N}$, такође мултипликативна.

66. Ако је $f : \mathbb{N} \to \mathbb{Z}$ мултипликативна функција, доказати да је: $f(1) = 1$, као и да је

$$\begin{aligned}\sum_{d|n} f(d) &= \prod_{i=1}^{k} \sum_{j=0}^{\alpha_i} f\left(p_i^j\right) \\ &= \left(1 + f(p_1) + \cdots + f(p_1^{\alpha_1})\right) \cdots \left(1 + f(p_k) + \cdots + f(p_k^{\alpha_k})\right),\end{aligned}$$

при чему је $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ канонска факторизација природног броја n.

Решење. Ако је за неко k, $f(k) \neq 0$ онда је

$$f(k) = f(k \cdot 1) = f(k)f(1),$$

одакле следи да је $f(1) = 1$.

Сви делиоци броја n су облика

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} = \prod_{i=1}^{k} p_i^{\beta_i}, \quad 0 \leqslant \beta_i \leqslant \alpha_i \quad (i = 1, 2, \ldots, k),$$

па је

$$\begin{aligned}
\sum_{d\mid n} f(d) &= \sum_{\substack{(\beta_1,\beta_2,\ldots,\beta_k)\\ 0\leqslant\beta_i\leqslant\alpha_i}} f\left(\prod_{i=1}^{k} p_i^{\beta_i}\right) = \sum_{\substack{(\beta_1,\beta_2,\ldots,\beta_k)\\ 0\leqslant\beta_i\leqslant\alpha_i}} \prod_{i=1}^{k} f\left(p_i^{\beta_i}\right)\\
&= \sum_{\beta_1=0}^{\alpha_1}\sum_{\beta_2=0}^{\alpha_2}\cdots\sum_{\beta_k=0}^{\alpha_k}\prod_{i=1}^{k} f\left(p_i^{\beta_i}\right)\\
&= \left(\sum_{\beta_1=0}^{\alpha_1} f\left(p_1^{\beta_1}\right)\right)\left(\sum_{\beta_2=0}^{\alpha_2} f\left(p_2^{\beta_2}\right)\right)\cdots\left(\sum_{\beta_k=0}^{\alpha_k} f\left(p_k^{\beta_k}\right)\right)\\
&= \prod_{i=1}^{k}\sum_{j=0}^{\alpha_i} f\left(p_i^{j}\right).
\end{aligned}$$

⌜ *Напомена.* Специјално, ако је $f(n) = 1$, тј, $f(n) = n^0$, $n \in \mathbb{N}$, добијамо да је

$$\begin{aligned}
\tau(n) &= \sum_{d\mid n} d^0\\
&= \big(1 + (p_1)^0 + \cdots + (p_1^{\alpha_1})^0\big)\cdots\big(1 + (p_k)^0 + \cdots + (p_k^{\alpha_k})^0\big)\\
&= (\alpha_1 + 1)\cdots(\alpha_k + 1)\,.
\end{aligned}$$

Такође, ако је $f(n) = n$, $n \in \mathbb{N}$, добијамо да је

$$\begin{aligned}
\sigma(n) &= \sum_{d\mid n} d\\
&= (1 + p_1 + \cdots + p_1^{\alpha_1})\cdots(1 + p_k + \cdots + p_k^{\alpha_k})\\
&= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\cdot\ldots\cdot\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.
\end{aligned}$$

⌟

67. Мебијусова функција $\mu : \mathbb{N} \to \mathbb{Z}$ дефинисана је на следећи начин: $\mu(1) = 1$ и

$$\mu(p_1^{\alpha_1} \cdots p_k^{\alpha_k}) = \begin{cases} (-1)^k, & \text{ако је } \alpha_1 = \cdots = \alpha_k = 1 \\ 0, & \text{бар један } \alpha_i \text{ је већи од } 1 \end{cases}$$

при чему су k и α_i природни, а p_i прости бројеви, $i = 1, 2, \ldots, k$, $p_i \neq p_j$, $i \neq j$. (На пример, $\mu(6) = 1$, $\mu(12) = 0$, $\mu(13) = -1$, $\mu(14) = 1$, $\mu(15) = 1$, $\mu(16) = 0$, $\mu(30) = -1, \ldots$)

Доказати:

1) Мебијусова функција је мултипликативна;

2) ако је $f : \mathbb{N} \to \mathbb{N}$ мултипликативна функција, тада важи:

$$\sum_{d|n} f(d)\mu(d) = (1 - f(p_1)) \cdots (1 - f(p_k)),$$

при чему је $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ канонска факторизација природног броја n;

3) $\sum\limits_{d|n} \mu(d) = 0,\ n > 1$;

4) $\sum\limits_{d|n} \dfrac{\mu(d)}{d} = \left(1 - \dfrac{1}{p_1}\right) \cdots \left(1 - \dfrac{1}{p_k}\right)$, $n > 1$ и $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ је канонска факторизација броја n.

68. Доказати да степен простог броја не може бити савршен број.

Решење. Претпоставимо супротно. Нека је p прост број, такав да је број p^α савршен. Тада је $\sigma(p^\alpha) = 2p^\alpha$, па је

$$2p^\alpha = \frac{p^{\alpha+1} - 1}{p - 1}, \quad \text{тј.} \quad 2p^\alpha = p^{\alpha+1} + 1,$$

одакле следи $2 > p$. Контрадикција.

69. Доказати да је природан број n савршен ако је збир реципрочних вредности његових позитивних делилаца једнак 2.

Решење. Услов $\sum_{d|n}\dfrac{1}{d}=2$ еквивалентан је услову $\sum_{d|n}\dfrac{n}{d}=2n$, тј. $\sigma(n)=2n$, па је број n савршен.

70. Показати да постоји бесконачно много природних бројева n таквих да је $\sigma(n)=2n-1$.

Решење. За сваки природан број m важи

$$\sigma(2^m)=2^{m+1}-1=2\cdot 2^m-1,$$

одакле следи тврђење задатка.

71. (Републичко такмичење 1999, IV разред) Нека је $n_1,n_2,n_3,\ldots$ строго растући низ природних бројева, такав да за свако $i\in\mathbb{N}$ важи $\sigma(n_i)-n_i=m$. Одредити m.

Решење. (1) Ако је n прост број, онда је $\sigma(n)-n=n+1-n=1$.

(2) Ако је n сложен број, онда је бар један његов делилац $d\geqslant\sqrt{n}>1$, па је $\sigma(n)-n\geqslant n+\sqrt{n}+1-n>\sqrt{n}$.

Ако су сви бројеви датог низа прости, онда је $m=1$. Ако је у датом низу бар један број сложен, онда су сви сложени због (2). Тада је могуће наћи n_i такав да је $\sigma(n_i)-n_i>\sqrt{n_i}>m$ за свако $m\in\mathbb{N}$. Дакле, мора бити $m=1$.

72. (Сабит ибн–Кора, $836-901$.) За природне бројеве m и n кажемо да су ***пријатељски бројеви*** ако је сваки од њих једнак збиру правих делилаца другог. Доказати следеће тврђење: Ако су $p=3\cdot 2^{k-1}-1$, $q=3\cdot 2^k-1$ и $r=9\cdot 2^{2k-1}-1$ прости бројеви, онда су $A=2^kpq$ и $B=2^kr$ пријатељски бројеви.

Решење. Збир свих позитивних делилаца броја $n=\prod_{i=1}^{k}p_i^{\alpha_i}$ је

$$\sigma(n)=\prod_{i=1}^{k}\sum_{j=0}^{\alpha_i}p_i^j\,.$$

Тако збир делилаца броја A износи

$$\sigma(A) = \left(1 + 2 + \cdots + 2^k\right)(1+p)(1+q) = \left(2^{k+1} - 1\right) \cdot 9 \cdot 2^{2k-1}.$$

Збир свих делилаца броја B је исти:

$$\sigma(B) = \left(1 + 2 + \cdots + 2^k\right)(1+r) = \left(2^{k+1} - 1\right) \cdot 9 \cdot 2^{2k-1}.$$

Такође је

$$\begin{aligned} A + B &= 2^k(pq + r) = 2^k\left(\left(3 \cdot 2^{k-1} - 1\right)\left(3 \cdot 2^k - 1\right) + 9 \cdot 2^{2k-1} - 1\right) \\ &= 2^k\left(9 \cdot 2^{2k} - 9 \cdot 2^{k-1}\right) = 2^{2k-1} \cdot 9 \cdot \left(2^{k+1} - 1\right). \end{aligned}$$

Збир правих делилаца броја A је дакле $\sigma(A) - A = (A+B) - A = B$, а правих делилаца броја B: $\sigma(B) - B = (A+B) - B = A$. Значи A и B су пријатељски бројеви.

73. Доказати да су свака два различита Фермаова броја узајамно проста.

Решење. Нека су f_n и f_{n+k}, $k > 0$ два различита Фермаова броја. Претпоставимо да је m цео позитиван број, такав да $m \mid f_n$ и $m \mid f_{n+k}$. Нека је $x = 2^{2^n}$. Тада је

$$\frac{f_{n+k} - 2}{f_n} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1,$$

па $f_n \mid f_{n+k} - 2$, одакле следи да $m \mid f_{n+k} - 2$. Како $m \mid f_{n+k}$ то $m \mid 2$. Међутим, како су Фермаови бројеви непарни следи да је $m = 1$, одакле следи тврђење задатка.

74. Доказати да Фермаови бројеви задовољавају рекурентну релацију $f_{n+1} = f_0 f_1 f_2 \cdots f_n + 2$.

Решење. Тврђење ћемо доказати индукцијом по n. За $n = 0$ је $f_0 = 3$, а $f_1 = 5$, па тврђење важи. Претпоставимо да тврђење важи за неки природан број n, тј. да је $f_n = f_0 f_1 \cdots f_{n-1} + 2$. Тада је

$$f_n - 2 = 2^{2^n} + 1 - 2 = 2^{2^n} - 1 = f_0 f_1 \cdots f_{n-1},$$

па је

$$\begin{aligned} f_{n+1} - 2 &= 2^{2^{n+1}} - 1 = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) \\ &= f_0 f_1 \cdots f_{n-1} \cdot f_n, \end{aligned}$$

одакле следи тврђење задатка.

⌜ *Напомена.* Коришћењем рекурентне формуле из претходног задатка се лако може показати да су свака два различита Фермаова броја узајамно проста. ⌟

75. Доказати да за $n > 5$ сваки број облика $2^{2^n} - 1$ има прост фактор већи од $1\,000\,000$.

Решење. На основу претходног задатка је

$$2^{2^n} - 1 = f_n - 2 = f_0 f_1 \cdots f_{n-1},$$

па је број $2^{2^n} - 1$ дељив сваким Фермаовим бројем f_i, $0 \leqslant i \leqslant n - 1$. Према томе, број $2^{2^n} - 1$ за $n > 5$ је дељив са $f_5 = 6\,700\,417 \cdot 641$, па садржи прост фактор $6\,700\,417 > 1\,000\,000$.

76. Доказати да за сваки природан број n број $2^{2^n} - 1$ има бар n различитих простих фактора.

Решење. $2^{2^n} - 1$ је производ n различитих Фермаових бројева који су по паровима узајамно прости, одакле следи тврђење задатка.

77. Доказати да је $n = 2^k$ ако је $2^n + 1$ прост број.

Решење. Претпоставимо супротно, тј. да је $n = 2^k \cdot m$, где је m непаран број већи од 1. Тада је

$$2^n + 1 = 2^{2^k \cdot m} + 1 = \left(2^{2^k}\right)^m + 1,$$

па како важи $x + y \mid x^m + y^m$ за непарно m, то и

$$2^{2^k} + 1 \mid 2^n + 1,$$

па је број $2^n + 1$ сложен. Контрадикција.

⌜ *Напомена.* Из претходног задатка следи да број облика $2^n + 1$ може бити прост само ако је он Фермаов број. ⌟

78. Доказати да за свако $n \in \mathbb{N}$, број $2^{2^n} + 2^{2^{n-1}} + 1$ има најмање n различитих простих фактора.

Решење. Доказаћемо тврђење индукцијом по n.
За $n = 1$ је $2^{2^1} + 2^{2^0} + 1 = 7$.
За сваки релан број x важи једнакост

$$x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1),$$

па је специјално и

$$2^{2^{n+1}} + 2^{2^n} + 1 = \left(2^{2^n} - 2^{2^{n-1}} + 1\right)\left(2^{2^n} + 2^{2^{n-1}} + 1\right).$$

Даље, имамо да је $\left(2^{2^n} - 2^{2^{n-1}} + 1, 2^{2^n} + 2^{2^{n-1}} + 1\right) = 1$, јер ако би ови бројеви имали заједнички прост фактор $p > 2$ $(p \neq 2$ јер су бројеви непарни), онда би било

$$p \mid \left(2^{2^n} + 2^{2^{n-1}} + 1\right) - \left(2^{2^n} - 2^{2^{n-1}} + 1\right) = 2 \cdot 2^{2^{n-1}},$$

што је немогуће (p је непаран прост број).

Дакле, по претпоставци, ако $2^{2^n} + 2^{2^{n-1}} + 1$ има најмање n различитих простих делилаца, онда $2^{2^{n+1}} + 2^{2^n} + 1$ има најмање $n + 1$ различитих простих делилаца.

79. Из скупа $\{1, 2, \ldots, 2n\}$ на произвољан начин изабран је $n + 1$ број. Доказати да међу изабраним бројевима увек постоји број дељив неким другим од изабраних бројева.

Решење. Нека су $a_1, a_2, \ldots, a_{n+1}$ произвољни бројеви из скупа $\{1, 2, \ldots, 2n\}$. Сваки од њих се може записати у облику $a_i = 2^{k_i} b_i$, где је b_i непаран. Тада су $b_1, b_2, \ldots, b_{n+1}$ непарни бројеви из интервала $[1, 2n-1]$, а како у интервалу $[1, 2n-1]$ постоји само n непарних бројева, два су једнака, тј. за неке $i, j \in \{1, \ldots, n-1\}$, $i \neq j$ је $b_i = b_j$, па један од бројева a_i, a_j дели други.

80. Доказати да за природне бројеве a, b и c важи:

$$abc = [a, b, c] \cdot (ab, bc, ca).$$

Решење. Нека је

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad c = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$$

(неки од бројева α_i, β_i, γ_i могу бити и једнаки нули). Тада је:

$$[a, b, c] = p_1^{\max\{\alpha_1, \beta_1, \gamma_1\}} \cdots p_k^{\max\{\alpha_k, \beta_k, \gamma_k\}},$$

и

$$(ab, bc, ca) = p_1^{\min\{\alpha_1+\beta_1, \beta_1+\gamma_1, \gamma_1+\alpha_1\}} \cdots p_k^{\min\{\alpha_k+\beta_k, \beta_k+\gamma_k, \gamma_k+\alpha_k\}}.$$

Пошто је

$$\max\{\alpha_i, \beta_i, \gamma_i\} + \min\{\alpha_i+\beta_i, \beta_i+\gamma_i, \gamma_i+\alpha_i\} = \alpha_i+\beta_i+\gamma_i \qquad (i = \overline{1, k})$$

(ако је, нпр. γ_i највећи, најмањи збир је $\alpha_i + \beta_i$), тврђење непосредно следи.

81. Доказати да за природне бројеве a, b и c важи:
(1) $(a, [b, c]) = [(a, b), (a, c)]$;
(2) $[a, (b, c)] = ([a, b], [a, c])$;
(3) $[a, b, c](a, b)(b, c)(c, a) = abc(a, b, c)$;

(4) $[a, b, c](a, b)([a, b], c) = abc.$

82. (ИМО 1997) Наћи све парове (a, b) природних бројева који задовољавају једначину $a^{b^2} = b^a$.

Решење. Нека је (a, b) решење дате једначине и нека су

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n} \quad \text{и} \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}$$

канонске факторизације бројева a и b, при чему је, због једначине коју ти бројеви задовољавају, јасно да мора бити $\alpha_i > 0$ и $\beta_i > 0$ за све $i \in \{1, 2, \dots, n\}$. Заменом у једначину добијамо

$$p_1^{\alpha_1 b^2} p_2^{\alpha_2 b^2} \cdots p_n^{\alpha_n b^2} = p_1^{\beta_1 a} p_2^{\beta_2 a} \cdots p_n^{\beta_n a}$$

одакле следи да за свако i важи $\alpha_i b^2 = \beta_i a$, односно $\dfrac{\alpha_i}{\beta_i} = \dfrac{a}{b^2} = r$ за неки рационалан број r. Одатле је

$$a = p_1^{\beta_1 r} p_2^{\beta_2 r} \cdots p_n^{\beta_n r} = b^r.$$

Замењујући поново у дату једначину добијамо

$$(b^r)^{b^2} = b^{b^r},$$

одакле је $rb^2 = b^r$, односно $r = b^{r-2}$.

Како рационалан степен природног броја b може бити једнак рационалном броју r само ако је r такође природан број, то следи да је $r \in \mathbb{N}$. Како је за $r \geqslant 5$, $r < 2^{r-2} \leqslant b^{r-2}$ (ово се може показати индукцијом), то остају могућности $r \in \{1, 2, 3, 4\}$. Разматрањем тих могућности добијамо три решења дате једначине: $(1, 1)$, $(27, 3)$ и $(16, 2)$.

83. Доказати да је изложилац са којим дати прост број p фигурише у канонској факторизацији броја $n!$ једнак

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots .$$

Решење. Сума је коначна јер за сваки $n \in \mathbb{N}$ и прост број p постоји природан број m такав да је $p^m \leqslant n$ и $p^{m+1} > n$.

Међу бројевима $1, 2, \ldots, n$ има $\left[\dfrac{n}{p}\right]$ бројева дељивих са p, $\left[\dfrac{n}{p^2}\right]$ дељивих са p^2, $\left[\dfrac{n}{p^3}\right]$ дељивих са p^3,. . . .

84. Са колико нула се завршава број 100! ?

Решење: $\left[\dfrac{100}{5}\right] + \left[\dfrac{100}{25}\right] + \left[\dfrac{100}{125}\right] + \cdots = 20 + 4 + 0 + \cdots = 24.$

85. Да ли постоји природан број n такав да се $n!$ завршава са 11 нула?

Решење. За $n \leqslant 49$ број $n!$ се завршава са мање од 11 нула; 50! се завршава са 12 нула; а за $n \geqslant 50$ са 12 или више нула. Не постоји број n такав да се $n!$ завршава са 11 нула.

86. Доказати да је

$$\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{m!} = \frac{n!}{m!(n-m)!}, \quad m < n,$$

цео број.

Решење. Довољно је доказати да за сваки прост број p и сваки природан број k важи неједнакост

$$\left[\frac{n}{p^k}\right] - \left(\left[\frac{m}{p^k}\right] + \left[\frac{n-m}{p^k}\right]\right) \geqslant 0$$

(видети теорему 1.1. (5)).

87. (ИМО 1972) Доказати да је за свака два ненегативна цела броја m и n број

$$\frac{(2m)!(2n)!}{m!n!(m+n)!}$$

цео.

Решење. Нека је p произвољан прост број и нека је k природан број такав да је $p^{k+1} > 2m$ и $p^{k+1} > 2n$. Тада је $p^{k+1} > m+n$. Према задатку 83, ако је α највећи природан број такав да $p^\alpha \mid (2m)!(2n)!$ тада је

$$\alpha = \left[\frac{2m}{p}\right] + \left[\frac{2m}{p^2}\right] + \cdots + \left[\frac{2m}{p^k}\right] + \left[\frac{2n}{p}\right] + \left[\frac{2n}{p^2}\right] + \cdots + \left[\frac{2n}{p^k}\right].$$

Такође, према задатку 83, ако је β највећи природан број такав да $p^\beta \mid m!n!(m+n)!$ тада је

$$\beta = \left[\frac{m}{p}\right] + \left[\frac{m}{p^2}\right] + \cdots + \left[\frac{m}{p^k}\right] + \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots + \left[\frac{n}{p^k}\right] + \\ + \left[\frac{m+n}{p}\right] + \left[\frac{m+n}{p^2}\right] + \cdots + \left[\frac{m+n}{p^k}\right].$$

Пошто за све ненегативне бројеве x и y важи неједнакост (видети теорему 1.1. (10))

$$[2x] + [2y] \geqslant [x] + [y] + [x+y],$$

стављајући да је $x = \dfrac{m}{p^i}$ и $y = \dfrac{n}{p^i}$, $i = 1, \ldots, k$ имамо да је

$$\left[\frac{2m}{p^i}\right] + \left[\frac{2n}{p^i}\right] \geqslant \left[\frac{m}{p^i}\right] + \left[\frac{n}{p^i}\right] + \left[\frac{m+n}{p^i}\right],$$

па је $\alpha \geqslant \beta$, одакле директно следи тврђење задатка.

88. (ИМО 1967) Нека су k, m и n природни бројеви, $m+k+1$ прост број већи од $n+1$. Нека је $C_s = s(s+1)$. Доказати да је производ $(C_{m+1} - C_k)(C_{m+2} - C_k) \cdots (C_{m+n} - C_k)$ дељив производом $C_1 C_2 \cdots C_n$.

Решење. Према дефиницији C_s лако добијамо

$$(*) \qquad C_p - C_q = p^2 + p - (q^2 + q) = (p - q)(p + q + 1).$$

Користећи $(*)$ добијамо:

$$\begin{aligned} A &= (C_{m+1} - C_k)(C_{m+2} - C_k) \cdots (C_{m+n} - C_k) \\ &= (m + 1 - k)(m + 1 + k + 1)(m + 2 - k) \\ &\quad \times (m + 2 + k + 1) \cdots (m + n - k)(m + n + k + 1) \\ &= [(m - k + 1)(m - k + 2) \cdots (m - k + n)] \\ &\quad \times [(m + k + 2)(m + k + 3) \cdots (m + k + n + 1)] \end{aligned}$$

Такође:

$$\begin{aligned} B &= C_1 C_2 \cdots C_n \\ &= 1 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 4 \cdot \ldots \cdot n \cdot (n + 1) = n!(n + 1)!. \end{aligned}$$

Треба показати да је $\dfrac{A}{B}$ цео број.

$$\begin{aligned} \frac{A}{B} &= \frac{(m - k + 1) \cdots (m - k + n)}{n!} \cdot \frac{(m + k + 2) \cdots (m + k + n + 1)}{(n + 1)!} \\ &= \binom{m - k + n}{n} \cdot \binom{m + k + n + 1}{n + 1} \cdot \frac{1}{m + k + 1}\,. \end{aligned}$$

Први биномни коефицијент $\dbinom{m - k + n}{n}$ је цео број (могућност $m - k + n \leqslant 0$ не мења ништа битно јер је производ n узастопних целих бројева увек дељив са $n!$ без обзира на знак). Производ $\dbinom{m + k + n + 1}{n + 1} \cdot \dfrac{1}{m + k + 1}$ је такође цео број јер је биномни коефицијент $\dbinom{m + k + n + 1}{n + 1}$ дељив са $m + k + 1$ зато што је $m + k + 1$

прост број већи од $n+1$ па према томе и узајамно прост са $(n+1)!$. Према томе, количник $\dfrac{A}{B}$ је цео број.

89. Доказати да за сваки природан број n важи $n!^{(n-1)!} \mid (n!)!$.

90. Ако су $d_1, d_2, \ldots, d_m$ сви позитивни делиоци броја $n \in \mathbb{N}$ (укључујући 1 и само n), доказати да је $d_1^2 \cdot d_2^2 \cdot \ldots \cdot d_m^2 = n^m$.

Решење. Ако су $d_1, d_2, \ldots, d_m$ сви позитивни делиоци броја $n \in \mathbb{N}$ (укључујући 1 и само n), онда су то и $\dfrac{n}{d_1}, \dfrac{n}{d_2}, \ldots, \dfrac{n}{d_m}$ (реч је заправо само о једној пермутацији низа делилаца). Дакле,

$$d_1^2 \cdot d_2^2 \cdot \ldots \cdot d_m^2 = d_1 \cdot d_2 \cdot \ldots \cdot d_m \cdot \frac{n}{d_1} \cdot \frac{n}{d_2} \cdot \ldots \cdot \frac{n}{d_m} = n^m.$$

91. (ИМО 2002) Нека је n природан број већи од 1. Нека су $d_1, d_2, \ldots, d_k$ сви позитивни делиоци броја n, при чему је

$$1 = d_1 < d_2 < \cdots < d_k = n.$$

Означимо: $D = d_1d_2 + d_2d_3 + \cdots + d_{k-1}d_k$.

(а) Доказати да је $D < n^2$.

(б) Одредити све n за које је D делилац од n^2.

Решење. (а) Приметимо да ако је d делилац од n, онда је то и $\dfrac{n}{d}$. Зато је

$$D = \sum_{1 \leqslant i < k} d_i d_{i+1} = n^2 \sum_{1 \leqslant i < k} \frac{1}{d_i d_{i+1}} \leqslant n^2 \sum_{1 \leqslant i < k} \left(\frac{1}{d_i} - \frac{1}{d_{i+1}} \right) < \frac{n^2}{d_1} = n^2.$$

(б) Нека је p најмањи прост делилац од n. Како је $D < n^2$, ако D дели n^2 мора D да буде мање или једнако са $\dfrac{n^2}{p}$. Сада је:

$$d_k = n,\ d_{k-1} = \frac{n}{p},\ \ldots,\ d_2 = p,\ d_1 = 1.$$

Тада је, за $k \neq 2$, $D > d_{k-1}d_k = \dfrac{n}{p} \cdot n = \dfrac{n^2}{p}$, што је немогуће. Дакле, $D = d_{k-1}d_k$, $k = 2$, па је $n = p$.

Обрнуто је такође тачно. Дакле, D дели n^2 ако и само ако је n прост број.

92. (а) Одредити најмањи природан број који има тачно четири делиоца.

(б) Одредити најмањи природан број који је дељив са 30 и има тачно 12 делилаца.

Решење. (а) Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ канонска факторизација броја n тада је $\tau(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$. Да бисмо одредили n треба одредити:

- k – број међусобно различитих простих делилаца од n,
- $p_1, p_2, \dots, p_k$ – просте чиниоце броја n,
- $\alpha_1, \alpha_2, \dots, \alpha_k$,

тако да је $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ најмањи број са особином:

$$(\alpha_1 + 1)(\alpha_2 + 1)\dots(\alpha_k + 1) = 4.$$

Пошто је $\alpha_i + 1 \geqslant 2$, $i = 1, 2 \dots, k$ и $4 = 2 \cdot 2$ следи да је $k = 2$, тј. да n има само два проста фактора и при томе је

$$\alpha_1 + 1 = 2 \quad \text{и} \quad \alpha_2 + 1 = 2,$$

тј.

$$\alpha_1 = 1 \quad \text{и} \quad \alpha_2 = 1.$$

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 $30 \mid n$, следи да $2 \mid n$, $3 \mid n$ и $5 \mid n$. Тада је

$$n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma \dots \qquad (\alpha, \beta, \gamma \geqslant 1),$$

па је

$$\tau(n) = (\alpha+1)(\beta+1)(\gamma+1)(\dots) = 12 = 2 \cdot 2 \cdot 3,$$

одакле се види да број n других (осим 2, 3 и 5) простих делилаца нема, тј. да је $n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$, као и да је, због услова минималности броја n,

$$\alpha + 1 = 3, \quad \beta + 1 = 2, \quad \gamma + 1 = 2.$$

Дакле, тражени број је $n = 2^2 \cdot 3 \cdot 5 = 60$.

93. Колико делилаца има број 10! ?

Решење. Како је $10! = 2^8 \cdot 3^4 \cdot 5^2 \cdot 7$ то је

$$\tau(10!) = (8+1)(4+1)(2+1)(1+1) = 270.$$

94. Наћи a ако $3 \mid a$, $4 \mid a$ и $\tau(a) = 14$.

Решење. Из датих услова следи $a = 2^{\alpha_1} \cdot 3^{\alpha_2}$, при чему је $\alpha_1 \geqslant 2$. Како је $\tau(a) = (\alpha_1+1)(\alpha_2+1) = 14$, због $\alpha_1 \geqslant 2$, је $\alpha_1 + 1 = 7$ и $\alpha_2 + 1 = 2$, одакле је $\alpha_1 = 6$ и $\alpha_2 = 1$, па је $a = 2^6 \cdot 3 = 192$.

95. Природан број n има непаран број делилаца ако и само ако је n потпун квадрат. Доказати.

Решење. Нека је n природан број са канонском факторизацијом $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ (за неке просте бројеве p_1, $p_2, \dots, p_k$ и неке природне бројеве $\alpha_1, \alpha_2, \dots, \alpha_k$). Укупан број (природних) делилаца броја n (укључујући 1 и само n) је $\tau(n) = (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1)$.

$$\begin{aligned}
\tau(n) \text{ је непаран број} &\Leftrightarrow (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) \text{ је непаран број}\\
&\Leftrightarrow \alpha_1+1, \alpha_2+1, \dots, \alpha_k+1 \text{ су непарни бројеви}\\
&\Leftrightarrow \alpha_1, \alpha_2, \dots, \alpha_k \ \text{ су парни бројеви}\\
&\Leftrightarrow p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \ \text{ је потпун квадрат}\\
&\Leftrightarrow n \ \text{ је потпун квадрат.}
\end{aligned}$$

96. (Републичко такмичење 1994, I разред) Колико највише делилаца може да има природан број мањи од 1 994?

Решење. Број делилаца природног броја чија је канонска факторизација $p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ је $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_m+1)$. Како је $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 > 1\,994$, то у канонској факторизацији природног броја који није већи од 1 994 могу да учествују највише четири проста броја. Довољно је одредити број делилаца следећих бројева: 2^{10}, $2^9 \cdot 3$, $2^8 \cdot 3$, $2^7 \cdot 3^2$, $2^7 \cdot 3 \cdot 5$, $2^6 \cdot 3^3$, $2^6 \cdot 3 \cdot 5$, $2^5 \cdot 3^3$, $2^5 \cdot 3^2 \cdot 5$, $2^4 \cdot 3^4$, $2^4 \cdot 3^2 \cdot 5$, $2^4 \cdot 3 \cdot 5 \cdot 7$ и $2^2 \cdot 3^2 \cdot 5 \cdot 7$. Највећи број делилаца међу њима има број $2^4 \cdot 3 \cdot 5 \cdot 7 = 1\,680$ и тај број делилаца једнак је $5 \cdot 2 \cdot 2 \cdot 2 = 40$.

97. Природан број n има два проста делиоца, а број n^2 има укупно 15 делилаца. Колико делилаца има број n^3?

Решење. По условима задатка је $n = p^\alpha q^\beta$, где су p и q прости бројеви, $n^2 = p^{2\alpha} q^{2\beta}$ и $(2\alpha+1)(2\beta+1) = 15$. Следи да је $2\alpha+1 = 3$ и $2\beta+1 = 5$, тј. $\alpha = 1$ и $\beta = 2$. Сада се лако добија

$$\tau(n^3) = (3\alpha+1)(3\beta+1) = 4 \cdot 7 = 28.$$

98. Природан број n има само три проста делиоца: 2, 3 и 5. Одредити број n ако је:

$$\tau\left(\frac{n}{2}\right) = \tau(n) - 30, \quad \tau\left(\frac{n}{3}\right) = \tau(n) - 35 \quad \text{и} \quad \tau\left(\frac{n}{5}\right) = \tau(n) - 42.$$

Решење. Нека је $n = 2^x \cdot 3^y \cdot 5^z$. Тада је:

$$\tau\left(\frac{n}{2}\right) = x(y+1)(z+1)$$
$$\tau\left(\frac{n}{3}\right) = (x+1)y(z+1)$$
$$\tau\left(\frac{n}{5}\right) = (x+1)(y+1)z,$$

па је:

$$\begin{aligned}\tau(n) = (x+1)(y+1)(z+1) &= x(y+1)(z+1) + 30\\ &= (x+1)y(z+1) + 35\\ &= (x+1)(y+1)z + 42,\end{aligned}$$

одакле добијамо систем једначина:

$$\begin{aligned}(y+1)(z+1) &= 30\\ (x+1)(z+1) &= 35\\ (x+1)(y+1) &= 42.\end{aligned}$$

Решење овог система је $x = 6$, $y = 5$, $z = 4$, па је $n = 9\,720\,000$.

99. Одредити најмањи природан број који је тачно 100 пута већи од броја својих делилаца, укључујући 1 и сам тај број.

Решење. Према услову задатка имамо да је

$$n = 2^{\alpha_1} 5^{\alpha_2} p_3^{\alpha_3} \dots p_k^{\alpha_k} = 2^2 5^2 (\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) = 100\tau(n).$$

(1) Ако су 2 и 5 једини прости делиоци броја n имамо да је

$$2^{\alpha_1} 5^{\alpha_2} = 2^2 5^2 (\alpha_1+1)(\alpha_2+1),$$

па је очигледно $\alpha_1 \geqslant 2$ и $\alpha_2 \geqslant 2$. Ниједан од ових бројева не може бити 2, јер би тада десна страна била дељива са 3, а лева не. Дакле,

$\alpha_1 \geqslant 3$ и $\alpha_2 \geqslant 3$. За $\alpha_2 = 3$ имамо решење $\alpha_1 = 4$, тј. $n = 2\,000$, што је очигледно најмање решење у овом случају.

(2) Нека сада n има и простих делилаца различитих од 2 и 5. Треба утврдити може ли бити $(\alpha_1+1)(\alpha_2+1)\dots(\alpha_k+1) < 20$. Ако је $\alpha_1 > 2$ или $\alpha_2 > 2$, неједнакост не може бити испуњена јер је број с леве стране тада бар $4\cdot 3\cdot 2 = 24$. Значи, остаје могућност $\alpha_1 = \alpha_2 = 2$ и $\alpha_3 = 1$, па добијамо да је $2^2 5^2 p_3 = 100\cdot 3\cdot 3\cdot 2$, што је немогуће јер је десна страна дељива са 9, а лева није.

Значи тражени број је 2 000.

100. (ИМО 1998) Одредити све природне бројеве k такве да за неко n важи $\dfrac{\tau(n^2)}{\tau(n)} = k$.

Решење. Ако је $n = p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ канонска факторизација броја n, онда је

$$\tau(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_s+1)$$

и

$$\tau(n^2) = (2\alpha_1+1)(2\alpha_2+1)\cdots(2\alpha_s+1),$$

па је

$$\frac{\tau(n^2)}{\tau(n)} = \frac{2\alpha_1+1}{\alpha_1+1}\cdot\frac{2\alpha_2+1}{\alpha_2+1}\cdot\ldots\cdot\frac{2\alpha_s+1}{\alpha_s+1}\,.$$

Ако је овај количник природан број, он је очигледно непаран.

Докажимо обрнуто, да за сваки непаран природан број k постоји природан број n такав да је $k = \dfrac{\tau(n^2)}{\tau(n)}$.То ћемо доказати трансфинитном индукцијом по k.

За $k = 1$ тврђење је тачно: $1 = \dfrac{\tau(1^2)}{\tau(1)}$.

Претпоставимо да тврђење важи за све непарне природне бројеве мање од неког непарног броја k и докажимо да је тачно и за k.

Број $k+1$ је паран, те га можемо написати у облику $k+1 = 2^m k_0$, при чему је k_0 непаран број. Пошто је очигледно $k_0 < k$, према индукцијској претпоставци постоји природан број n_0 такав да је $k_0 = \dfrac{\tau(n_0^2)}{\tau(n_0)}$. Изаберимо међусобно различите просте бројеве $p_0, p_1, \dots, p_{m-1}$ који су узајамно прости са n_0 и нека је (за сада) α произвољан природан број. Ако је

$$n = p_0^{\alpha} p_1^{2\alpha} \cdots p_{m-1}^{2^{m-1}\alpha} \cdot n_0,$$

с обзиром на то да је функција τ мултипликативна, добијамо

$$\frac{\tau(n^2)}{\tau(n)} = \frac{2\alpha+1}{\alpha+1} \cdot \frac{2^2\alpha+1}{2\alpha+1} \cdot \ldots \cdot \frac{2^m\alpha+1}{2^{m-1}\alpha+1} \cdot \frac{\tau(n_0^2)}{\tau(n_0)} = \frac{2^m\alpha+1}{\alpha+1} \cdot k_0.$$

Ако ставимо да је $\alpha = (2^m-1)k_0 - 1$, имаћемо

$$\frac{\tau(n^2)}{\tau(n)} = \frac{2^m\alpha+1}{2^m-1} = \frac{2^m(\alpha+1)}{2^m-1} - 1 = 2^m k_0 - 1 = k,$$

чиме је доказ завршен.

101. (Дирихле) Доказати једнакост

$$\tau(1) + \tau(2) + \cdots + \tau(n) = \left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{n}\right].$$

Решење. Приметимо најпре да је

$$\left[\frac{n+1}{k}\right] = \begin{cases} \left[\dfrac{n}{k}\right], & k \nmid n+1 \\[2ex] \left[\dfrac{n}{k}\right] + 1, & k \mid n+1\,. \end{cases}$$

Заиста, ако је $n+1 = qk + r$ и $1 \leqslant r \leqslant k-1$, тада је

$$n = qk + r - 1 \quad \text{и} \quad \left[\frac{n+1}{k}\right] = \left[\frac{n}{k}\right] = q.$$

Ако је $n+1=qk$, онда је $\left[\dfrac{n+1}{k}\right]=q$ и $\left[\dfrac{n}{k}\right]=q-1$.

Дакле, имамо да је

$$\left[\frac{n+1}{1}\right]+\left[\frac{n+1}{2}\right]+\cdots+\left[\frac{n+1}{n+1}\right]=\left[\frac{n}{1}\right]+\left[\frac{n}{2}\right]+\cdots+\left[\frac{n}{n}\right]+\tau(n+1).$$

Ако је

$$\left[\frac{n}{1}\right]+\left[\frac{n}{2}\right]+\cdots+\left[\frac{n}{n}\right]=\tau(1)+\tau(2)+\cdots+\tau(n),$$

онда је

$$\left[\frac{n+1}{1}\right]+\left[\frac{n+1}{2}\right]+\cdots+\left[\frac{n+1}{n+1}\right]=\tau(1)+\tau(2)+\cdots+\tau(n)+\tau(n+1),$$

па тврђење важи на основу принципа математичке индукције, јер тврђење очигледно важи за $n=1$.

102. Нека је p_n n-ти прост број. Доказати да за сваки природан број $n>4$ важи неједнакост $p_n>2n$.

Решење. За $n=5$ тврђење важи јер је $p_5=11>10$. Ако је $p_n>2n$, онда је $p_{n+1}\geqslant p_n+2>2n+2=2(n+1)$. Дакле, за свако $n>4$ је $p_n>2n$.

103. (Савезно такмичење 1984, II разред) Нека је p_n n-ти прост број ($p_1=2, p_2=3, p_3=5, \dots$) и нека је $\pi(n)$ број простих бројева који нису већи од n. Ако је

$$A=\{n+p_n \mid n\in\mathbb{N}\} \quad \text{и} \quad B=\{n+\pi(n)+1 \mid n\in\mathbb{N}\},$$

тада је $A\cap B=\emptyset$, $A\cup B=\mathbb{N}\setminus\{1\}$. Доказати.

Решење. Функција π има следећа својства:

(1) $\pi(p_k)=k$ за свако $k\in\mathbb{N}$,

(2) $\pi(n) \leqslant \pi(n+1)$ за свако $n \in \mathbb{N}$,
(3) $\pi(n) < \pi(n+1)$ ако и само ако је $n+1$ прост број.

Претпоставимо супротно, тј. да је $A \cap B \neq \emptyset$, односно да за неке природне бројеве m и n важи

$$m + p_m = n + \pi(n) + 1. \tag{$*$}$$

Размотрићемо две могућности: $p_m \leqslant n$ и $p_m > n$.

Ако би било $p_m \leqslant n$, тада би из те релације и из

$$m = \pi(p_m) \leqslant \pi(n)$$

следило
$$m + p_m \leqslant n + \pi(n) < n + \pi(n) + 1,$$
што је супротно са $(*)$.

Како је у случају $p_m > n$, $m = \pi(p_m) > \pi(n)$ то је $m \geqslant \pi(n) + 1$ и $m + p_m > n + \pi(n) + 1$, што поново противуречи претпоставци $(*)$.

Тиме је доказано да је $A \cap B = \emptyset$.

Докажимо сада да је $A \cup B = \mathbb{N} \setminus \{1\}$. Јасно је да $1 \notin A \cup B$ и да $2 \in B$. Нека је $n > 2$ произвољан природан број који не припада скупу A. Докажимо да тада $n \in B$. Нека за неко $m \in \mathbb{N}$ важи

$$m + p_m < n < m + 1 + p_{m+1},$$

тј.
$$p_m \leqslant n - m - 1 < p_{m+1}.$$
Тада је $\pi(n - m - 1) = m$, па следи
$$n = \pi(n - m - 1) + (n - m - 1) + 1 \in B.$$

104. (Савезно такмичење 1988, I разред) Доказати да је природан број $n > 1$ прост ако и само ако важи

$$\left[\frac{n}{1}\right] + \left[\frac{n}{2}\right] + \cdots + \left[\frac{n}{n}\right] = 2 + \left[\frac{n-1}{1}\right] + \left[\frac{n-1}{2}\right] + \cdots + \left[\frac{n-1}{n-1}\right].$$

Решење. Како је $\left[\frac{n}{1}\right]=n$, $\left[\frac{n}{n}\right]=1$ и $\left[\frac{n-1}{1}\right]=n-1$ то из дате једнакости следи

$$\left[\frac{n}{2}\right]+\cdots+\left[\frac{n}{n-1}\right]=\left[\frac{n-1}{2}\right]+\cdots+\left[\frac{n-1}{n-1}\right].$$

С обзиром на то да за свако $k\in\{2,3,\ldots,n-1\}$ важи $\left[\frac{n}{k}\right]\geqslant\left[\frac{n-1}{k}\right]$, то због претходне једнакости за све k важи $\left[\frac{n}{k}\right]=\left[\frac{n-1}{k}\right]$. Ако би n био сложен број, онда би за неко $k\in\{2,3,\ldots,n-1\}$ број $\frac{n}{k}$ био цео, па би важило

$$\frac{n}{k}=\left[\frac{n}{k}\right]=\left[\frac{n-1}{k}\right]\leqslant\frac{n-1}{k}.$$

Дакле, n мора бити прост број.

105. (Савезно такмичење 1970, IV разред) Ако је p прост број, доказати да је $\frac{(2p)!}{(p!)^2}-2$ дељиво са p^2.

Решење. За свако реално x важи

$$(1+x)^p(1+x)^p=(1+x)^{2p}.$$

Ако развијемо ове изразе по биномној формули и изједначимо коефицијенте уз x^p добијамо

$$1+\binom{p}{1}\binom{p}{p-1}+\binom{p}{2}\binom{p}{p-2}+\cdots+\binom{p}{p-1}\binom{p}{1}+1=\binom{2p}{p},$$

односно

$$N=\frac{(2p)!}{(p!)^2}-2=\binom{2p}{p}-2=\sum_{i=1}^{p-1}\binom{p}{i}^2.$$

Како је p прост број, то је сваки од бројева
$$\binom{p}{i} = \frac{p(p-1)\cdots(p-i+1)}{i!}$$
дељив са p, па је последњи збир, а са њим и број N, дељив са p^2.

⌜ *Напомена.* $\binom{n}{k} = \binom{n}{n-k}$ и $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$. ⌟

106. (Мала олимпијада 1979) Нађи све природне бројеве $n < 1\,979$ који задовољавају следећи услов: ако је m природан број, $1 < m < n$ и $(m, n) = 1$, онда је m прост број.

Решење. Нека је S скуп свих природних бројева за које важе наведени услови. Ако је $n \in S$ и $p^2 < n$, где 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 $n \geqslant 2 \cdot 3 \cdot 5 \cdot 7 = 210 > 11^2$, па и $11 \mid n$. Даље следи $n \geqslant 210 \cdot 11 = 2\,310 > 1\,979$, 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 дељив са $2 \cdot 3 \cdot 5 = 30$. Такав број је само 30.

(б) Нека је $9 < n \leqslant 25$. Тада $n \in S$ ако и само ако је n дељиво са $2 \cdot 3 = 6$. То важи за бројеве $12, 18, 24$.

(в) Нека је $4 < n \leqslant 9$. Тада $n \in S$ ако и само ако је n паран број. Дакле, $6 \in S$, $8 \in S$.

(г) Лако се проверава да сваки од бројева $2, 3, 4$ припада скупу S.

Према томе, $S = \{2, 3, 4, 6, 8, 12, 18, 24, 30\}$.

107. (Пролећно математичко такмичење, Бугарска 2002, 8. разред) Нађи све природне бројеве који имају тачно 16 делилаца (укључујући 1 и сам тај број) тако да је збир свих делилаца једнак $4\,032$.

Решење: $4\,032 = 2^6 \cdot 3^2 \cdot 7$. Ако број има тачно 16 делилаца, онда он има једну од следећих факторизација: p^{15}, p^7q, p^3q^3, p^3qr, $pqrs$, где су p, q, r и s различити прости бројеви. Збир свих делилаца (који је једнак $4\,032 = 2^6 \cdot 3^2 \cdot 7$) у сваком од ових случајева је:

$$
\begin{aligned}
&1 + p + p^2 \cdots + p^{15} = (1+p)(1+p^2)(1+p^4)(1+p^8);\\
&(1 + p + p^2 \cdots + p^7)(1+q) = (1+p)(1+p^2)(1+p^4)(1+q);\\
&(1 + p + p^2 + p^3)(1 + q + q^2 + q^3) = (1+p)(1+p^2)(1+q)(1+q^2);\\
&(1 + p + p^2 + p^3)(1+q)(1+r) = (1+p)(1+p^2)(1+q)(1+r);\\
&(1+p)(1+q)(1+r)(1+s).
\end{aligned}
$$

Фактор $1 + p^2$ јавља се у прва четири случаја. Пошто број тог облика није дељив са $3, 4$ или 7 ови случајеви не воде решењу. Не умањујући општост, можемо претпоставити да важи $p < q < r < s$. Запишимо у врсти редом просте бројеве:

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, \ldots .$$

Тада број $4\,032$ 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 две могућности: $2 \cdot 3 \cdot 7 \cdot 41 = 1\,722$ и $2 \cdot 3 \cdot 13 \cdot 23 = 1\,794$. 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 $2 \cdot 7 \cdot 11 \cdot 13 = 2\,002$.

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 $3 \cdot 5 \cdot 11 \cdot 13 = 2\,145$. Ако је $1 + q \geqslant 8$, тада је $(1+q)(1+r)(1+s) \geqslant 8 \cdot 12 \cdot 14 > 2^4 \cdot 3^2 \cdot 7$, што значи да у том 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: $1\,722$, $1\,794$, $2\,002$ и $2\,145$.

108. (ЈБМО 2002) Наћи све природне бројеве N који имају следеће особине:

- N има тачно 16 делилаца $1 = d_1 < d_2 < \cdots < d_{15} < d_{16} = N$;
- делилац са индексом d_5 (то јест d_{d_5}) једнак је $(d_2 + d_4)d_6$.

Решење. Приметимо најпре да N не може имати више од четири проста делиоца и да је $d_2 = 2$. Ако би N имао више од четири проста делиоца, онда би укупан број делилаца био најмање $2^5 = 32$. (Број $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ има $(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ делилаца.) d_2 и d_4 су делиоци броја N, $d_2 + d_4 \mid d_{d_5}$, па је и $d_2 + d_4$ делилац броја N. Ако би било $d_2 \neq 2$ онда су d_2 и d_4 непарни бројеви па је $d_2 + d_4$ паран број, па мора бити и N паран број, односно мора имати делилац 2 (контрадикција са $d_2 \neq 2$).

На основу датих претпоставки је $d_{d_5} = (2 + d_4) \cdot d_6 > d_6$, па је $d_5 > 6$ (индекси), тј. $d_5 \geqslant 7$. Пошто је $2 + d_4$ делилац то мора бити $2 + d_4 \geqslant d_5$. Дакле, $2 + d_4 \geqslant d_5 \geqslant 7$, одакле је $d_4 \geqslant 5$. Како је $d_4 < d_5 \leqslant 2 + d_4$ то је $d_5 = 1 + d_4$ (1) или је $d_5 = 2 + d_4$ (2).

У случају (1) имаћемо $d_6 = 2 + d_4$ одакле закључујемо да $3 \mid N$ ($d_4, d_4 + 1, d_4 + 2$ су делиоци броја N), па је $d_3 = 3$. Тада и $6 \mid N$ па је $d_4 = 6$ (због $d_5 \geqslant 7$), а онда је $d_5 = 7, d_6 = 8$, па $4 \mid N$ и $d_4 = 4$. Контрадикција.

Остаје случај (2): $d_5 = 2 + d_4$. Размотрићемо следеће могућности:

• Ако $4 \mid N$ због $d_4 \geqslant 5$ следи $d_3 = 4$, па $8 \mid N$. (Ако не би 8 делило N, тада би се у канонској факторизацији броја N прост број

2 јавио са степеном 2, па би $2+1=3$ био фактор укупног броја делилаца, тј. броја 16, што је немогуће). Како је $d_6 > d_5 \geqslant 7$ то је $d_6 \geqslant 8$ па мора бити $8 \in \{d_4, d_5, d_6\}$. Сви ови случајеви доводе до контрадикције. За $d_4 = 8$ мора бити $d_5 = 10$, па $5 \mid N$ и $d_4 = 5$, што је немогуће. За $d_5 = 8$ имаћемо $d_4 = 6$, па $3 \mid N$, одакле следи $d_3 = 3$, што је немогуће. За $d_6 = 8$ мора бити $d_5 = 7$ (због $d_5 \geqslant 7$), односно $d_4 = 5$ и $10 \mid N$. Међутим, $d_7 = (2+5)\cdot 8 = 56 > 10$. Контрадикција.

Пошто N није дељиво са 4 закључујемо да је d_3 прост број (ако би био сложен онда би постојала два мања проста делиоца, што је немогуће јер је $d_1 = 1$).

• Ако $3 \mid N$, тада је $d_3 = 3$. Тада $6 \mid N$, па због $d_4 \geqslant 5$ мора бити $d_4 = 6$ (јер је $d_5 \geqslant 7$). Онда је $d_5 = 2 + d_4 = 8$, па $4 \mid N$. Контрадикција.

Према томе, $3 \nmid N$ и закључујемо да је $d_3 \geqslant 5$ и $d_4 \geqslant 7$.

Како 4 не дели N и $2 + d_4$ закључујемо да је d_4 непарно. Како $2+d_4$ и d_4 нису дељиви са 3 то је $d_4 = 3k+2$ за неки цео број k, а како је непаран то је $d_4 = 6l+5$ за неко l. Како је d_{d_5} делилац, то је $d_5 \leqslant 16$ па је $7 \leqslant d_4 \leqslant 14$. Једина могућност је $d_4 = 11$ и $d_5 = 13$. Пошто су 2 и d_3 делиоци броја N то и $2d_3 \mid N$ и $2d_3 \geqslant d_4$, па је $d_3 \geqslant 6$. Пошто је d_3 прост и $d_3 < 11$ мора бити $d_3 = 7$. Дакле $N = 2 \cdot 7 \cdot 11 \cdot 13 = 2\,002$.

4. Конгруенције

Дефиниција 4.1. *Нека је дат природан број m, већи од 1. Цели бројеви a и b су конгруентни по модулу m ако дају исти остатак при дељењу са m. Пише се* $a \equiv b \pmod{m}$.

Теорема 4.1. 1. $a \equiv b \pmod{m}$ *ако и само ако је* $a = mt + b$ *за неки цео број* t.

2. $a \equiv b \pmod{m}$ *ако и само ако је разлика бројева* a *и* b *дељива са* m.

3. *Бити конгруентан по датом модулу је релација еквиваленције у скупу целих бројева.*

Доказ теореме 4.1. је лак па га остављамо читаоцима за вежбу.

Теорема 4.2. 1. *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$*, онда за свака два цела броја* x, y *важи* $ax + cy \equiv bx + dy \pmod{m}$.

2. *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$*, онда је* $ac \equiv bd \pmod{m}$.

3. *Ако је* $a \equiv b \pmod{m}$ *и* $m = \alpha d$, $d > 1$*, онда је* $a \equiv b \pmod{d}$.

4. *Ако је* $P(x)$ *полином по* x *са целобројним коефицијентима, онда из* $a \equiv b \pmod{m}$ *следи да је* $P(a) \equiv P(b) \pmod{m}$.

Доказ.

1. Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, тада $m \mid a - b$ и $m \mid c - d$, па важи и $m \mid (a - b)x$ и $m \mid (c - d)y$. Дакле,

$$m \mid (a - b)x + (c - d)y = (ax + cy) - (bx + dy),$$

тј. $ax + cy \equiv bx + dy \pmod{m}$.

2. Из $a \equiv b \pmod{m}$, следи да $m \mid a - b$, па и $m \mid (a - b)c$. Такође, из $c \equiv d \pmod{m}$ следи да $m \mid (c - d)b$. Дакле,

$$m \mid (ac - bc) + (cb - bd) = ac - bd,$$

тј. $ac \equiv bd \pmod{m}$.

3. Ако $m \mid a-b$ и $d \mid m$, $d>1$, тада због транзитивности релације дељивости, имамо да и $d \mid a-b$, тј. да је $a \equiv b \pmod{d}$.

4. Према 2. имамо да за сваки природан број n важи следећа импликација

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

а одавде и из 1. имамо да

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

за сваки полином $P(x)$ са целобројним коефицијентима. ■

ТЕОРЕМА 4.3. 1. *Ако су a и m узајамно прости и $ax \equiv ay \pmod{m}$, онда је $x \equiv y \pmod{m}$.*

2. $ax \equiv ay \pmod{m}$ *ако и само ако* $x \equiv y \pmod{\frac{m}{(a,m)}}$.

3. $x \equiv y \pmod{a}$ *и* $x \equiv y \pmod{b}$ *ако и само ако* $x \equiv y \pmod{[a,b]}$.

ДОКАЗ. 1. Из $ax \equiv ay \pmod{m}$, тј. из $m \mid a(x-y)$, због услова $(a,m)=1$ следи да $m \mid x-y$, тј. $x \equiv y \pmod{m}$.

2. Ако је $ax \equiv ay \pmod{m}$, тада је $a(x-y)=km$, за неки цео број k, па је и $\frac{a}{(a,m)}(x-y) = k\frac{m}{(a,m)}$. Дакле, $\frac{m}{(a,m)} \mid \frac{a}{(a,m)}(x-y)$. Како је $\left(\frac{m}{(a,m)}, \frac{a}{(a,m)}\right)=1$, следи да $\frac{m}{(a,m)} \mid x-y$, тј. да је $x \equiv y \pmod{\frac{m}{(a,m)}}$

Обрнуто, ако је $x \equiv y \pmod{\frac{m}{(a,m)}}$, тада је $x-y = k\frac{m}{(a,m)}$, за неки цео број k, па је и $ax-ay = \frac{ak}{(a,m)}m$, тј. $m \mid ax-ay$.

3.

$$\begin{aligned} x \equiv y \ (\mathrm{mod}\ a),\ x \equiv y \ (\mathrm{mod}\ b) \quad &\Leftrightarrow \quad a \mid x-y,\ b \mid x-y \\ &\Leftrightarrow \quad [a,b] \mid x-y \\ &\Leftrightarrow \quad x \equiv y \ (\mathrm{mod}\ [a,b]). \end{aligned}$$

■

4.1. Системи остатака

Дефиниција 4.2. *Скуп од m целих бројева у коме не постоји ни један пар бројева конгруентних по модулу m зове се* ***потпуни систем остатака по модулу*** m.

Теорема 4.4. 1. *Скуп* $\{0, 1, 2, \ldots, m-1\}$ *је потпуни систем остатака по модулу* m.

2. *Ако је m непаран број, скуп* $\left\{-\dfrac{m-1}{2}, \ldots, -1, 0, 1, \ldots, \dfrac{m-1}{2}\right\}$ *је потпуни систем остатака по модулу* m.
Ако је m паран сваки од скупова $\left\{-\dfrac{m}{2}+1, \ldots, -1, 0, 1, \ldots, \dfrac{m}{2}\right\}$ *и* $\left\{-\dfrac{m}{2}, \ldots, -1, 0, 1, \ldots, \dfrac{m}{2}-1\right\}$ *представља потпуни систем остатака по модулу* m.

3. *Ако је* $\{x_1, x_2, \ldots, x_m\}$ *потпуни систем остатака по модулу m и* $(a, m) = 1$, *тада је и* $\{ax_1 + b, ax_2 + b, \ldots, ax_m + b\}$ *потпуни систем остатака по модулу m, за сваки цео број b.*

Доказ. 3. Довољно је доказати да скуп $\{ax_1 + b, ax_2 + b, \ldots, ax_m + b\}$ садржи целе бројеве такве да не постоји ниједан пар бројева конгруентних по модулу m.

Заиста, ако би за неке i и j било

$$ax_i + b \equiv ax_j + b \pmod{m},$$

имали бисмо најпре да је $ax_i \equiv ax_j \pmod{m}$, а како је $(a, m) = 1$ и да је $x_j \equiv x_j \pmod{m}$, што је немогуће због претпоставке да је $\{x_1, x_2, \ldots, x_m\}$ потпуни систем остатака по модулу m. ■

Пример 4.1. *Скупови* $\{0, 1, 2, 3, 4, 5, 6, 7\}$ *и* $\{16, 9, -6, 11, 44, 5, 14, 31\}$ *су потпуни системи остатака по модулу* 8.

ДЕФИНИЦИЈА 4.3. *Скуп свих елемената потпуног система остатака по модулу m који су релативно прости са m назива се* ***сведени (редуковани) систем остатака по модулу*** m.

ПРИМЕР 4.2. $\{1, 3, 5, 7\}$ *и* $\{9, 11, 5, 31\}$ *су сведени системи остатака по модулу* 8.

ДЕФИНИЦИЈА 4.4. *Број природних бројева који нису већи од датог природног броја m и релативно су прости са њим, тј. број елемената произвољног сведеног система остатака по модулу m означава се са $\varphi(m)$. Функција φ зове се* ***Ојлерова функција***.

Ако је p прост број, тада је $\varphi(p) = p - 1$.
$\varphi(1) = \varphi(2) = 1$, $\varphi(3) = \varphi(4) = \varphi(6) = 2$ итд.

ТЕОРЕМА 4.5. *Ако је $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ сведени систем остатака по модулу m и $(a, m) = 1$, тада је и $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ сведени систем остатака по модулу m.*

ДОКАЗ. Тврђење следи из чињенице да скуп $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ садржи $\varphi(m)$ целих бројева, међу којима нема конгруентних по модулу m и сваки од њих је узајамно прост са m. ■

ПРИМЕР 4.3. *Нека је $m = 12$ и $a = 7$. Тада су m и a узајамно прости, па је скуп $\{7\cdot0, 7\cdot1, 7\cdot2, \ldots, 7\cdot11\} = \{0, 7, 14, \ldots, 77\}$ потпуни систем остатака по модулу 12, а скуп $\{7\cdot1, 7\cdot5, 7\cdot7, 7\cdot11\} = \{7, 35, 49, 77\}$ је сведени систем остатака по модулу 12.*

ТЕОРЕМА 4.6. *Ојлерова функција φ је мултипликативна.*

ДОКАЗ. Нека су m и n узајамно прости бројеви, тј. $(m, n) = 1$. Треба доказати да је $\varphi(mn) = \varphi(m)\varphi(n)$.

Распоредимо бројеве од 1 до mn у следећу табелу:

1	2	$\cdots$	k	$\cdots$	m
$m+1$	$m+2$	$\cdots$	$m+k$	$\cdots$	$2m$
$\cdots$	$\cdots$	$\cdots$	$\cdots$	$\cdots$	
$(n-1)m+1$	$(n-1)m+2$	$\cdots$	$(n-1)m+k$	$\cdots$	mn

Приметимо сада да је неки број узајамно прост са mn ако и само ако је узајамно прост и са m и са n. Доказ ћемо извести тако што ћемо најпре пребројати колико у табели има бројева узајамно простих са m, а затим колико међу њима има узајамно простих са n.

Бројеви сваке колоне горње табеле припадају истој класи еквиваленције у односу на релацију $\equiv \pmod{m}$, па сви бројеви једне колоне имају исти највећи заједнички делилац са m; тј. ако је један број у некој колони узајамно прост са m, тада су узајамно прости са m и сви остали бројеви те колоне. Последње нам омогућава да говоримо о „колонама узајамно простим са m“; очигледно таквих колона има $\varphi(m)$.

Посматрајмо сада једну колону бројева узајамно простих са m:

$$k,\ m+k,\ 2m+k,\ \ldots,\ (n-1)m+k.$$

Бројеви ове колоне су облика $mx+k,\ x \in \{0,1,2,\ldots,n-1\}$. Пошто је $(m,n) = 1$ бројеви ове колоне образују потпуни систем остатака по модулу n, па се међу њима налази $\varphi(n)$ бројева узајамно простих са n.

Дакле, свака колона наше таблице садржи $\varphi(n)$ бројева узајамно простих са n, тј. читава таблица има $\varphi(m)\cdot\varphi(n)$ бројева узајамно простих и са m и са n, па тиме и са mn. ∎

ТЕОРЕМА 4.7. *Ако је* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ *канонска факторизација броја*

n, онда је

$$\begin{aligned}\varphi(n) &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)\\ &= p_1^{\alpha_1-1}p_2^{\alpha_2-1}\cdots p_k^{\alpha_k-1}(p_1-1)(p_2-1)\cdots(p_k-1).\end{aligned}$$

ДОКАЗ. Нека је $n = p^\alpha$, за неки прост број p и неки природан број α. Међу природним бројевима од 1 до p^α има $p^{\alpha-1}$ бројева који нису узајамно прости са p^α, тј. бројева који су дељиви са p; то су:

$$p,\ 2p, \ldots,\ p^2, \ldots,\ p^\alpha.$$

Дакле, међу природним бројевима од 1 до p^α има $p^\alpha - p^{\alpha-1}$ бројева узајамно простих са p^α, тј.

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\left(1-\frac{1}{p}\right).$$

Ако је, сада, $n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ канонска факторизација броја n, применом претходне теореме (више пута) имамо:

$$\begin{aligned}\varphi(n) &= \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})\\ &= p^{\alpha_1}\left(1-\frac{1}{p_1}\right)p^{\alpha_2}\left(1-\frac{1}{p_2}\right)\cdots p^{\alpha_k}\left(1-\frac{1}{p_k}\right)\\ &= n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).\end{aligned}$$

■

ПРИМЕР 4.4.

$$\varphi(1008) = \varphi(2^4\cdot 3^2\cdot 7) = 2^3\cdot 3^1\cdot 7^0(2-1)(3-1)(7-1) = 288.$$

ТЕОРЕМА 4.8. (***Гаус***) *За сваки природан број n је* $\sum_{d|n}\varphi(d) = n$.

Доказ. Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја n. Тада су сви делиоци броја n (укључујући 1 и n):

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad 0 \leqslant \beta_i \leqslant \alpha_i \quad (i = 1, 2, \ldots, k),$$

па је (видети задатак 66)

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \cdots + \varphi(p_i^{\alpha_i})).$$

Пошто је

$$1+\varphi(p_i)+\cdots+\varphi(p_i^{\alpha_i}) = 1+(p_i-1)+(p_i^2-p_i)+\cdots+(p_i^{\alpha_i}-p_i^{\alpha_i-1}) = p_i^{\alpha_i},$$

то је

$$\sum_{d|n} \varphi(d) = \prod_{i=1}^{k} (1 + \varphi(p_i) + \cdots + \varphi(p_i^{\alpha_i})) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = n.$$

■

Пример 4.5.

$$\begin{aligned} \sum_{d|12} \varphi(d) &= \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) \\ &= 1 + 1 + 2 + 2 + 2 + 4 = 12. \end{aligned}$$

Теорема 4.9. (***Ојлер***) *Ако је* $(a, m) = 1$ *онда је* $a^{\varphi(m)} \equiv 1 \pmod{m}$.

Доказ. Нека је $\{x_1, x_2, \ldots, x_{\varphi(m)}\}$ сведени систем остатака по модулу m. Тада је и $\{ax_1, ax_2, \ldots, ax_{\varphi(m)}\}$ сведени систем остатака по модулу m, јер је $(a, m) = 1$. Према томе, за свако x_i постоји тачно један ax_j такав да је $x_i \equiv ax_j \pmod{m}$, па је

$$(ax_1)(ax_2) \cdots (ax_{\varphi(m)}) \equiv x_1 x_2 \cdots x_{\varphi(m)} \pmod{m},$$

односно

$$a^{\varphi(m)}x_1x_2\cdots x_{\varphi(m)} \equiv x_1x_2\cdots x_{\varphi(m)} \pmod{m}.$$

Како је $(x_1x_2\cdots x_{\varphi(m)}, m) = 1$, имамо да је

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

■

НАПОМЕНА. Број $\varphi(m)$ није најмањи природан број k такав да је $a^k \equiv 1 \pmod{m}$ (видети задатак 159 и поглавље 4.2.).

ТЕОРЕМА 4.10. (***Мала Фермаова теорема***) *Ако је p прост број и $p \nmid a$, онда је $a^{p-1} \equiv 1 \pmod{p}$.*

ДОКАЗ. Ако p не дели a, онда је $(a,p) = 1$ и како за сваки прост број p важи $\varphi(p) = p-1$, то је ово специјалан случај Ојлерове теореме. ■

ПОСЛЕДИЦА. Ако је p прост број и a произвољан цео број, онда важи $a^p \equiv a \pmod{p}$.

4.2. Поредак броја по датом модулу

ДЕФИНИЦИЈА 4.5. ***Поредак броја** a **по модулу** m је најмањи природан број t, ако постоји, за који важи $a^t \equiv 1 \pmod{m}$.*

ПРИМЕР 4.6. *Поредак броја 3 по модулу 11 је 5, јер $3^1, 3^2, 3^3, 3^4 \not\equiv 1 \pmod{11}$, а $3^5 \equiv 1 \pmod{11}$.*

Из Ојлерове теореме следи да поредак броја a по модулу m постоји ако су a и m узајамно прости. Важи и обрнуто: Ако је $a^t \equiv 1 \pmod{m}$ за неко t, онда је $1 = a^t - mu$, одакле следи $(a,m) = 1$.

Теорема 4.11. *Ако је t поредак броја a по модулу m и $a^s \equiv 1 \pmod{m}$, тада $t \mid s$. Специјално, $t \mid \varphi(m)$.*

Доказ. Претпоставимо да $t \nmid s$. Тада, за неке целе бројеве q и r, важи $s = qt + r$ и $0 < r < t$, па је $a^s = a^{qt+r} = (a^t)^q \cdot a^r$. Пошто је $a^t \equiv 1 \pmod{m}$ и $a^s \equiv 1 \pmod{m}$, следи да је $a^r \equiv 1 \pmod{m}$. Чињеница да је $a^r \equiv 1 \pmod{m}$ и $0 < r < t$, у контрадикцији је са чињеницом да је t најмањи природан број са особином $a^t \equiv 1 \pmod{m}$. ■

Последица. Ако је t поредак броја a по модулу m, тада је

$$a^x \equiv a^y \pmod{m} \quad \text{ако и само ако} \quad x \equiv y \pmod{t}.$$

Дефиниција 4.6. *Ако је поредак броја a по модулу m једнак $\varphi(m)$, број a се назива* ***примитивним кореном по модулу*** *m.*

Теорема 4.12. *Ако је a примитиван корен по модулу m, бројеви*

$$1 = a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}$$

образују сведени систем остатака по модулу m.

Доказ. Довољно је доказати да међу бројевима

$$1 = a^0,\ a^1,\ a^2,\ \ldots,\ a^{\varphi(m)-1}$$

не постоје два која су конгруентна по модулу m. Претпоставимо супротно, да постоје i и j такви да је

$$a^i \equiv a^j \pmod{m}, \quad 0 \leqslant i < j < \varphi(m).$$

Тада је

$$a^{j-i} \equiv 1 \pmod{m}, \quad 0 < j - i < \varphi(m),$$

супротно претпоставци да је a примитивни корен по модулу m. ■

Последица. Ако је p прост број и a примитиван корен по модулу p, тада бројеви $1, a, a^2, \ldots, a^{p-2}$ образују сведени систем остатака по модулу p.

ПРИМЕР 4.7. *2 је примитиван корен по модулу 11, па бројеви* $1,\ 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10,\ 2^6 \equiv 9,\ 2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6 \pmod{11}$ *образују сведени систем остатака по модулу* 11.

ТЕОРЕМА 4.13. (***Вилсон***) *Ако је p прост број, тада важи:*

$$(p-1)! \equiv -1 \ (\mathrm{mod}\ p).$$

ДОКАЗ. Тврђење очигледно важи ако је $p = 2$ или $p = 3$.

Нека је p прост број већи од 3. Тада је $1 \equiv 1 \pmod{p}$ и $p-1 \equiv -1 \pmod{p}$.

Да бисмо доказали теорему, довољно је доказати да за сваки број x такав да је $2 \leqslant x \leqslant p-2$, постоји тачно један број y такав да је

$$x \cdot y \equiv 1 \ (\mathrm{mod}\ p), \quad 2 \leqslant y \leqslant p-2,\ x \neq y.$$

Заиста, ако $x \in \{2, \ldots, p-2\}$, пошто је $(x,p) = 1$, скуп

$$\{0, x, 2x, \ldots, (p-1)x\}$$

образује потпуни систем остатака по модулу p, и тачно један елемент овог скупа (који је различит од нуле) је когруентан са 1 по модулу p.

Ако би било $y = 1$, имали бисмо да је $x \equiv 1 \pmod{p}$, што је немогуће.

Слично се доказује да не може бити ни $y = p-1$.

Најзад, ако би било $x = y$, имали бисмо да је $x^2 \equiv 1 \pmod{p}$, тј. да $p \mid x-1$ или $p \mid x+1$, односно да је $x \equiv 1 \pmod{p}$ или $x \equiv -1 \pmod{p}$, што је немогуће. ■

НАПОМЕНА. Важи и обрнуто тврђење Вилсонове теореме: *ако је* $(p-1)! \equiv -1 \pmod{p}$*, тада је p прост број.* Ако то не би важило, тада би p имао прост делилац $q < p$, па би важило да $q \mid (p-1)!$, па $q \nmid (p-1)! + 1$, а самим тим и $p \nmid (p-1)! + 1$. Контрадикција.

ТЕОРЕМА 4.14. *Конгруенција* $kx \equiv 1 \pmod{m}$ *има бар једно решење (по* x*) ако и само ако је број* k *узајамно прост са* m*, и тада свака од конгруенција* $kx \equiv n \pmod{m}$ *има решење по* x.

ДОКАЗ. Доказ следи из чињенице да је $(k, m) = 1$ ако и само ако постоје $a, b \in \mathbb{Z}$ такви да је $ak + bm = 1$. ■

ТЕОРЕМА 4.15. (***Кинеска теорема о остацима***) *Нека су* $a_1, a_2, \ldots, a_r$ *произвољни цели бројеви и нека су* $m_1, m_2, \ldots, m_r$ *по паровима узајамно прости природни бројеви, тј.* $(m_i, m_j) = 1$ *за* $i \neq j$*. Тада постоји решење система конгруенција:*

$$(1) \quad x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \; \ldots, \quad x \equiv a_r \pmod{m_r}.$$

Ако је x_0 *једно решење система једначина* (1)*, тада је* x *решење система* (1) *ако и само ако је облика* $x_0 + km$*, где је* k *произвољан цео број, а* $m = m_1 m_2 \cdots m_r$.

ДОКАЗ. Доказ ћемо извести за систем две конгруенције:

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2},$$

при чему је $(m_1, m_2) = 1$.

Свако решење прве од ових конгруенција је облика $x = a_1 + ym_1$, $y \in \mathbb{Z}$. Оно је решење и друге од ових конгруенција ако и само ако је $m_1 y \equiv a_2 - a_1 \pmod{m_2}$. Пошто су m_1 и m_2 узајамно прости, на основу претходне теореме следи да последња конгруенција има бар једно решење y_0, па је $x_0 = a_1 + m_1 y_0$ једно заједничко решење датог система конгруенција.

Даље, ако су x_0 и x_0' било која заједничка решења датих конгруенција, из $x_0 \equiv a_1 \pmod{m_1}$ и $x_0' \equiv a_1 \pmod{m_1}$ следи да $m_1 \mid x_0 - x_0'$. Слично се доказује да $m_2 \mid x_0 - x_0'$, па $[m_1, m_2] \mid x_0 - x_0'$, тј. $x_0 \equiv x_0'$ $(\mathrm{mod}\ [m_1, m_2])$. ■

4.3. Критеријуми дељивости – Паскалов метод

ТЕОРЕМА 4.16. *Да би број* $a = \overline{a_n a_{n-1} \cdots a_1 a_0} = \sum_{i=0}^{n} a_i \cdot 10^i$ *био дељив природним бројем* m*, неопходно је и довољно да је са* m *дељив збир*

$$a_n r_n + a_{n-1} r_{n-1} + \cdots + a_1 r_1 + a_0 r_0,$$

где су r_i *произвољни цели бројеви за које важи* $10^i \equiv r_i \pmod{m}$*,* $i = 0, 1, \ldots, n$.

ДОКАЗ. Доказ је једноставан, јер због особина конгруенција имамо да је

$$a = \sum_{i=0}^{n} a_i \cdot 10^i \equiv \sum_{i=0}^{n} a_i \cdot r_i \pmod{m}.$$

ПОСЛЕДИЦА 1. Да би за неко $t \in \mathbb{N}$ број $a = \overline{a_n \cdots a_1 a_0}$ био дељив са 2^t (односно са 5^t), неопходно је и довољно да је са 2^t (5^t) дељив број $\overline{a_{t-1} \cdots a_1 a_0}$.

ПОСЛЕДИЦА 2. Нека је t такав број да је $10^t \equiv 1 \pmod{m}$. Да би број a био дељив са m, неопходно је и довољно да је са m дељив збир бројева који се добијају поделом здесна налево броја a на групе по t цифара.

Специјално:

$$3 \mid a \quad \Leftrightarrow \quad 3 \mid \sum_{i=0}^{n} a_i \qquad (t = 1),$$

$$9 \mid a \quad \Leftrightarrow \quad 9 \mid \sum_{i=0}^{n} a_i \qquad (t = 1),$$

$$11 \mid a \quad \Leftrightarrow \quad 11 \mid \sum_{i=0}^{n} (10 a_{2i+1} + a_{2i}) \qquad (t = 2).$$

Пример 4.8. $11 \mid 4\,243\,657$ *јер* $11 \mid 121 = 57 + 36 + 24 + 4$.

Последица 3. Нека је t такав број да је $10^t \equiv -1 \pmod{m}$. Да би a било дељиво са m, неопходно је и довољно да је са m дељив збир бројева који се добијају на исти начин као у претходном случају (последица 2), али им се још наизменично промени знак.

Специјално:

$$\begin{aligned} 11 \mid a \quad &\Leftrightarrow \quad 11 \mid \sum_{i=0}^{n} (-1)^i a_i \qquad (t = 1),\\ 101 \mid a = \sum_{i=0}^{n} b_i \cdot 100^i \quad &\Leftrightarrow \quad 101 \mid \sum_{i=0}^{n} (-1)^i b_i \qquad (t = 2),\\ 7 \mid a = \sum_{i=0}^{n} c_i \cdot 1\,000^i \quad &\Leftrightarrow \quad 7 \mid \sum_{i=0}^{n} (-1)^i c_i \qquad (t = 3),\\ 13 \mid a = \sum_{i=0}^{n} c_i \cdot 1\,000^i \quad &\Leftrightarrow \quad 13 \mid \sum_{i=0}^{n} (-1)^i c_i \qquad (t = 3). \end{aligned}$$

Пример 4.9. $11 \mid 4\,243\,657$ *јер је* $7 - 5 + 6 - 3 + 4 - 2 + 4 = 11 \equiv 0 \pmod{11}$.

Пример 4.10. $101 \mid 5\,953\,546$ *јер је* $46 - 35 + 95 - 5 = 101 \equiv 0 \pmod{101}$.

Пример 4.11. $7 \mid 2\,232\,706$ *јер је* $706 - 232 + 2 = 476 \equiv 0 \pmod{7}$.

Пример 4.12. $13 \mid 596\,336$ *јер је* $336 - 596 = -260 \equiv 0 \pmod{13}$.

4.4. Задаци

109. Одредити остатак при дељењу броја 2^{30} са 13.

Решење. Како је $2^{30} = (2^5)^6$, $2^5 = 32 \equiv 6 \pmod{13}$ и $2^{10} \equiv 6^2 \equiv 10 \pmod{13}$, то је коначно $2^{30} \equiv 10^3 \equiv 12 \pmod{13}$.

110. Доказати да је број $2^{702} \cdot 19^{826} - 11^{347} \cdot 17^{195}$ дељив са 3.

Решење. Тврђење следи из:
$2 \equiv -1 \pmod 3 \Rightarrow 2^{702} \equiv 1 \pmod 3$;
$19 \equiv 1 \pmod 3 \Rightarrow 19^{826} \equiv 1 \pmod 3$;
$11 \equiv -1 \pmod 3 \Rightarrow 11^{347} \equiv -1 \pmod 3$;
$17 \equiv -1 \pmod 3 \Rightarrow 17^{195} \equiv -1 \pmod 3$.

111. За које природне бројеве n је $2^n - 1$ дељиво са 7?

Решење. За $n = 3k$ имамо $2^n = 8^k \equiv 1^k \equiv 1 \pmod 7$. За $n = 3k+1$ имамо $2^n = 2 \cdot 8^k \equiv 2 \cdot 1^k \equiv 2 \pmod 7$. За $n = 3k+2$ имамо $2^n = 4 \cdot 8^k \equiv 4 \cdot 1^k \equiv 4 \pmod 7$. Дакле, решења су сви природни бројеви дељиви са 3.

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

Решење: $323 = 17 \cdot 19$. Нека је n произвољан паран број. Из

$$20 \equiv 3 \pmod{17} \Rightarrow 20^n \equiv 3^n \pmod{17}$$

и

$$16 \equiv -1 \pmod{17} \Rightarrow 16^n \equiv 1 \pmod{17}$$

следи да $17 \mid 20^n + 16^n - 3^n - 1$.

Такође, из

$$20 \equiv 1 \pmod{19} \Rightarrow 20^n \equiv 1 \pmod{19}$$

и

$$16 \equiv -3 \pmod{19} \Rightarrow 16^n \equiv 3^n \pmod{19}$$

следи да и $19 \mid 20^n + 16^n - 3^n - 1$.

113. Доказати да је број $2\,222^{5555} + 5\,555^{2222}$ дељив са 7.

Решење. Како је

$$2\,222 \equiv 3 \pmod 7, \quad 3^6 \equiv 1 \pmod 7 \quad \text{и} \quad 5\,555 \equiv 5 \pmod 6,$$

то је

$$\begin{aligned} 2\,222^{5555} &= 2\,222^{6\cdot 925+5} = (2\,222^6)^{925} \cdot 2\,222^5 \equiv (3^6)^{925} \cdot 3^5 \\ &\equiv 1 \cdot 3^5 \equiv 5 \pmod 7. \end{aligned}$$

Слично, из

$$5\,555 \equiv 4 \pmod 7, \quad 4^3 \equiv 1 \pmod 7 \quad \text{и} \quad 2\,222 \equiv 2 \pmod 3)$$

следи

$$5\,555^{2222} = 5\,555^{3\cdot 740+2} \equiv 4^2 \equiv 2 \pmod 7.$$

Сада се тврђење добија из

$$2\,222^{5555} + 5\,555^{2222} \equiv 5 + 2 \pmod 7.$$

114. Наћи остатак који се добије при дељењу броја $3^{105} + 4^{105}$ са 11.

Решење.
$3^3 \equiv 5 \pmod{11}$, $3^2 \equiv -2 \pmod{11} \Rightarrow 3^5 \equiv -10 \equiv 1 \pmod{11}$;
$4^3 = 64 \equiv -2 \pmod{11}$, $4^2 \equiv 5 \pmod{11} \Rightarrow 4^5 \equiv -10 \equiv 1 \pmod{11}$.
Дакле, $3^{105} + 4^{105} \equiv 1 + 1 \pmod{11}$.

115. Доказати да број n^2+3n+5 није дељив са 121 ни за један природан број n.

Решење. Испитајмо најпре за које n, $11 \mid n^2+3n+5$. Разликујемо следеће случајеве:

$n \equiv 0 \pmod{11} \Rightarrow n^2+3n+5 \equiv 5 \pmod{11}$
$n \equiv 1 \pmod{11} \Rightarrow n^2+3n+5 \equiv 9 \pmod{11}$
$n \equiv 2 \pmod{11} \Rightarrow n^2+3n+5 \equiv 4 \pmod{11}$
$n \equiv 3 \pmod{11} \Rightarrow n^2+3n+5 \equiv 1 \pmod{11}$
$n \equiv 4 \pmod{11} \Rightarrow n^2+3n+5 \equiv 0 \pmod{11}$
$n \equiv 5 \pmod{11} \Rightarrow n^2+3n+5 \equiv 1 \pmod{11}$
$n \equiv 6 \pmod{11} \Rightarrow n^2+3n+5 \equiv 4 \pmod{11}$
$n \equiv 7 \pmod{11} \Rightarrow n^2+3n+5 \equiv 9 \pmod{11}$
$n \equiv 8 \pmod{11} \Rightarrow n^2+3n+5 \equiv 5 \pmod{11}$
$n \equiv 9 \pmod{11} \Rightarrow n^2+3n+5 \equiv 3 \pmod{11}$
$n \equiv 10 \pmod{11} \Rightarrow n^2+3n+5 \equiv 3 \pmod{11}$

Дакле, $11 \mid n^2+3n+5$ једино ако је $n \equiv 4 \pmod{11}$. До истог резултата много брже се долази ако приметимо да је

$$n^2+3n+5 \equiv n^2-8n+16 = (n-4)^2 \pmod{11},$$

па

$$11 \mid n^2+3n+5 \Leftrightarrow 11 \mid (n-4)^2 \Leftrightarrow 11 \mid n-4.$$

Дакле, $n = 11k+4$, за неки k. Али, тада је

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

одакле следи да $121 \nmid n^2+3n+5$.

Наравно, ако $11 \nmid n^2+3n+5$, тада $121 \nmid n^2+3n+5$.

116. Колико има природних бројева n таквих да је број

$$a = n(n+1)(n+2)+2^n$$

дељив са 3 003?

Решење. Ако би постојао природан број n такав да $3\,003 \mid a$, онда би важило и $3 \mid a$, што је немогуће, јер за сваки природан број n, $3 \mid n(n+1)(n+2)$, док је:

$2^1 \equiv 2 \pmod 3$, $\quad 2^2 \equiv 1 \pmod 3$,
$2^3 \equiv 2 \pmod 3$, $\quad 2^4 \equiv 1 \pmod 3$, $\ldots$,

па $3 \nmid 2^n$ за сваки природан број n.

117. (а) Ако је a цео, а n природан број, доказати да је број $a(a^{2n}-1)$ дељив са 6.

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

Решење. За произвољне бројеве x, y и сваки природан број n важи $x-y \mid x^n - y^n$.

Специјално, за сваки цео број a и сваки природан број n,

$$(*) \qquad a^2-1 \mid \left(a^2\right)^n - 1.$$

(а) За сваки цео број a и сваки природан број n, $6 \mid (a-1)a(a+1)$, тј. $6 \mid a(a^2-1)$, па према формули $(*)$ следи да $6 \mid a(a^{2n}-1)$.

(б) Ако је a непаран цео број, тада је $a = 2m+1$, за неки m, па је

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

Пошто $2 \mid m(m+1)$, да бисмо показали да $24 \mid a(a^2-1)$ остаје да покажемо да је један од бројева m, $m+1$, $2m+1$ дељив са 3. Разликујемо следеће случајеве:

(1) ако је $m \equiv 0 \pmod 3$, тада $3 \mid m(m+1)(2m+1)$;

(2) ако је $m \equiv 1 \pmod 3$, тада је $2m+1 \equiv 0 \pmod 3$, па важи $3 \mid m(m+1)(2m+1)$;

(3) ако је $m \equiv 2 \pmod 3$, тада је $m+1 \equiv 0 \pmod 3$, па опет важи $3 \mid m(m+1)(2m+1)$.

Дакле, $3 \mid m(m+1)(2m+1)$, па, на основу претходног разматрања, $24 \mid a(a^2-1)$, а на основу $(*)$ важи и $24 \mid a(a^{2n}-1)$.

118. 1) Доказати да се Фермаови бројеви f_n, $n \geqslant 2$, (у декадном запису) завршавају цифром 7.

2) Доказати да не постоји Фермаов број који је потпун квадрат.

3) Да ли постоји природан број m такав да је $1+2+\cdots+m = f_n$, за неки $n \geqslant 2$?

119. Ако је n непаран природан број, доказати да се број

$$2^{2n}\left(2^{2n+1}-1\right)$$

завршава цифрама 28.

120. (Зимско математичко такмичење, Бугарска 2000, 9. разред) Доказати да је цифра стотина броја $2^{1999}+2^{2000}+2^{2001}$ парна.

Решење. Запишимо дати број у облику

$$2^{1999}(1+2+4) = 7\cdot 2^9\cdot 2^{10}\cdot 2^{1980} = 7\cdot 2^9\cdot 2^{10}\cdot \left(2^{20}\right)^{99}.$$

Пошто је $2^9 = 512$, $2^{10} = 1\,024$ и $2^{20} = \left(2^{10}\right)^2$ то се двоцифрени завршетак броја 2^{20} поклапа са двоцифреним завршетком броја 24^2, па је двоцифрени завршетак броја 2^{20} једнак 76. Двоцифрени завршетак броја 76^2 је такође 76, па је двоцифрени завршетак датог броја једнак двоцифреном завршетку производа $7\cdot 12\cdot 24\cdot 76$, а то је 16. Пошто је број $2^{1999}+2^{2000}+2^{2001}$ дељив са 8, а двоцифрени завршетак му је 16, то цифра стотина мора бити парна.

121. Одредити последњу цифру броја $7^{7^{7^7}}$.

Решење. Како је $7 \equiv -1 \pmod 4$, то је $7^{7^7} \equiv -1 \pmod 4$, јер је 7^7 непаран број. Дакле, $7^{7^7} = 4k+3$, за неки $k \in \mathbb{N}$. Пошто је $7^2 \equiv -1$

$(\text{mod } 10)$ то је $7^4 \equiv 1 \pmod{10}$, па је и $7^{4k} \equiv 1 \pmod{10}$. Дакле,

$$7^{7^{7^7}} = 7^{4k+3} = 7^{4k} \cdot 7^3 \equiv 7^3 \equiv 3 \,(\text{mod } 10).$$

122. Одредити две последње цифре броја 9^{9^9}.

Решење. Како је $9^{10} = (10-1)^{10} \equiv 1 \pmod{100}$, то је $9^{10q+r} \equiv 9^r$ $(\text{mod } 100)$. Како је $9^9 \equiv 9 \pmod{10}$, то је $9^{9^9} \equiv 9^9 \equiv 89 \pmod{100}$. Према томе, последње две цифре броја 9^{9^9} су 8 и 9.

123. Ако је $a \equiv b \pmod{p^n}$, где је p прост број, доказати да је $a^p \equiv b^p \pmod{p^{n+1}}$.

Решење. Према услову задатка је $a = b + qp^n$, за неки цео број q. Степеновањем леве и десне стране са p добијамо $a^p = b^p + p^{n+1}t$, где је t цео број. Одатле следи тврђење.

124. Доказати да је $\displaystyle\sum_{k=1}^{m} k^n \equiv 0 \pmod{m}$, где су m и n непарни бројеви.

Решење. За свако k, $1 \leqslant k \leqslant m$ важи конгруенција $k \equiv k - m$ $(\text{mod } m)$. Степеновањем претходних конгруенција са n и сабирањем добијамо

$$\sum_{k=1}^{m} k^n \equiv \sum_{k=1}^{m} (-k)^n \pmod{m},$$

одакле је $\displaystyle 2\sum_{k=1}^{m} k^n \equiv 0 \pmod{m}$, тј. $\displaystyle\sum_{k=1}^{m} k^n \equiv 0 \pmod{m}$.

125. (а) Наћи остатак при дељењу квадрата непарног целог броја са 8.

(б) Нека су b и a_1, a_2, a_3, a_4, a_5 цели 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.

Решење. (а) За сваки природан број n је

$$(2n+1)^2 = 4n^2 + 4n + 1 = 4n(n+1) + 1,$$

па пошто $8 \mid 4n(n+1)$ (јер $2 \mid n(n+1)$), то је остатак при дељењу $(2n+1)^2$ са 8 једнак 1, тј. $(2n+1)^2 \equiv 1 \pmod 8$.

(б) Није тешко видети да за сваки природан број m важи:

$$m^2 \text{ је паран број } \Leftrightarrow m \text{ је паран број}$$

тј.

$$m^2 \text{ је непаран број } \Leftrightarrow m \text{ је непаран број.}$$

Нека су b и a_1, a_2, a_3, a_4, a_5 цели бројеви, такви да важи

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

Тада постоје две могућности:

1. b је паран број. У овом случају тврђење задатка важи;

2. b је непаран број. Тада је, према (а), $b^2 \equiv 1 \pmod 8$. Даље, ако би и сви бројеви a_1, a_2, a_3, a_4, a_5 били непарни, имали бисмо да је $a_i^2 \equiv 1 \pmod 8$, $i = 1, 2, 3, 4, 5$, па би важило

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

што је немогуће ако је $a_1^2 + a_2^2 + a_3^2 + a_4^2 + a_5^2 = b^2$, јер $5 \not\equiv 1 \pmod 8$. Дакле, бар један од бројева a_1, a_2, a_3, a_4, a_5 је паран.

126. Доказати да једначина $ax^2 + bx + c = 0$ нема рационалних решења ако су a, b, c цели непарни бројеви.

Решење. Претпоставимо супротно. Тада је дискриминанта дате квадратне једначине квадрат неког природног броја, тј. $b^2 - 4ac = k^2$. Како је b^2 непаран број, то је и k^2 непаран број, па је и k непаран број. У једнакости $b^2 - k^2 = 4ac$, десна страна је дељива са 4, али не и са 8, јер су a и c непарни бројеви. Квадрати непарних бројева при дељењу са 8 дају остатак 1, па је $b^2 - k^2$ дељиво са 8. Контрадикција.

127. Нека је $a_1, a_2, \dots, a_n$ произвољан поредак бројева $1, 2, \dots, n$. Доказати да је $(a_1-1)(a_2-2)\cdots(a_n-n)$ паран број ако је n непаран.

Решење. (*Прво решење*) Претпоставимо супротно, тј. да је n непарно и да је посматрани производ непаран. Тада су сви бројеви $a_i - i = b_i$ непарни, па је

$$\begin{aligned}0 &= (a_1 + a_2 + \cdots + a_n) - (1 + 2 + \cdots + n)\\ &= b_1 + b_2 + \cdots + b_n\\ &\equiv \underbrace{1 + 1 + \cdots + 1}_{n} \pmod 2\\ &\equiv n \equiv 1 \pmod 2.\end{aligned}$$

Контрадикција. Дакле, посматрани производ је паран.

(*Друго решење*) Нека је $s_1 = a_1 - 1,\ s_2 = a_2 - 2, \dots s_n = a_n - n$.

Ако би производ $s_1 s_2 \cdots s_n = (a_1 - 1)(a_2 - 2)\cdots(a_n - n)$ био непаран, сваки од чинилаца $s_1, s_2, \dots, s_n$ би био непаран. Пошто је n непаран број, тада би збир $s_1 + s_2 + \cdots + s_n$ такође био непаран, што је немогуће јер је

$$\begin{aligned}s_1 + s_2 + \cdots + s_n &= (a_1 - 1) + (a_2 - 2) + \cdots + (a_n - n)\\ &= (a_1 + a_2 + \cdots + a_n) - (1 + 2 + \cdots + n) = 0.\end{aligned}$$

128. Доказати да се међу било којих пет природних бројева могу изабрати три таква да им је збир дељив са 3.

Решење. Ако међу уочених пет бројева постоје три броја која имају исти остатак при дељењу са 3, онда је и њихов збир дељив са 3. Ако то није случај, онда се сваки остатак $(0, 1, 2)$ мора јавити бар једном. Тада бирамо три броја са различитим остацима. Њихов збир је дељив са 3:

$$3k + 3l + 1 + 3m + 2 = 3(k + l + m + 1).$$

129. (Изборно такмичење за ЈБМО 2003) Дато је једанаест различитих природних бројева. Доказати да међу њима постоји шест бројева чији је збир дељив са 6.

Решење. Изаберимо било којих пет од једанаест датих бројева. Међу њима можемо изабрати три броја тако да је њихов збир дељив са 3. На тај начин од тих једанаест бројева можемо изабрати три групе по три броја тако да је у свакој групи збир бројева дељив са 3. Сада, од те три групе постоје две, такве да су збирови њихових елемената исте парности, па је збир тих шест бројева дељив са 6.

130. (1) Које остатке при дељењу са 9 дају квадрати природних бројева?

(2) Доказати да не постоје природни бројеви m и n такви да је

$$m^2 + n^2 = 6\underbrace{00\ldots0}_{13}.$$

Решење. (1) Остаци при дељењу квадрата природних бројева са 9 су 0, 1, 4 или 7, што се лако види из следећих импликација:

$$\begin{aligned}
&x \equiv 0 \pmod 9) \Rightarrow x^2 \equiv 0 \pmod 9 \\
&x \equiv \pm1 \pmod 9 \Rightarrow x^2 \equiv 1 \pmod 9 \\
&x \equiv \pm2 \pmod 9 \Rightarrow x^2 \equiv 4 \pmod 9 \\
&x \equiv \pm3 \pmod 9 \Rightarrow x^2 \equiv 0 \pmod 9 \\
&x \equiv \pm4 \pmod 9 \Rightarrow x^2 \equiv 7 \pmod 9.
\end{aligned}$$

(2) Према делу (1), ако би такви бројеви постојали, тада би било $m^2 + n^2 \equiv r \pmod 9$, $r \in \{0, 1, 2, 4, 5, 7, 8\}$. Међутим, пошто је

$10 \equiv 1 \pmod 9$, то је $10^{13} \equiv 1 \pmod 9$, па је и $6 \cdot 10^{13} \equiv 6 \pmod 9$. Контрадикција.

131. Три дата цела броја су потпуни квадрати. Ако је збир та три броја дељив са 9, онда се међу њима могу изабрати два чија је разлика дељива са 9. Доказати.

Решење. Могући остаци при дељењу квадрата целог броја са 9 су: 0, 1, 4, 7.

Нека су x, y и z цели бројеви такви да $9 \mid x^2 + y^2 + z^2$. Претпоставимо да не постоје два броја од x^2, y^2, z^2 која дају исти остатак при дељењу са 9. Тада постоје следеће могућности:

1. Ако је $x^2 \equiv 0 \pmod 9$, $y^2 \equiv 1 \pmod 9$, $z^2 \equiv 4 \pmod 9$, тада је

$$x^2 + y^2 + z^2 \equiv 5 \ (\mathrm{mod}\ 9),$$

што је немогуће јер $9 \mid x^2 + y^2 + z^2$. Исти резулатат се добија ако претпоставимо да је $x^2 \equiv 0 \pmod 9$, $z^2 \equiv 1 \pmod 9$, $y^2 \equiv 4 \pmod 9$ или $y^2 \equiv 0 \pmod 9$, $z^2 \equiv 1 \pmod 9$, $x^2 \equiv 4 \pmod 9, \ldots$ па те случајеве не треба разматрати.

2. Ако је $x^2 \equiv 0 \pmod 9$, $y^2 \equiv 4 \pmod 9$, $z^2 \equiv 7 \pmod 9$, тада је

$$x^2 + y^2 + z^2 \equiv 2 \ (\mathrm{mod}\ 9),$$

што је опет немогуће јер $9 \mid x^2 + y^2 + z^2$.

3. Ако је $x^2 \equiv 1 \pmod 9$, $y^2 \equiv 4 \pmod 9$, $z^2 \equiv 7 \pmod 9$, тада је

$$x^2 + y^2 + z^2 \equiv 3 \ (\mathrm{mod}\ 9),$$

што је такође немогуће јер $9 \mid x^2 + y^2 + z^2$.

4. Ако је $x^2 \equiv 0 \pmod 9$, $y^2 \equiv 1 \pmod 9$, $z^2 \equiv 7 \pmod 9$, тада је

$$x^2 + y^2 + z^2 \equiv 8 \ (\mathrm{mod}\ 9),$$

што је такође немогуће јер $9 \mid x^2 + y^2 + z^2$.

132. Нека је $S(a)$ збир цифара природног броја a приказаног у декадном бројном систему, а m дати природан број. Доказати да је разлика $S(a^m) - S^m(a)$ дељива са 9 за било који природан број a.

Решење. Нека је $a = \overline{a_n a_{n-1} \cdots a_1 a_0} = \sum_{k=0}^{n} a_k \cdot 10^k$. Тада је

$$a - S(a) = \sum_{k=0}^{n} a_k(10^k - 1) = 9 \sum_{k=1}^{n} a_k \cdot \underbrace{11 \cdots 1}_{k},$$

тј. за сваки природан број a важи $9 \mid a - S(a)$, односно збир цифара природног броја a даје исти остатак при дељењу са 9 као и сам број a.

Користећи претходно доказану чињеницу и једнакост

$$\begin{aligned} &S(a^m) - S^m(a) = (S(a^m) - a^m) + (a^m - S^m(a)) \\ &= (S(a^m) - a^m) + (a - S(a))\left(a^{m-1} + a^{m-2}S(a) + \cdots + S^{m-1}(a)\right) \end{aligned}$$

добијамо да $9 \mid S(a^m) - S^m(a)$.

133. Наћи најмањи природан број који је 2 004 пута већи од збира својих цифара.

Решење. Нека је n тражени природан број, а $S(n)$ збир његових цифара. Тада је $n = 2\,004 S(n)$, па је $n - S(n) = 2\,003 S(n)$. Пошто $9 \mid n - S(n)$, а $9 \nmid 2\,003$ следи да $9 \mid S(n)$. Дакле, $S(n) \in \{9, 18, 27, \dots\}$. Ако је $S(n) = 9$, имали бисмо да је

$$n = 2\,004 \cdot 9 = 18\,036 \quad \text{и} \quad 1 + 8 + 0 + 3 + 6 = 18 > 9.$$

За $S(n) = 18$, имамо

$$n = 2\,004 \cdot 18 = 36\,072 \quad \text{и} \quad 3 + 6 + 0 + 7 + 2 = 18.$$

Дакле, тражени број је 36 072.

134. Дат је низ $1, 2, 4, 8, 16, 23, \dots$ у којем је сваки следећи број једнак збиру претходног броја и збира његових цифара, тј. $a_1 = 1$ и $a_n = a_{n-1} + S\left(a_{n-1}\right)$ за $n > 1$, где је $S\left(x\right)$ – збир цифара броја x. Да ли се у том низу појављује број 2 004 ?

Решење. Бројеви x и $S(x)$ дају једнаке остатке при деоби са 3, тј. $x \equiv S(x) \pmod 3$. Отуда је $a_n \equiv 2a_{n-1} \pmod 3$, 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 идуктивно следи $a_{2k-1} \equiv 1 \pmod 3$ и $a_{2k} \equiv 2 \pmod 3$ за свако $k \geqslant 1$. Како је $2\,004 \equiv 0 \pmod 3$, број 2 004 није члан датог низа.

135. (ИМО 1975) Нека је A збир цифара броја $4\,444^{4444}$, а B збир цифара броја A. Наћи збир цифара броја B.

Решење. Нека је C збир цифара броја B. Како је $4\,444^{4444} < 10\,000^{4444}$ број цифара броја $4\,444^{4444}$ није већи од $4 \cdot 4\,444 < 20\,000$. Зато је $A < 9 \cdot 20\,000 = 180\,000$. Дакле, $B \leqslant 9 \cdot 5 = 45$, па је $C \leqslant 12$. (Лако се види да је 39 број, међу бројевима $\leqslant 45$, са највећим збиром цифара: $3 + 9 = 12$.) Како је $4\,444 \equiv -2 \pmod 9$, имамо

$$
\begin{aligned}
4\,444^{4444} &\equiv (-2)^{4444} = (-2)^{3 \cdot 1481 + 1} = (-8)^{1481} \cdot (-2) \\
&\equiv 1^{1481} \cdot (-2) = -2 \equiv 7 \,(\mathrm{mod}\ 9).
\end{aligned}
$$

Пошто сваки број и његов збир цифара дају исти остатак при дељењу са 9, имамо да је $4\,444^{4444} \equiv A \equiv B \equiv C \pmod 9$, тј.

$$C \leqslant 12 \quad \text{и} \quad C \equiv 7 \,(\mathrm{mod}\ 9),$$

па је $C = 7$.

136. Нека су m и n различити 14-цифрени природни бројеви чији декадни записи садрже тачно по два пута сваку од цифара 1, 2, 3, 4, 5, 6 и 7. Да ли је могуће да број $\dfrac{m}{n}$ буде цео?

Решење. Природан број k и збир његових цифара $S(k)$ дају исти остатак при дељењу са 9.

Претпоставимо да је $\dfrac{m}{n}=k$ цео број. Пошто је $m\neq n$ имамо да је $k\geqslant 2$. Највећи број датог типа је $M=77\,665\,544\,332\,211$, а најмањи је $N=11\,223\,344\,556\,677$. Тада је

$$(*)\qquad 77\,665\,544\,332\,211\geqslant m=nk\geqslant k\cdot 11\,223\,344\,556\,677$$

Збир цифара бројева m и n је

$$2(1+2+3+4+5+6+7)=56\quad\text{и}\quad 56=9\cdot 6+2.$$

Зато је $m=9u+2$ и $n=9v+2$, за неке природне бројеве u и v. Али, како је $m=kn$, тада из једнакости $9u+2=k\cdot(9v+2)$ добијамо да је $9(u-kv)=2(k-1)$, одакле следи да $9\mid k-1$. Пошто је $k-1\neq 0$ имамо да је $k\geqslant 10$, што је немогуће због неједнакости $(*)$.

137. Одредити све природне бројеве n за које је збир цифара броја $n!$ једнак 9.

Решење. Нека је z_n збир цифара броја $n!$. Приметимо да је број $n!$ дељив са 9 ако и само ако је $n\geqslant 6$, као и да је:
$6!=720,\ z_6=9;$
$7!=5\,040,\ z_7=9;$
$8!=40\,320,\ z_8=9;$
$9!=362\,880,\ z_9=z_{10}>9.$
Нека је $n\geqslant 11$ и $n!=\overline{c_mc_{m-1}\dots c_1c_0}$. Претпоставимо да је

$$(*)\qquad c_m+c_{m-1}+\dots+c_1+c_0=9.$$

Како је $n\geqslant 11$, број $n!$ је дељив са 11, па је

$$(**)\qquad c_0-c_1+\dots+(-1)^mc_m=11k,\quad k\in\mathbb{Z}.$$

Како је

$$
\begin{aligned}
-9 = -(c_0 + c_1 + \dots + c_m) &\leqslant c_0 - c_1 + \dots + (-1)^m c_m \\
&= 11k \leqslant c_0 + c_1 + \dots + c_m = 9,
\end{aligned}
$$

следи да је $k = 0$.

Сабирајући једнакости $(*)$ и $(**)$ добијамо $2(c_0+c_2+c_4+\dots) = 9$. Контрадикција.

Тражени бројеви су $6, 7$ и 8.

138. Који је први број у низу:

$$3, 34, 343, 3\,434, 34\,343, 343\,434, \dots$$

који је дељив са 198?

Решење. Пошто је $198 = 2 \cdot 3^2 \cdot 11$, тражени број мора бити дељив са 2, па се мора завршавати са 4, тј. облика је

$$\underbrace{343434\dots34}_{2k \text{ цифара}}$$

Да би био дељив са 9, збир цифара мора да буде дељив са 9, тј. $3k + 4k = 7k$ мора бити дељив са 9, па је $k = 9\ell$. Поред тога, да би био дељив са 11 разлика цифара на парним и непарним местима мора бити дељива са 11, тј. $4k - 3k = k$ мора бити дељиво са 11, па је $k = 11m$. Најмањи број који задовољава наведене услове је $k = 9 \cdot 11 = 99$, па тражени број има 198 цифара и налази се на 198. месту у низу.

139. Да ли постоји природан број који се у декадном запису завршава са 11, који је дељив са 11 и чији је збир цифара 11?

Решење. Не постоји. Претпоставимо супротно. Нека је

$$\overline{a_{2k}a_{2k-1}\dots a_2a_111}$$

један такав број, где је $a_{2k-1} \neq 0$, док је могуће $a_{2k} = 0$, $k \geqslant 1$. Из услова задатка и критеријума за дељивост са 11 следи

$$(1) \qquad (a_1 + a_3 + \cdots + a_{2k-1}) + (a_2 + a_4 + \cdots + a_{2k}) = 9$$

и

$$(a_1 + a_3 + \cdots + a_{2k-1}) - (a_2 + a_4 + \cdots + a_{2k}) = 11t\,,$$

где је t неки цео број. Апсолутна вредност разлике два природна броја није већа од њиховог збира. Отуда је $t = 0$ и

$$(2) \qquad (a_1 + a_3 + \cdots + a_{2k-1}) - (a_2 + a_4 + \cdots + a_{2k}) = 0\,.$$

Једнакости (1) и (2) су контрадикторне, јер су збир и разлика два цела броја исте парности.

140. Доказати да се из сваког 2 005-цифреног броја у чијем се декадном запису појављују само цифре 9 и 6, може одстранити једна цифра, тако да добијени 2 004-цифрени број буде дељив са 11.

Решење. Доказаћемо општије тврђење:

„Из сваког $(2n+1)$-цифреног броја у чијем се декадном запису појављују само цифре a и b, може се одстранити једна цифра, тако да добијени $2n$-цифрени број буде дељив са 11.“

Ако неки број садржи две једнаке суседне цифре, онда се њиховим брисањем добија број који даје исти остатак при дељењу са 11 као и почетни. Ово следи из добро познатог тврђења да број даје исти остатак при дељењу са 11 као и разлика збирова његових цифара које стоје на непарним и парним местима, тј.

$$\overline{a_n a_{n-1} \ldots a_2 a_1 a_0} \equiv (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \pmod{11}\,.$$

Нека је A произвољан $(2n+1)$-цифрен број састављен искључиво од цифара a и b. Ако A има пар једнаких суседних цифара, тада њиховим брисањем добијамо $(2n-1)$-цифрен број A_1, такав да је

$A \equiv A_1 \pmod{11}$. На A_1 применимо исту операцију коју понављамо све до појаве броја A_k који нема једнаких суседних цифара. A_k такође има непаран број цифара и облика је $aba\dots ba$ или $bab\dots ab$. Брисањем средње цифре у A_k, означимо је са x, добијамо број A_{k-1} облика $ab\dots abba\dots ba$ или $ba\dots baab\dots ab$. A_{k-1} је очигледно дељив са 11.

Извршимо сад инверзну операцију, тј. „вратимо натраг", један по један, парове избрисаних једнаких цифара. Очигледно, сви тако добијени бројеви дељиви су са 11. У ствари, сваки се може сматрати да је настао од неког A_i брисањем цифре x. Последњи у низу добијен је на тај начин од A. Према томе, у броју A треба одстранити цифру x.

141. Без употребе калкулатора одредити цифре које стоје уместо звездица у изразу

$$109^{10} = 23673 * *67459211723401.$$

Решење. Означимо непознате цифре са x и y:

$$109^{10} = 23673xy67459211723401.$$

Како је

$$109^{10} - 1 = (9 \cdot 12 + 1)^{10} - 1 = 9k$$

и

$$109^{10} - 1 = (11 \cdot 10 - 1)^{10} - 1 = 11\ell,$$

број $109^{10} - 1$ је дељив и са 9 и са 11. Из дељивости са 9 следи да је $x + y + 72$ дељиво са 9, а из дељивости са 11 да је $y - x - 8$ дељиво са 11. С обзиром на то да $x, y \in \{0, 1, \dots, 9\}$ у обзир долазе следеће могућности: $x + y = 9$ или $x + y = 18$ и $y - x - 8 = 0$ или $y - x - 8 = -11$. Провером се констатује да је једино решење $x = 6$ и $y = 3$.

142. Познато је да је

$$28! = 30488a34461171386050150 4b00000.$$

Одредити цифре a и b.

Решење. Број 28! се завршава са (видети задатке 83 и 84)

$$\left[\frac{28}{5}\right] + \left[\frac{28}{5^2}\right] + \left[\frac{28}{5^3}\right] + \cdots = 5 + 1 = 6$$

нула. Према томе, $b = 0$.

Такође, $9 \mid 28!$, па 9 дели збир цифара броја $28!$, тј. $9 \mid 82 + a$. Пошто је $a \in \{0, 1, 2, \ldots, 9\}$, то је $a = 8$.

143. (ЈБМО 2004) Ако су природни бројеви x и y такви да су бројеви $3x + 4y$ и $4x + 3y$ потпуни квадрати, доказати да су и x и y дељиви са 7.

Решење. Нека је:

$$3x + 4y = m^2, \quad 4x + 3y = n^2. \tag{1}$$

Тада

$$7(x + y) = m^2 + n^2 \Rightarrow 7 \mid m^2 + n^2. \tag{2}$$

Узимајући $m = 7k + r$, $r \in \{0, 1, 2, 3, 4, 5, 6\}$ добијамо да су $0, 1, 2, 4$ могући остаци при дељењу квадрата целог броја са 7. Сада лако закључујемо да је $m^2 + n^2 \equiv 0 \pmod 7$ ако и само ако су и m и n дељиви са 7, па је тада

$$m^2 + n^2 \equiv 0 \pmod{7^2},$$

тј. $7(x + y) \equiv 0 \pmod{7^2}$, одакле добијамо

$$x + y \equiv 0 \pmod 7. \tag{3}$$

Даље, из (1) добијамо да је $x - y = n^2 - m^2$ и како је $n^2 - m^2 \equiv 0 \pmod{7^2}$, то је

$$x - y \equiv 0 \pmod 7. \tag{4}$$

Из (3) и (4) сада имамо да је $x + y = 7k$ и $x - y = 7\ell$, где су $k, \ell \in \mathbb{N}$. Отуда је:

$$2x = 7(k + \ell), \quad 2y = 7(k - \ell),$$

где су $k + \ell$ и $k - \ell$ природни бројеви, па $7 \mid 2x$ и $7 \mid 2y$, одакле коначно добијамо $7 \mid x$ и $7 \mid y$.

144. Доказати да $21 \mid a^2 + b^2$ повлачи $441 \mid a^2 + b^2$.

145. (I селекционо такмичење за ЈБМО, Румунија 2003) Нека су $n_1 < n_2 < \cdots < n_{31}$ прости бројеви. Доказати да ако 30 дели $n_1^4 + n_2^4 + \cdots + n_{31}^4$, тада су међу датим бројевима три узастопна проста броја.

Решење. Означимо $S = n_1^4 + n_2^4 + \cdots + n_{31}^4$ и $A = \{n_1, n_2, \ldots, n_{31}\}$.

Приметимо прво да $2 \in A$, јер би у супротном сви бројеви n_i, $i = 1, 2, \ldots, 31$ били непарни, па би и S био непаран број, што је немогуће.

Даље, $3 \in A$, јер би у супротном важило $n_i \equiv \pm 1 \pmod 3$, тј. $n_i^4 \equiv 1 \pmod 3$ за све $i = 1, 2, \ldots, 31$, одакле би следило $S \equiv 31 \equiv 1 \pmod 3$, што је немогуће.

Показаћемо још да $5 \in A$. Ако то не би био случај, тада би било $n_i \equiv \pm 1 \pmod 5$ или $n_i \equiv \pm 2 \pmod 5$, па би за све $i = 1, 2, \ldots, 31$ важило $n_i^4 \equiv 1 \pmod 5$, односно $S \equiv 31 \equiv 1 \pmod 5$, што је немогуће.

146. (БМО 1989) Нека су $d_1, d_2, \ldots, d_k$ сви делиоци природног броја n, такви да је $1 = d_1 < d_2 < \cdots < d_k = n$. Наћи све бројеве n

за које је $k \geqslant 4$ и важи

$$d_1^2 + d_2^2 + d_3^2 + d_4^2 = n.$$

Решење. Прво докажимо да је n паран број. Претпоставимо супротно; нека је n непаран број. Тада су сви делиоци 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

$$1^2 + 2^2 + d_3^2 + d_4^2 = n$$

следи 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 делилац 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 дељиво са $4 = d_3$ (квадрати непарних бројева при дељењу са 4 дају остатак 1, а број облика $4k + 22$ није дељив са 4). Контрадикција!

(2) $d_4 = 2a$, $a > 1$. 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

$$d_4 = 4, \quad d_3 = 3 \quad \text{и} \quad n = 1^2 + 2^2 + 3^2 + 4^2 = 30.$$

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 $d_3 = 5$. Следи да је $d_4 = 10$ и $n = 1^2 + 2^2 + 5^2 + 10^2 = 130$. Лако је проверити да су $1, 2, 5$ и 10 четири најмања делиоца броја 130.

Дакле, једини број који задовољава дати услов је 130.

147. Сви могући низови од по 7 цифара (од 0000000 до 9999999) исписани су један иза другог у произвољном поретку. На тај начин добијен је запис неког 70 000 000-цифреног броја. Доказати да је тај број дељив са 4 649.

Решење. Приметимо прво да је $4\,649 \mid 9\,999\,999$, и стога $10^7 \equiv 1 \pmod{4\,649}$, а самим тим и $10^{7k} \equiv 1 \pmod{4\,649}$ за све $k \geqslant 1$. Ако дати 70 000 000-цифрени број обележимо са n, биће

$$n \equiv 1\cdot1+2\cdot1+\cdots+9\,999\,999\cdot1 = 5\,000\,000\cdot9\,999\,999 \equiv 0 \pmod{4\,649}.$$

148. Странице једне књиге нумерисане су бројевима од 1 до 100 на уобичајен начин. Из књиге је истргнут известан број листова и при томе се испоставило да збир бројева којима су нумерисане истргнуте стране износи $4\,949$. Колико листова је истргнуто?

Решење. Сваки лист нумерисан је бројевима $2n-1$ и $2n$ за неко $1 \leqslant n \leqslant 50$. Њихов збир је $4n-1$. Обележимо са k број листова који су остали. Тада је

$$(4n_1-1)+(4n_2-1)+\cdots+(4n_k-1) = (1+2+\cdots+100)-4\,949,$$

односно $4(n_1+n_2+\cdots+n_k)-k = 101$.

С обзиром на то да је $101 \equiv 1 \pmod 4$, то је $k \equiv 3 \pmod 4$. Дакле, $k \in \{3,7,11,\ldots,97\}$. Како је $4(n_1+n_2+\cdots+n_k)-k \geqslant 105 > 101$ за $k \geqslant 7$, остаје $k=3$. То је могуће, јер је на пример 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.

149. На командној табли налази се 100 светлећих дугмади распоређених у облику квадрата 10×10. Притиском на једно дугме мења се његово стање као и стања свих дугмади која су са њим у истој врсти или у истој колони; упаљена се гасе, а угашена се пале. На почетку сва дугмад светле. Колики је минималан број притисака потребан да би се сва угасила?

Решење. Претпоставимо да су одређеним бројем притисака сва дугмад угашена. Нека је при томе $p_{i,j}$ пута притиснуто дугме које се налази у i-тој врсти и j-тој колони; то дугме зваћемо (i,j)–дугме. Обележимо још са r_i и c_j укупан број притисака на дугмад i-те врсте, односно j-те колоне. Укупан број промена стања (i,j)–дугмета износи $r_i + c_j - p_{i,j}$ и тај број је непаран јер је дугме угашено. Дакле

$$r_i + c_j - p_{i,j} \equiv 1 \pmod 2\,. \tag{1}$$

Слично је $r_i + c_k - p_{i,k} \equiv 1 \pmod 2$. Из ове две конгруенције следи $c_j - p_{ij} \equiv c_k - p_{ik} \pmod 2$. Тако је:

$$\begin{gathered} c_j - p_{1,j} \equiv c_k - p_{1,k} \pmod 2 \\ c_j - p_{2,j} \equiv c_k - p_{2,k} \pmod 2 \\ \vdots \\ c_j - p_{10,j} \equiv c_k - p_{10,k} \pmod 2\,. \end{gathered}$$

Сабирањем ових конгруенција и имајући у виду да је

$$p_{1,j} + p_{2,j} + \cdots + p_{10,j} = c_j \quad \text{и} \quad p_{1,k} + p_{2,k} + \cdots + p_{10,k} = c_k$$

добијамо $9c_j \equiv 9c_k \pmod 2$, односно $c_j \equiv c_k \pmod 2$. Када се то уврсти у горњи систем добијамо $p_{i,j} \equiv p_{i,k} \pmod 2$. То значи да су за сву дугмад једне врсте бројеви притисака исте парности. Слично се показује да исто важи и за дугмад исте колоне, одакле следи да су бројеви притисака на сву дугмад табле исте парности. Дакле, $p_{i,j} \equiv p \pmod 2$ за свако $i \in \{1, 2, \ldots, 10\}$ и свако $j \in \{1, 2, \ldots, 10\}$. Када то уврстимо у (1) добијамо $19p \equiv 1 \pmod 2$, односно $p \equiv 1 \pmod 2$. Дакле, свако дугме је непаран број пута притиснуто. Минималан број притисака је према томе 100; свако дугме притиснуто је тачно једанпут. Заиста, при томе се стање сваког дугмета промени 19 пута.

150. Квадратна таблица 3×3 попуњена је бројевима као на слици:

$$\begin{matrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{matrix}\,.$$

Таблица се може трансформисати у нову тако што се два броја из суседних поља умање за вредност мањег од та два броја, док се остали бројеви не мењају. Да ли се оваквим трансформацијама може добити таблица попуњена нулама?

Решење. Описаном трансформацијом парност збира свих елемената се не мења. Како је тај збир у почетку 45, он никада не може постати нула.

151. (Чешко-словачка математичка олимпијада – прва рунда, 2003) У једном кораку тројку (p,q,r) целих бројева можемо заменити тројком $(r+5q, 3r-5p, 2q-3p)$. Наћи, ако постоји, цео број k, такав да се из тројке $(1,3,7)$ после коначно много корака добије тројка $(k,k+1,k+2)$.

Решење. Сабирајући бројеве у новодобијеној тројци имамо

$$(r+5q)+(3r-5p)+(2q-3p) = 4r+7q-8p = 3(r+2q-3p)+(p+q+r).$$

Овај број даје исти остатак при дељењу са 3 као и број $p+q+r$, тј. остатак при дељењу са 3 збира елемената уређене тројке је инваријантан. Збир елемената тројке $(1,3,7)$ даје остатак 2 при дељењу са 3, док је збир три узастопна цела броја дељив са 3. Према томе, од тројке $(1,3,7)$ описаним поступком не може се добити тројка у којој су три узастопна цела броја.

152. У таблици 10×10

$$\begin{array}{ccccc} 0 & 1 & 2 & \dots & 9 \\ 9 & 0 & 1 & \dots & 8 \\ 8 & 9 & 0 & \dots & 7 \\ \dots & \dots & \dots & \dots & \dots \\ 1 & 2 & 3 & \dots & 0 \end{array}$$

заокружено је 10 елемената, у свакој врсти и колони по један. Доказати да су међу њима барем два једнака.

Решење. Приметимо да је у таблици сваки број конгруентан по модулу 10 са збиром првог броја у његовој врсти и првог броја у његовој колони. Дакле, збир заокружених елемената је по модулу 10 конгруентан са

$$(0+1+\cdots+9)+(0+9+8+\cdots+1)=90\equiv 0 \pmod{10}.$$

Међутим, ако би сви елементи били различити, тај збир би био

$$0+1+\cdots+9=45\equiv 5 \pmod{10}.$$

153. Нека је $\{a_1, a_2, \dots, a_m\}$ потпуни систем остатака по модулу m, $\{b_1, b_2, \dots, b_n\}$ потпуни систем остатака по модулу n и $(m,n)=1$. Доказати да је скуп $\{a_in+b_jm \mid i=1,2,\dots,m,\ j=1,2,\dots,n\}$ потпуни систем остатака по модулу mn.

Решење. Ако би било $a_in+b_jm \equiv a_\nu n+b_\mu m \pmod{mn}$, тада би важило $a_in \equiv a_\nu n \pmod{m}$, односно $a_i \equiv a_\nu \pmod{m}$ (јер је $(m,n)=1$), тј. да је $i=\nu$. Слично се добија да је $j=\mu$. Значи, не постоји пар елемената посматраног скупа који су међусобно конгруентни по модулу mn, па, према томе, овај скуп чини потпуни систем остатака по модулу mn.

154. Нека је $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ сведени систем остатака по модулу m, $\{b_1, b_2, \ldots, b_{\varphi(n)}\}$ сведени систем остатака по модулу n и $(m, n) = 1$. Доказати да је скуп

$$S = \{a_i n + b_j m \mid i = 1, 2, \ldots, \varphi(m),\ j = 1, 2, \ldots, \varphi(n)\}$$

сведени систем остатака по модулу mn.

Решење. Из задатка 153 следи да не постоји пар бројева из скупа S који су међусобно конгруентни по модулу mn.

Како је $(a_i n + b_j m, m) = (a_i n, m)$ и $(a_i, m) = (n, m) = 1$ то је $(a_i n + b_j m, m) = 1$. Слично се добија и $(a_i n + b_j m, n) = 1$. Зато је $(a_i n + b_j m, mn) = 1$.

Нека је N узајамно прост са mn. Како су m и n узајамно прости, постоје цели бројеви a и b такви да је $N = an + bm$. Како $(a, b) \mid N$, то је $(a, m) = 1$. Зато је a конгруентно по модулу m једном од елемената сведеног система остатака по модулу m, нпр. $a = a_i + k_i m$. Слично је и $b = b_j + \ell_j n$, па је

$$N = (a_i + k_i m)n + (b_j + \ell_j n)m \equiv a_i n + b_j m \pmod{mn}.$$

Како је сваки елемент релативно прост са mn конгруентан по модулу mn једном елементу скупа S, то је S сведени систем остатака по модулу mn.

155. Решити једначину $\varphi(n) = 3\,600$, ако су 3, 5 и 7 једини прости фактори броја n.

Решење. Нека је $n = 3^x \cdot 5^y \cdot 7^z$. Тада је

$$\begin{aligned} 3\,600 = \varphi(n) &= 3^{x-1} \cdot 5^{y-1} \cdot 7^{z-1} \cdot (3-1) \cdot (5-1) \cdot (7-1) \\ &= 3^{x-1} \cdot 5^{y-1} \cdot 7^{z-1} \cdot 2 \cdot 4 \cdot 6, \end{aligned}$$

односно $3^{x-1} \cdot 5^{y-1} \cdot 7^{z-1} = 3 \cdot 5^2$, па је $x = 2$, $y = 3$ и $z = 1$. Тада је $n = 3^2 \cdot 5^3 \cdot 7 = 7\,875$.

156. Наћи остатак при дељењу броја 317^{259} са 15.

Решење. Како је $317 = 21 \cdot 15 + 2$, биће $317^{259} \equiv 2^{259} \pmod{15}$. Према Ојлеровој теореми је $2^{\varphi(15)} \equiv 1 \pmod{15}$, па због $\varphi(15) = 8$, следи да је $2^8 \equiv 1 \pmod{15}$. Како је $259 = 32 \cdot 8 + 3$, то је $2^{259} = (2^8)^{32} \cdot 2^3 \equiv 8 \pmod{15}$.

157. Нека је $(a, m) = 1$ и $b \equiv c \pmod{\varphi(m)}$. Доказати да је тада $a^b \equiv a^c \pmod{m}$.

Решење. На основу Ојлерове теореме је $a^{\varphi(m)} \equiv 1 \pmod{m}$. Према услову задатка је $b = c + q \cdot \varphi(m)$ за неки цео број q. Зато је $a^{c+q\cdot\varphi(m)} \equiv a^c \pmod{m}$, тј. $a^b \equiv a^c \pmod{m}$.

158. (Зимско математичко такмичење, Бугарска 1997, 11. разред) Наћи све природне бројеве $m, n \geqslant 2$ такве да је

$$\frac{1 + m^{3^n} + m^{2\cdot 3^n}}{n}$$

цео број.

Решење. Нека m и n задовољавају услове задатка. Тада је n непаран број и $(m, n) = 1$. Ако је $n = 3$, тада је $m \equiv 1 \pmod{3}$, јер би у случају $m \equiv -1 \pmod{3}$ имали

$$1 + m^{3^n} + m^{2\cdot 3^n} \equiv 1 - 1 + 1 \equiv 1 \ (\mathrm{mod}\ 3).$$

Нека је сада $n > 3$. Тада важи $m^{3^n} \not\equiv 1 \pmod{n}$ јер би у супротном следило $1 + m^{3^n} + m^{2\cdot 3^n} \equiv 3 \pmod{n}$, тј. $n \mid 3$. Пошто је

$$1 + m^{3^n} + m^{2\cdot 3^n} = \frac{m^{3^{n+1}} - 1}{m^{3^n} - 1},$$

то је $m^{3^{n+1}} \equiv 1 \pmod{n}$. Нека је k најмањи природан број такав да је $m^k \equiv 1 \pmod{n}$. Тада $k \mid 3^{n+1}$ и $k \nmid 3^n$, па је $k = 3^{n+1}$. Како је

$(m,n)=1$ на основу Ојлерове теореме је $m^{\varphi(n)}\equiv 1\pmod n$, па је $k\leqslant\varphi(n)$. Према томе, $3^{n+1}\leqslant\varphi(n)\leqslant n-1$, што је немогуће.

Дакле, тражени бројеви су $n=3$ и сви бројеви $m\geqslant 4$ такви да је $m\equiv 1\pmod 3$.

159. (Уопштена Ојлерова функција) Нека је $L:\mathbb{N}\to\mathbb{N}$ функција дефинисана на следећи начин: $L(1)=1$, а за $m>1$

$$L(m)=\left[p_1^{\alpha_1-1}(p_1-1),p_2^{\alpha_2-1}(p_2-1),\dots,p_k^{\alpha_k-1}(p_k-1)\right],$$

при чему је $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ канонска факторизација броја m.

1) Наћи $L(360)$, $L(525)$, $L(222\,301)$.

2) Ако је $(a,m)=1$, доказати да је $a^{L(m)}\equiv 1\pmod m$.

Решење: 1) $L(360)=L(2^3\cdot 3^2\cdot 5)=[4,6,4]=12$;
$L(525)=L(3\cdot 5^2\cdot 7)=[2,20,6]=60$;
$L(222\,301)=L(31\cdot 71\cdot 101)=[30,70,100]=2\,100$.

2) Нека је $m=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ канонска факторизација броја m. Тада је према Ојлеровој теореми

$$a^{p_i^{\alpha_i-1}(p_i-1)}\equiv 1\ (\mathrm{mod}\ p_i^{\alpha_i}),\quad i=1,2,\dots,k.$$

Пошто $p_i^{\alpha_i-1}(p_i-1)\mid L(m)$ имамо да је $a^{L(m)}\equiv 1\pmod{p_i^{\alpha_i}}$, за све i из $\{1,2,\dots,k\}$, па је

$$a^{L(m)}\equiv 1\ (\mathrm{mod}\ [p_1^{\alpha_1},p_2^{\alpha_2},\dots,p_k^{\alpha_k}]),$$

тј. $a^{L(m)}\equiv 1\pmod m$.

На пример, како је $L(546)=L(2\cdot 3\cdot 7\cdot 13)=[1,2,6,12]=12$ и $(5,546)=1$, имамо да је

$$5^{12}=625^3\equiv 79^3\equiv 1\ (\mathrm{mod}\ 546).$$

160. Ако је $(a,65)=1$ и $(b,65)=1$, доказати да је $a^{12}-b^{12}$ дељиво са 65.

Решење: $65 = 13 \cdot 5$ и $(5, 13) = 1$.

Због $(a, 65) = (b, 65) = 1$ важи $13 \nmid a,\ 13 \nmid b$, па на основу Мале Фермаове теореме следи да је $a^{12} \equiv 1 \pmod{13}$ и $b^{12} \equiv 1 \pmod{13}$, тј. $a^{12} \equiv b^{12} \pmod{13}$. Аналогно се доказује да је и $a^{12} \equiv b^{12} \pmod 5$, па је $a^{12} \equiv b^{12} \pmod{65}$.

161. Доказати да је за сваки природан број n и сваки прост број p, број $1 + \sum_{k=1}^{p-1} k^{n(p-1)}$ дељив са p.

Решење. За свако $k \in \{1, 2, \ldots, p-1\}$, при чему је p прост број, је $(k, p) = 1$, па је, према Малој Фермаовој теореми $k^{p-1} \equiv 1 \pmod p$, па и за свако $n \in \mathbb{N}$, $k^{n(p-1)} \equiv 1 \pmod p$.

Дакле, $\sum_{k=1}^{p-1} k^{n(p-1)} \equiv p-1 \pmod p$, тј. $1+\sum_{k=1}^{p-1} k^{n(p-1)} \equiv 0 \pmod p$.

162. Ако су p, q различити прости бројеви, доказати да је

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}.$$

Решење. Према Малој Фермаовој теореми је

$$p^{q-1} \equiv 1 \pmod q \quad \text{и} \quad q^{p-1} \equiv 1 \pmod p,$$

јер је $(p, q) = 1$.

Дакле, $p \mid q^{p-1} - 1$, па и $p \mid p^{q-1} + q^{p-1} - 1$; и $q \mid p^{q-1} - 1$, па и $q \mid p^{q-1} + q^{p-1} - 1$. Како је $(p, q) = 1$, то $pq \mid p^{q-1} + q^{p-1} - 1$.

163. Показати да је $2^{n-1} \equiv 1 \pmod n$ за $n = 73 \cdot 37$.

Решење. На основу Мале Фермаове теореме је

$$2^{72} \equiv 1 \pmod{73} \ \text{ и } \ 2^{36} \equiv 1 \pmod{37},$$

па је и $2^{72} = (2^{36})^2 \equiv 1^2 \equiv 1 \pmod{37}$. Сада је $2^{72} \equiv 1 \pmod{[73, 37]}$, тј. $2^{72} \equiv 1 \pmod{73 \cdot 37}$, па је и $2^{72\cdot 37} \equiv 1^{37} \pmod{73 \cdot 37}$.

$$2^{n-1} = 2^{73\cdot 37-1} = 2^{72\cdot 37+37-1} = 2^{72\cdot 37} \cdot 2^{36} \equiv 2^{36} \equiv 1 \ (\mathrm{mod}\ 37 \cdot 73),$$

јер је $2^{36} = (2^9)^4 \equiv 1 \pmod{73}$.

164. Одредити, ако постоји, прост број p такав да $p^2 \mid 5^{p^2} + 1$.

Решење. Ако претпоставимо да постоји прост број 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

$$5^{p^2} \equiv 5^p \equiv 5 \ (\mathrm{mod}\ p)$$

и

$$5^{p^2} + 1 \equiv 6 \ (\mathrm{mod}\ p).$$

С друге стране, из услова $p^2 \mid 5^{p^2} + 1$, следи да

$$5^{p^2} + 1 \equiv 0 \ (\mathrm{mod}\ p).$$

Дакле, $6 \equiv 0 \pmod{p}$, па $p \in \{2, 3\}$.

За $p = 2$ имамо да је

$$5^4 + 1 = 626 \equiv 2 \ (\mathrm{mod}\ 4),$$

па 2 не задовољава услов задатка.

За $p = 3$ имамо

$$5^9 + 1 = 1\,953\,126 = 9 \cdot 217\,014 \equiv 0 \ (\mathrm{mod}\ 9),$$

па је 3 једини прост број који задовољава услов задатка.

165. 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.

Решење. 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 $(a, c) = 1$ и $(b, c) = 1$, имамо да је $(ab, c) = 1$, тј. $(p, b) = 1$, па према Малој Фермаовој теореми $p \mid b^{p-1} - 1$. Дакле, $p \mid A_p$.

Ако је $|ab + c| = 1$, тј. $ab + c = d$, $d \in \{-1, 1\}$, имамо да је

$$A_{n+2} = ab^3(b^{n-1} - 1) + ab(b^2 - 1) + d.$$

Тада је $ab(b^2 - 1) + d > 1$, па постоји прост број p такав да

$$p \mid ab(b^2 - 1) + d, \quad \text{тј.} \quad p \mid ab^3 + c.$$

Како је $(ab^3, c) = 1$, то $p \nmid b$, па према малој Фермаовој теореми $p \mid b^{p-1} - 1$, тј. $p \mid A_{p+2}$.

166. Доказати да за сваки прост број p и сваки цео број a који није дељив са p важи

$$a^p + (p-1)!\,a \equiv 0 \pmod{p}.$$

Решење. На основу Мале Фермаове теореме је $a^{p-1} \equiv 1 \pmod{p}$, па је $a^p \equiv a \pmod{p}$.

На основу Вилсонове теореме је $(p-1)! \equiv -1 \pmod{p}$, одакле следи $(p-1)!\,a \equiv -a \pmod{p}$.

Сада се једноставно добија $a^p + (p-1)!\,a \equiv a + (-a) \equiv 0 \pmod{p}$.

167. Нека су p и q узајамно прости природни бројеви, при чему је $q > 1$ и непаран. Доказати да постоје природни бројеви n и k такви да је $\dfrac{p}{q} = \dfrac{n}{2^k - 1}$.

Решење. Како је $(q, 2) = 1$ то је на основу Мале Фермаове теореме $2^{q-1} \equiv 1 \pmod{q}$. Тада постоји $n' \in \mathbb{N}$ такав да је $2^{q-1} - 1 = n' \cdot q$.

Одавде је $q = \dfrac{2^{q-1}-1}{n'}$. Сада је

$$\frac{p}{q} = \frac{pn'}{2^{q-1}-1} = \frac{n}{2^k-1}, \quad n = pn', \;\; k = q-1.$$

168. (Савезно такмичење 1969, IV разред) Ако је $p \neq 2$ прост број и a цео број који није дељив са p, онда је један и само један од бројева

$$A = a^{1+2+\cdots+(p-1)} + 1, \quad B = a^{1+2+\cdots+(p-1)} - 1$$

дељив са p. Доказати.

Решење. Важи $A - B = 2$ и $A \cdot B = (a^p)^{p-1} - 1$. Како број $A - B$ није дељив са p (јер је p прост број већи од 2), то нису оба броја A и B дељива са p. Број $A \cdot B$ је дељив са p на основу Мале Фермаове теореме. Зато је тачно један од бројева A и B дељив са p.

169. Доказати да за сваки природан број n важи

$$2^{4\cdot 5^{n-1}} \equiv 1 \pmod{5^n}.$$

Решење. Како је $\varphi(5^n) = 4 \cdot 5^{n-1}$ и како су бројеви 2 и 5^n узајамно прости то је на основу Ојлерове теореме

$$2^{\varphi(5^n)} = 2^{4\cdot 5^{n-1}} \equiv 1 \pmod{5^n}.$$

170. Доказати да су за произвољан природан број k последњих $2k$ цифара броја $2^{4\cdot 5^{2k-1}+2k} - 2^{2k}$ нуле.

Решење. На основу задатка 169, за $n = 2k$, следи да

$$5^{2k} \mid 2^{4\cdot 5^{2k-1}} - 1, \quad \text{тј.} \quad 10^{2k} \mid 2^{2k}\left(2^{4\cdot 5^{2k-1}} - 1\right),$$

одакле директно следи тврђење.

171. Доказати да за произвољан природан број k, постоји природан број n, такав да се у декадном запису броја 2^n појављује k узастопних нула.

Решење. Нека је $\overline{c_{r-1}c_{r-2}\ldots c_1c_0}$ декадни запис броја 2^{2k}. Тада је очигледно $r \leqslant k$. С обзиром на то и задатак 170, број $2^{4\cdot 5^{2k-1}+2k}$ се завршава низом од следећих $2k$ цифара

$$\overline{\ldots\underbrace{00\ldots0}_{2k-r}c_{r-1}c_{r-2}\ldots c_1c_0},$$

при чему је $2k - r \geqslant k$.

172. Доказати да је број $0,1248163264128\ldots$ ирационалан. (Иза децималне запете исписани су редом степени двојке.)

Решење. Ако би број $0,1248163264128\ldots$ био рационалан, онда би његов декадни запис био периодичан. Међутим, према задатку 171, за сваки природан број n у том декадном запису се може наћи n узастопних нула, па би се периода састојала од самих нула, што је очигледна контрадикција.

173. Ако су p и q узајамно прости природни бројеви и $p \geqslant 2$, тада у низу $\left(\dfrac{p^n}{qn+1}\right)$ има бесконачно много целих бројева. Доказати.

Решење. Како је $(p,q) = 1$, тада је $(p^k,q) = 1$ за све $k \in \mathbb{N}$. На основу Ојлерове теореме је $\left(p^k\right)^{\varphi(q)} \equiv 1 \pmod q$, тј. $q \mid p^{k\varphi(q)} - 1$. Нека је $n_k = \dfrac{p^{k\varphi(q)}-1}{q}$. Тада важи

$$\frac{p^{n_k}}{qn_k+1} = \frac{p^{n_k}}{p^{k\varphi(q)}} = p^{n_k - k\varphi(q)}.$$

За $p \geqslant 2$ и довољно велике k важи $n_k \geqslant k\varphi(q)$, па следи тврђење задатка.

174. Нека је p прост број. Сваки примитиван корен по модулу p^α, $\alpha \in \mathbb{N}$, је примитиван корен и по модулу p. Доказати.

Решење. Претпоставимо да a није примитиван корен по модулу p. Тада постоји природан број t такав да је, $1 \leqslant t < p-1$ и важи $a^t \equiv 1 \pmod p$, тј. $a^t = 1 + pq$, за неки q. Према биномној формули имамо да је

$$\begin{aligned} a^{tp^{\alpha-1}} &= (1+pq)^{p^{\alpha-1}} \\ &= 1 + p^{\alpha-1}pq + \frac{p^{\alpha-1}(p^{\alpha-1}-1)}{1\cdot 2}(pq)^2 + \cdots \\ &\equiv 1 \ (\mathrm{mod}\ p^\alpha), \end{aligned}$$

при чему је $tp^{\alpha-1} < p^{\alpha-1}(p-1) = \varphi(p^\alpha)$, па број a није примитиван корен по модулу p^α.

175. Нека је p прост број и $\alpha \geqslant 2$. Ако је a примитиван корен по модулу p и важи

$$a^{p^{\alpha-2}(p-1)} \not\equiv 1 \ (\mathrm{mod}\ p^\alpha),$$

доказати да је a примитиван корен по модулу p^α.

Решење. Нека је t поредак броја a по модулу p^α. Тада је $a^t \equiv 1 \pmod{p^\alpha}$ и $t \mid p^{\alpha-1}(p-1) = \varphi(p^\alpha)$. Пошто је $a^t \equiv 1 \pmod p$ и a је примитиван корен по модулу p (тј. $p-1$ је његов поредак по модулу p) имамо да $p-1 \mid t$, тј. $t = (p-1)q$, за неки q, па $(p-1)q \mid p^{\alpha-1}(p-1)$. Дакле, $q \mid p^{\alpha-1}$, тј. $q = p^\beta$, $0 \leqslant \beta \leqslant \alpha-1$, па је

$$(*) \qquad a^{p^\beta(p-1)} \equiv 1 \ (\mathrm{mod}\ p),\ 0 \leqslant \beta \leqslant \alpha-1.$$

Ако би било $0 \leqslant \beta \leqslant \alpha-2$, степеновањем конгруенције $(*)$ са $p^{\alpha-2-\beta}$, добили бисмо

$$a^{p^{\alpha-2}(p-1)} \equiv 1 \ (\mathrm{mod}\ p),$$

супротно претпоставци задатка. Дакле, $\beta = \alpha - 1$, па је

$$t = p^{\alpha-1}(p-1) = \varphi\left(p^{\alpha}\right).$$

176. Нека је p непаран прост број. Ако је a примитиван корен по модулу p, доказати да је бар један од бројева a и $a+p$ примитиван корен по модулу p^2.

177. (Корејска математичка олимпијада, 2003) Нека је m природан број. Доказати да ако $2^{m+1}+1$ дели $3^{2^m}+1$, тада је $2^{m+1}+1$ прост број?

Решење. Нека је $q = 2^{m+1}+1$. Тада из датог услова следи

$$(*) \qquad 3^{2^m} \equiv -1 \pmod{q},$$

одакле следи да је $(3,q)=1$. Квадрирањем обе стране конгруенције $(*)$ добијамо $3^{2^{m+1}} \equiv 1 \pmod{q}$, одакле следи да је поредак броја 3 по модулу q делилац од $2^{m+1} = q-1$. Према томе, поредак броја 3 по модулу q је облика 2^r, за неки природан број $r \leqslant m+1$. Ако би било $r \leqslant m$ тада би важило $3^{2^m} \equiv 1 \pmod{q}$, што је контрадикција са $(*)$. Дакле, $r = m+1$.

С друге стране, према Ојлеровој теореми, поредак броја 3 по модулу q је делилац броја $\varphi(q)$. Тако $2^{m+1} = q-1$ дели $\varphi(q)$. Пошто је $\varphi(q) \leqslant q-1$, то је $\varphi(q) = q-1$, па је број q прост.

178. (а) Одредити највећи заједнички делилац бројева $2\,002!+1$ и $2\,003!$.

(б) Доказати да су бројеви $2\,003!+1$ и $2\,004!$ узајамно прости.

Решење. (а) За сваки прост број $p < 2\,003$ важи $p \mid 2\,002!$, па према томе $p \nmid 2\,002!+1$ (јер је $(2\,002!+1, 2\,002!) = 1$). Како $2\,003!$ нема простих делилаца већих од $2\,003$, и како према Вилсоновој теореми $2\,003 \mid 2\,002!+1$, то је $(2\,002!+1, 2\,003!) = 2\,003$.

(б) Аналогно делу (а), за просте бројеве $p < 2\,004$ не може важити $p \mid 2\,003! + 1$. Међутим, број $2\,004!$ нема простих делилаца већих од $2\,003$, па је узајамно прост са $2\,003! + 1$.

179. Ако је p прост број, доказати да $p^3 \mid (p!)^2 - p^2$.

Решење. Тврђење следи из

$$(p!)^2 - p^2 = (p! - p)(p! + p) = p^2\left((p-1)! - 1\right)\left((p-1)! + 1\right)$$

и $p \mid (p-1)! + 1$.

180. Ако је p непаран прост број, доказати:

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p,$$

$$2^2 \cdot 4^2 \cdot 6^2 \cdot \ldots \cdot (p-1)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

Решење. На основу Вилсонове теореме је

$$(*) \qquad 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) = (p-1)! \equiv -1 \pmod p.$$

Даље, за свако $i = 0, \pm 1, \pm 2, \ldots$ важи

$$(**) \qquad i \equiv -(p-i) \pmod p.$$

Заменимо $\dfrac{p-1}{2}$ парних бројева на левој страни конгруенције $(*)$ њима конгруентним бројевима који се добијају из конгруенције $(**)$ за $i = 2, 4, \ldots, p-1$. Добијамо

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 (-1)^{\frac{p-1}{2}} \equiv (-1) \pmod p,$$

тј.

$$1^2 \cdot 3^2 \cdot 5^2 \cdot \ldots \cdot (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod p.$$

Аналогно се добија и друга конгруенција.

181. Доказати да је природан број $p > 2$ прост ако и само ако је $(p-2)! - 1 \equiv 0 \pmod{p}$.

Решење. Применом Вилсонове теореме добијамо

$$\begin{aligned}(p-1)!+1 &= (p-2)!(p-1)+1 = (p-2)!p - ((p-2)!-1)\\ &\equiv 0 \ (\mathrm{mod}\ p),\end{aligned}$$

одакле је $(p-2)! - 1 \equiv 0 \pmod{p}$.

182. Доказати да је природан број n прост ако и само ако $n \mid N$, где је $N = \sum_{k=1}^{n-3} k \cdot k!$.

Решење. Како је $k \cdot k! = (k+1)k! - k! = (k+1)! - k!$, то је

$$\begin{aligned}N &= 1\cdot 1! + 2\cdot 2! + \cdots + (n-3)(n-3)!\\ &= (2!-1!) + (3!-2!) + \cdots + ((n-2)! - (n-3)!)\\ &= (n-2)! - 1.\end{aligned}$$

Множењем претходне једнакости са $n-1$ и додавањем обема странама једнакости n, добијамо

$$(n-1)N + n = (n-1)! + 1.$$

На основу Вилсонове теореме, број n је прост ако и само ако $n \mid N$ јер је $(n, n-1) = 1$.

183. Наћи најмањи природан број x за који је $x \equiv 5 \pmod{7}$, $x \equiv 7 \pmod{11}$, $x \equiv 3 \pmod{13}$.

Решење. Како су 7, 11 и 13 узајамно прости по паровима, задовољени су услови Кинеске теореме о остацима. Овде је $a_1 = 5$, $a_2 = 7$, $a_3 = 3$; $m_1 = 7$, $m_2 = 11$, $m_3 = 13$; $m = 7 \cdot 11 \cdot 13 = 1\,001$.

$\frac{m}{m_j}$ је цео број и $\left(\frac{m}{m_j}, m_j\right) = 1$ за $j = 1, 2, 3$.
$\frac{m}{m_1} = 143$, $\frac{m}{m_2} = 91$ и $\frac{m}{m_3} = 77$.

⌜ *Напомена.* Ако је $(a, m) = 1$, $a, m \in \mathbb{N}$, конгруенција $ax \equiv b \pmod{m}$ увек има решење. Решење је $x = b \cdot a^{\varphi(m)-1}$. Наиме, на основу Ојлерове теореме је

$$ax - b = a \cdot b \cdot a^{\varphi(m)-1} - b = b\left(a^{\varphi(m)} - 1\right) \equiv 0 \pmod{m}.$$

⌟

Према томе, за све $j = 1, 2, 3$ постоје цели бројеви b_j такви да је $\frac{m}{m_j} \cdot b_j \equiv 1 \pmod{m_j}$. Јасно је да важи $\frac{m}{m_j} \cdot b_j \equiv 0 \pmod{m_i}$ за $i \neq j$.

Одредимо b_1, b_2, b_3 у нашем случају.
(i) $143b_1 \equiv 1 \pmod{7}$, тј. $3b_1 \equiv 1 \pmod{7}$, па је

$$b_1 \equiv 3^{\varphi(7)-1} \equiv 3^{6-1} \equiv 243 \equiv 5 \pmod{7}.$$

(ii) $91b_2 \equiv 1 \pmod{11}$, тј. $3b_2 \equiv 1 \pmod{11}$, па је

$$b_2 \equiv 3^{\varphi(11)-1} \equiv 3^{10-1} \equiv \left(3^3\right)^3 \equiv 5^3 \equiv 4 \pmod{11}.$$

(iii) $77b_3 \equiv 1 \pmod{13}$, тј. $-b_3 \equiv 1 \pmod{13}$, па је

$$b_3 \equiv -1 \pmod{13}.$$

Нека је $x_0 = \sum_{j=1}^{3} \frac{m}{m_j} b_j a_j$. Тада је

$$x_0 \equiv \frac{m}{m_i} b_i a_i \equiv a_i \pmod{m_i}, \quad i = 1, 2, 3,$$

па x_0 јесте решење датог система конгруенција.

$$x_0 = 143 \cdot 5 \cdot 5 + 91 \cdot 4 \cdot 7 + 77 \cdot (-1) \cdot 3 = 5\,892 = 5 \cdot 1\,001 + 887,$$

па је 887 најмањи природан број који задовољава дати систем конгруенција.

184. Доказати да постоји k узастопних природних бројева од којих је сваки дељив са квадратом природног броја већег од 1.

Решење. Нека су $p_1, p_2, \ldots, p_k$ различити прости бројеви. По Кинеској теореми о остацима систем

$$x \equiv -1 \pmod{p_1^2}, \ \ x \equiv -2 \pmod{p_2^2}, \ \ldots, \ x \equiv -k \pmod{p_k^2}$$

има решење. Ово значи да бројеви $x+1, x+2, \ldots, x+k$ имају тражену особину. Наиме $x+i$ је дељив са p_i^2 за $i = 1, 2, \ldots, k$.

185. (а) Нека су $a_1, a_2, \ldots, a_n$, $n \in \mathbb{N}$, различити узајамно прости у паровима природни бројеви. Доказати да постоји бесконачно много природних бројева b таквих да су $b + a_1, b + a_2, \ldots, b + a_n$ такође узајамно прости у паровима.

(б) Дато је n различитих природних бројева $a_1, a_2, \ldots, a_n$. За сваки прост број p означимо са $r_i(p)$ остатак који се добија при дељењу броја a_i, $i = 1, 2, \ldots, n$, са p. Доказати да постоји бесконачно много целих бројева b таквих да су $b + a_1, b + a_2, \ldots, b + a_n$ узајамно прости у паровима ако важи следећи услов: За сваки прост број p бар један елемент скупа $\{0, 1, \ldots, p-1\}$ се не појављује више од једанпут међу остацима $r_1(p), r_2(p), \ldots, r_n(p)$.

Решење. (а) Нека је

$$P = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} |a_i - a_j|.$$

Посматрајмо бесконачан скуп $\{P, 2P, 3P, \dots\}$. Покажимо да су бројеви $a_1 + kP, a_2 + kP, \dots, a_n + kP$ узајамно прости у паровима за сваки природан број k. Претпоставимо супротно. Тада за неке $i, j \in \{1, 2, \dots, n\}$, $i \neq j$, бројеви $a_i + kP$ и $a_j + kP$ имају заједнички делилац $d > 1$. Одавде следи да је $a_i - a_j = (a_i + kP) - (a_j + kP)$ дељиво са d, тј. да је P дељиво са d. Међутим, ако су и $a_i + kP$ и P дељиви са d тада $d \mid a_i$. Слично, ако $d \mid a_j + kP$ и $d \mid P$, тада $d \mid a_j$. Дакле, $d > 1$ је заједнички делилац бројева a_i и a_j супротно претпоставци да су ови бројеви узајамно прости. Дакле, за свако $k \in \mathbb{N}$ бројеви $a_i + kP$, $i = 1, 2, \dots, n$, су узајамно прости у паровима.

(б) Означимо са d разлику између највећег и најмањег од бројева $a_1, a_2, \dots, a_n$. Претпоставимо да важи задати услов. Посматрајмо све просте бројеве $p \leqslant d$. За сваки такав p нека је r_p елемент скупа $\{0, 1, \dots, p-1\}$ који се појављује не више од једанпут међу бројевима $r_1(p), r_2(p), \dots, r_n(p)$. Нека је

$$r_p^* = \begin{cases} p - r_p, & r_p > 0 \\ 0, & r_p = 0. \end{cases}$$

Пошто су различити прости бројеви узајамно прости, према Кинеској теореми о остацима следи да постоји цео број b такав да су конгруенције

$$b \equiv r_p^* \pmod{p}$$

задовољене за све просте бројеве $p \leqslant d$.

Докажимо да су бројеви $a_1 + b, a_2 + b, \dots, a_n + b$ узајамно прости у паровима. Претпоставимо да $a_i + b$ и $a_j + b$ имају заједнички прост фактор $\overline{p}$, за неке $i, j \in \{1, 2, \dots, n\}$, $i \neq j$. Разликујемо следеће случајеве:

(1) $\overline{p} > d$. У овом случају из

$$a_i + b \equiv 0 \pmod{\overline{p}} \quad \text{и} \quad a_j + b \equiv 0 \pmod{\overline{p}}$$

следи да $p \mid a_i - a_j$, тј. да је $|a_i - a_j| \geqslant \overline{p}$, што је у контрадикцији са $\overline{p} > d \geqslant |a_i - a_j|$.

(2) $\overline{p} \leqslant d$. У овом случају имамо да је

$$a_i+b=(mp+r_i(p))+(np+r_p^*) \quad \text{и} \quad a_j+b=(\ell p+r_j(p))+(np+r_p^*),$$

где су m, n, ℓ неки цели бројеви.

Претпоставимо да је $r_p^* = p - r_p$. Тада је број $a_i + b$ дељив са p само ако је $r_i(p) - r_p$ дељив са p, тј. ако је $r_i(p) = r_p$. Слично, $a_j + b$ је дељиво са p ако је $r_j(p) = r_p$. Међутим, остатак r_p појављује се највише једанпут у скупу остатака $\{r_1(p), r_2(p), \ldots, r_n(p)\}$. Контрадикција.

Ако је $r_p^* = 0$, тада су оба броја $r_i(p)$ и $r_j(p)$ дељива са p. Ово нас доводи до једнакости $r_i(p) = r_j(p) = 0 = r_p$, што нас поново доводи до контрадикције са избором броја r_p.

Дакле, бројеви $a_1 + b, a_2 + b, \ldots, a_n + b$ су узајамно прости у паровима.

Нека је

$$P^* = \prod_{\substack{i,j=1 \\ i \neq j}}^{n} |(a_i + b) - (a_j + b)|.$$

Према делу задатка (а) бројеви:

$$a_1 + b + kP^*, a_2 + b + kP^*, \ldots, a_n + b + kP^*$$

су узајамно прости у паровима.

186. Доказати да је број $a = (c_n \ldots c_1 c_0)_{12}$ дељив са 9, ако и само ако је његов двоцифрен завршетак $(c_1 c_0)_{12}$ дељив са 9.

187. Користећи Паскалов метод извести критеријум дељивости са 11_b броја записаног у бројевном систему са основом b, $b > 1$.

188. Користећи Паскалов метод извести критеријум дељивости са 6 броја записаног у бројевном систему са основом 7.

189. Користећи Паскалов метод извести критеријум дељивости са 37 броја записаног у бројевном систему са основом $1\,000$.

190. Доказати да је број $a = (3630)_p$ дељив са 7 ако и само ако је p облика $7k$ или $7k + 6$, $k \in \mathbb{N}$.

5. Диофантове једначине

5.1. Линеарне Диофантове једначине

Теорема 5.1. *Линеарна Диофантова једначина* $ax + by = c$ *има решења ако и само ако* $(a, b) \mid c$. *У том случају сва решења (има их бесконачно много) дате једначине су:*

$$x = \frac{c}{(a,b)}\, x_0 + \frac{b}{(a,b)}\, t, \quad y = \frac{c}{(a,b)}\, y_0 - \frac{a}{(a,b)}\, t \qquad (t \in \mathbb{Z}),$$

где је уређени пар (x_0, y_0) *једно решење једначине* $ax + by = (a, b)$, *које се може одредити, нпр. Еуклидовим алгоритмом.*

Доказ. Нека је $d = (a, b)$. Ако $d \nmid c$, онда је лева страна једначине $ax + by = c$ дељива са d, а десна није, па једначина нема решење.

Једначина $ax + by = d$ увек има решење у скупу целих бројева, које се може добити нпр. Еуклидовим алгоритмом.

Ако $d \mid c$, тада једначина $ax + by = c$ има решење $x_1 = \dfrac{c}{d}x_0$, $y_1 = \dfrac{c}{d}y_0$, где је пар (x_0, y_0) решење једначине $ax + by = d$. Међутим, у том случају једначина има бесконачно много решења. Претпоставимо да је (u, v) произвољно решење једначине $ax + by = c$. Тада је

$$ax_1 + by_1 = au + bv,$$

одакле је

$$\frac{a}{d}(u - x_1) = \frac{b}{d}(y_1 - v).$$

Како је $d = (a,b)$, то је $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, па

$$\frac{b}{d} \mid u - x_1 \quad \text{и} \quad \frac{a}{d} \mid y_1 - v,$$

одакле је

$$u = x_1 + \frac{b}{d}t \quad \text{и} \quad v = y_1 - \frac{a}{d}t, \quad t \in \mathbb{Z}.$$

Непосредном провером видимо да уређени пар (u,v) задовољава једначину $ax + by = c$ за све $t \in \mathbb{Z}$. ■

Пример 5.1. *Једначина* $27x+59y = 20$ *има решења јер је* $(27,59) = 1$. *Најпре треба наћи једно целобројно решење једначине* $27x + 59y = 1$. *Користећи Еуклидов алгоритам добијамо* $27 \cdot (-24) + 59 \cdot 11 = 1$, *па је опште решење дате једначине*

$$x = 20 \cdot (-24) + 59t, \quad y = 20 \cdot 11 - 27t \qquad (t \in \mathbb{Z}),$$

тј.

$$x = -480 + 59t, \quad y = 220 - 27t \qquad (t \in \mathbb{Z}).$$

5.2. Нелинеарне Диофантове једначине

Познато је да не постоји „општи поступак“ за решавање Диофантових једначина, тј. алгоритам којим бисмо могли утврдити да ли дата једначина има или нема целобројних решења. Међутим, ипак постоје методе којима се могу решавати неке специјалне класе ових једначина. Упознаћемо се само са неким елементарним методима.

Чињеница да се, за сваки природан број m, сваки цео број на **коначно** много начина може написати као производ m целих бројева, као и да се сваки природан број може на **коначно** много начина представити као збир m ненегативних бројева, често може бити од користи при решавању неких једноставнијих нелинеарних Диофантових једначина.

Ако су $I_1(x, y, \dots), \dots, I_m(x, y, \dots)$ цели алгебарски изрази, тада је једначина

$$I_1(x, y, \dots) \cdot \ldots \cdot I_m(x, y, \dots) = a,$$

за неки цео број a, еквивалентна дисјункцији система једначина:

$$\begin{array}{c} I_1(x, y, \dots) = c_1 \\ \vdots \\ I_m(x, y, \dots) = c_m \end{array} \quad \vee \quad \begin{array}{c} I_1(x, y, \dots) = d_1 \\ \vdots \\ I_m(x, y, \dots) = d_m \end{array} \quad \vee \quad \cdots$$

при чему је $a = c_1 \cdot \ldots \cdot c_m = d_1 \cdot \ldots \cdot d_m = \dots$ представљено на све могуће начине као производ m целих бројева (**метод производа**).

ПРИМЕР 5.2. *Решимо једначину* $xy + 3y - 5x = 18$ *у скупу целих бројева. Како је*

$xy + 3y - 5x = 18 \Leftrightarrow xy + 3y - 5x - 15 = 3 \Leftrightarrow (x + 3)(y - 5) = 3$, *разликујемо следеће случајеве:*

(i) $x + 3 = 3, \ \ y - 5 = 1$;

(ii) $x + 3 = 1, \ \ y - 5 = 3$;

(iii) $x + 3 = -3, \ \ y - 5 = -1$;

(iv) $x + 3 = -1, \ \ y - 5 = -3$.

Дакле, скуп целобројних решења дате једначине је

$$\mathcal{R} = \{(-2, 8), (-4, 2), (0, 6), (-6, 4)\}.$$

Слично, ако су $I_1(x, y, \dots), \dots, I_m(x, y, \dots)$ цели алгебарски изрази, тада је једначина

$$(I_1(x, y, \dots))^2 + \cdots + (I_m(x, y, \dots))^2 = a,$$

за неки природан број a, еквивалентна дисјункцији система једначина:

$$\begin{matrix} (I_1(x, y, \dots))^2 = s_1 \\ \vdots \\ (I_m(x, y, \dots))^2 = s_m \end{matrix} \quad \vee \quad \begin{matrix} (I_1(x, y, \dots))^2 = t_1 \\ \vdots \\ (I_m(x, y, \dots))^2 = t_m \end{matrix} \quad \vee \quad \cdots$$

при чему је $a = s_1 + \cdots + s_m = t_1 + \cdots + t_m = \dots$ представљено на све могуће начине као збир m потпуних квадрата (**метод збира**).

Пример 5.3. *У скупу целих бројева решимо једначину* $x^4 + y^2 + 2y = 1$. *Дата једначина је еквивалентна са* $x^4 + (y+1)^2 = 2$. *Збир два квадрата је једнак* 2 *ако и само ако су оба једнака* 1, *па је* $x^4 = 1$ *и* $(y+1)^2 = 1$, *одакле је* $x = 1$ *или* $x = -1$ *и* $y = 0$ *или* $y = -2$.

Скуп решења је $\mathcal{R} = \{(1, 0), (1, -2), (-1, 0), (-1, -2)\}$.

Једначине које су *линеарне*, односно *квадратне* по једној од променљивих чине класу једначина коју често можемо решавати комбиновањем метода из теорије обичних алгебарских једначина и теорије целих бројева.

На пример, једначина $A(x)y + B(x) = 0$, при чему су $A(x)$ и $B(x)$ неки цели алгебарски изрази по x, може се решавати анализом рационалног алгебарског израза $\dfrac{A(x)}{B(x)}$ (**метод количника**).

Пример 5.4. *Решимо једначину* $xy + 7x - 3y = 23$ *у скупу целих бројева.*

$xy + 7x - 3y = 23 \Leftrightarrow x(y+7) = 3y + 23$
За $y = -7$ *нема решења, а за* $y \neq -7$ *је*

$$x = \frac{3y+23}{y+7} = 3 + \frac{2}{y+7}\,.$$

Да би решење x *било целобројно, мора* $y + 7 \in \{1, -1, 2, -2\}$, *тј.* $y \in \{-6, -8, -5, -9\}$, *па је скуп решења*
$\mathcal{R} = \{(5,-6), (1,-8), (4,-5), (2,-9)\}$.

Природа решања једначине $A(x)y^2 + B(x)y + C(x) = 0$ зависи од дискриминанте

$$D(x) = (B(x))^2 - 4A(x)C(x).$$

Пошто тражимо целобројна решења, анализа дискриминанте заснива се на чињеници да је $D(x) \geqslant 0$, али и више, да је $D(x) = m^2$, за неки цео број m.

ПРИМЕР 5.5. *Решимо једначину* $7x + 14y = 5x^2 + 5xy + 5y^2$ *у скупу целих бројева. Дата једначина, записана у еквивалентном облику:*

$$5y^2 + (5x - 14)y + (5x^2 - 7x) = 0,$$

је квадратна по y. *Како је*

$$D(x) = (5x - 14)^2 - 4 \cdot 5(5x^2 - 7x) = 196 - 75x^2,$$

дата једначина има решења ако је $x^2 \leqslant \dfrac{196}{75} = 2,6133\ldots$, *тј. ако* $x \in \{-1, 0, 1\}$. *Према томе, имамо следеће могућности:*

$x = -1 \Rightarrow 5y^2 - 19y + 12 = 0 \Rightarrow y = 3 \vee y = \dfrac{4}{5}$, *тј.* $y = 3$;

$x = 0 \Rightarrow \cdots \Rightarrow y = 0 \quad \left(\vee\, y = \dfrac{14}{5}\right)$;

$x = 1 \Rightarrow \cdots \Rightarrow y = 2 \quad \left(\vee\ y = -\dfrac{1}{5}\right).$
Дакле, $\mathcal{R} = \{(-1, 3), (0, 0), (1, 2)\}$.

Из теорије полинома је познато да се сваки симетричан полином са више променљивих може изразити преко тзв. елементарних симетричних полинома. Специјално, у случају симетричног полинома са две променљиве ($P(x, y) = P(y, x)$) претходно речено значи да се $P(x, y)$ може изразити преко полинома $\sigma = x + y$ и $\pi = xy$. Често се користи растављање $x^2 + y^2 = (x + y)^2 - 2xy = \sigma^2 - 2\pi$.

ПРИМЕР 5.6. *Решимо једначину* $x^3+x^2y+xy^2+y^3 = 8(x^2+xy+y^2+1)$ *у скупу целих бројева.*

Једначина је симетрична по x, y *па се може записати у еквивалентном облику*

$$((x + y)^2 - 2xy)(x + y) = 8((x + y)^2 - xy + 1),$$

тј. у облику

$$u(u^2 - 2v) = 8(u^2 - v + 1),$$

при чему је $u = x + y$ *и* $v = xy$. *Из* $u^3 - 2uv = 8u^2 - 8v + 8$, *најпре закључујемо да* $2 \mid u$, *тј. да је* $u = 2t$, $t \in \mathbb{Z}$. *Сада, последња једначина постаје*

$$2t^3 - tv = 8t^2 - 2v + 2$$

и линеарна је по v. *За* $t \neq 2$ *имамо да је*

$$v = 2t^2 - 4t - 8 - \frac{18}{t - 2}$$

па су могуће вредности израза $t - 2$ *делиоци броја 18, тј. елементи скупа* $\{\pm 1, \pm 2, \pm 3, \pm 6, \pm 9, \pm 18\}$. *Разматрајући све добијене случајеве (наравно и случај* $t = 2$*), добијамо да је скуп решења* $\mathcal{R} = \{(8, 2), (2, 8)\}$.

Метод остатака

Разликовање случајева може се извршити и испитивањем остатка који се добија при дељењу неким бројем (најчешће $2, 3, 4, 5, 10$) леве, односно десне стране. Овај метод често је користан за доказивање да дата једначина нема решења. Наиме, ако за неки природан број $n > 1$ важи $L(x, y, \dots) \equiv r \pmod{n}$ при чему $r \in R \subseteq \{0, 1, 2, \dots, n-1\}$, а $D(x, y, \dots) \equiv s \pmod{n}$ при чему $s \in S \subseteq \{0, 1, 2, \dots, n-1\}$, тада у случају да је $R \cap S = \emptyset$, једначина $L(x, y, \dots) = D(x, y, \dots)$ нема решења у скупу целих бројева.

Метод остатака при дељењу са 10, често се назива **метод последње цифре**, док се метод остатака при дељењу са 2 назива **метод парности**.

На примеру $\equiv \pmod{10}$, илустроваћемо формирање табела које могу бити од велике користи:

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

ПРИМЕР 5.7. *За сваки цео број x важи:*

$x \equiv 0 \pmod{3} \Rightarrow x^2 \equiv 0 \pmod{3}$

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

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

Према томе, могући остаци при дељењу квадрата целог броја са 3 *су* 0 *и* 1.

Искористимо ту чињеницу сада да покажимо да једначине:

$3x^2 + 8 = y^2$ *и* $x^2 - 3y = 17$

немају решења у скупу целих бројева.

Ако би постојали цели бројеви x *и* y *такви да је* $3x^2 + 8 = y^2$*, из* $3x^2 \equiv 0 \pmod 3$ *и* $8 \equiv 2 \pmod 3$*, следило би да је* $y^2 \equiv 2 \pmod 3$*, што је немогуће.*

Слично се доказује да једначина $x^2 - 3y = 17$ *нема целобројна решења. То се оставља читаоцима да покажу.*

Метод неједнакости

Примену метода неједнакости илустроваћемо на следећем примеру:

ПРИМЕР 5.8. *Решимо једначину* $x^3 + 8x^2 - 6x + 8 = y^3$ *у скупу ненегативних целих бројева.*

Како је за $x \geqslant 0$

$$y^3 - (x+1)^3 = 5x^2 - 9x + 7 > 0$$

и

$$(x+3)^3 - y^3 = x^2 + 33x + 19 > 0$$

добијамо да је $x + 1 < y < x + 3$*. Имајући у виду да су* x *и* y *цели бројеви закључујемо да мора бити* $y = x+2$*, па дата једначина постаје* $2x(x-9) = 0$*. Решења су* $(0, 2)$ *и* $(9, 11)$*.*

5.2.1. Једначине облика $x^2 + y^2 = z^2$

Природни бројеви x, y, z, који су решења једначине $x^2 + y^2 = z^2$ представљају тзв. **Питагорине тројке**.

Ако x, y, z немају заједничких делилаца, онда се такво решење (x, y, z) назива **примитивно решење**. Налажењем свих примитивних решења (x, y, z) налазимо и сва остала решења, јер су она облика $(\alpha x, \alpha y, \alpha z)$, $\alpha \in \mathbb{N}$.

ТЕОРЕМА 5.2. *Да би уређена тројка* (x, y, z) *представљала примитивно решење једначине* $x^2 + y^2 = z^2$ *у скупу природних бројева, неопходно је и довољно да се* x, y, z *изражавају у облику*

$$\begin{aligned}
&x = 2mn,\ y = m^2 - n^2,\ z = m^2 + n^2 && (m, n \in \mathbb{N},\ (m, n) = 1,\\
& && m, n - \textit{различите парности})\\
&x = m^2 - n^2,\ y = 2mn,\ z = m^2 + n^2 && (m, n \in \mathbb{N},\ (m, n) = 1,\\
& && m, n - \textit{различите парности}).
\end{aligned}$$

ДОКАЗ. Нека је (x, y, z) примитивно решење једначине $x^2 + y^2 = z^2$.

Показаћемо најпре да од бројева x и y један мора бити паран, а други непаран и да z мора бити непаран број. Ако су x и y оба парни, тада је и z паран број, па се једначина може скратити, тј. посматрана тројка није примитивно решење. Ако су x и y оба непарни, тада је $z^2 = x^2 + y^2 \equiv 1 + 1 = 2 \pmod 4$, што је немогуће.

Нека је $x = 2a$ паран, а y непаран број. Тада је z непаран број. Дата једначина се може написати у облику

$$x^2 = z^2 - y^2 = (z - y)(z + y).$$

Оба чиниоца на десној страни су парни бројеви, па су бројеви

$$u = \frac{z + y}{2} \quad \text{и} \quad v = \frac{z - y}{2}$$

цели. Тада је $x^2 = 4a^2 = 4uv$, тј. $a^2 = uv$. Бројеви u и v су узајамно прости (видети задатак 32), па на основу теореме 3.6. следи да они морају бити квадрати целих бројева: $u = m^2$ и $v = n^2$, при чему m и n немају заједничких делилаца и различите су парности. Дакле, добијамо да је $x = 2a = 2mn$, $y = u - v = m^2 - n^2$ и $z = u + v = m^2 + n^2$, при чему су $m, n \in \mathbb{N}$, $(m, n) = 1$, $m > n$ и бројеви m и n су различите парности.

Лако се проверава да је

$$(m^2 - n^2)^2 + (2mn)^2 = m^4 + 2m^2n^2 + n^4 = (m + n)^2,$$

тј. да тројка (x, y, z) задовољава једначину $x^2 + y^2 = z^2$. ■

Једна од најпознатијих теорема у математици, о којој је доста писано, и то не само у математичким часописима, а коју је коначно 1995. после више од 300 година доказао Ендру Вајлс (Andrew Wiles) је ***Велика Фермаова теорема***:

ТЕОРЕМА 5.3. *Ако је n ма који природан број већи од 2, онда једначину*

$$x^n + y^n = z^n$$

не могу задовољавати никаква три природна броја x, y, z.

ПРИМЕР 5.9. *Нађимо све Питагорине тројке за $0 < z < 20$, $x < y$. Нађимо најпре све примитивне Питагорине тројке које задовољавају $0 < z < 20$, $x < y$.*

- *За $n = 1$, $m = 2$ добијамо $m^2 + n^2 = 5$, $m^2 - n^2 = 3$, $2mn = 4$, односно добијамо тројку $(3, 4, 5)$.*
- *За $n = 2$, $m = 3$ добијамо $m^2 + n^2 = 13$, $m^2 - n^2 = 5$, $2mn = 12$, односно добијамо тројку $(5, 12, 13)$.*
- *За $n = 3$, $m = 4$ добијамо $m^2 + n^2 = 25 > 20$.*
- *За $n = 1$, $m = 4$ добијамо $m^2 + n^2 = 17$, $m^2 - n^2 = 15$, $2mn = 8$, односно добијамо тројку $(8, 15, 17)$.*

Тражене Питагорине тројке су:
$(3, 4, 5)$, $(6, 8, 10)$, $(9, 12, 15)$, $(5, 12, 13)$, $(8, 15, 17)$.

5.2.2. Пелова једначина

Диофантова једначина облика

$$(*) \qquad x^2 - Dy^2 = 1,$$

где је D природан број, позната је као ***Пелова једначина.***

Лако се уверавамо да су парови $(1,0)$ и $(-1,0)$ решења једначине $(*)$ за било које D. Ова решења називамо ***тривијалним***. Основни проблем је, за задато D, одредити, ако постоје, целобројна решења различита од тривијалних. Приметимо, такође, да ако је пар (x_0, y_0) решење једначине $(*)$, тада су решења и парови $(x_0, -y_0)$, $(-x_0, y_0)$ и $(-x_0, -y_0)$. Ова чињеница нам омогућава да се при решавању једначине $(*)$ ограничимо на решавање једначине $(*)$ у скупу природних бројева.

Ако је D квадрат природног броја, тј. $D = d^2$ за неки природан број d, тада је $x^2 - Dy^2 = (x - dy)(x + dy) \neq 1$ за све природне бројеве x и y, па једначина $(*)$ нема нетривијалних решења. Зато ћемо убудуће под Пеловом једначином подразумевати једначину $(*)$ где је D природан број који није потпун квадрат.

ЛЕМА 5.1. *Ако су a, b, c, d рационални бројеви и θ ирационалан број, тада из једнакости $a + b \cdot \theta = c + d \cdot \theta$ следи $a = c$ и $b = d$.*

ДОКАЗ. Ако је $b = d$, онда је и $a = c$.

Ако је $b \neq d$, тада бисмо имали да је $\theta = \dfrac{a-c}{d-b}$, што је немогуће јер је θ ирационалан број, док је $\dfrac{a-c}{d-b}$ рационалан. ■

Лема 5.2. *Нека је θ ирационалан број и n произвољан природан број већи од* 1. *Тада постоје цели бројеви x и y такви да је*

$$|x - y\theta| < \frac{1}{n}, \quad 1 \leqslant y \leqslant n.$$

Лема 5.3. *Постоји бесконачно много различитих парова целих бројева (x, y) таквих да важи:* $|x - y\theta| < \dfrac{1}{y}$.

Доказ. Нека је n_1 произвољан природан број већи од 1. На основу леме 5.2. постоје цели бројеви x_1 и y_1 такви да је

$$0 < |x_1 - y_1\theta| < \frac{1}{n_1}, \quad 1 \leqslant y_1 \leqslant n_1.$$

Даље, постоји природан број n_2 такав да је

$$\frac{1}{n_2} < |x_1 - y_1\theta| < \frac{1}{n_1},$$

а тиме, опет на основу леме 5.2., и цели бројеви x_2 и y_2 такви да је

$$|x_2 - y_2\theta| < \frac{1}{n_2}, \quad 1 \leqslant y_2 \leqslant n_2.$$

На описани начин можемо формирати бесконачне низове целих бројева: $1 < n_1 < n_2 < n_3 < \ldots$; $x_1, x_2, x_3, \ldots$ и $y_1, y_2, y_3, \ldots$ тако да важи:

$$(*) \qquad \frac{1}{n_1} > |x_1 - y_1\theta| > \frac{1}{n_2} > |x_2 - y_2\theta| > \frac{1}{n_3} > |x_3 - y_3\theta| > \cdots$$

при чему је $1 \leqslant y_i \leqslant n_i$, $i \in \mathbb{N}$. Из неједнакости $(*)$ следи да су парови (x_1, y_1), (x_2, y_2), (x_3, y_3), $\ldots$ међусобно различити. ■

ЛЕМА 5.4. *Постоји бесконачно много целобројних решења неједначине*

$$\left|x^2 - Dy^2\right| < 1 + 2\sqrt{D},$$

при чему је D природан број који није потпун квадрат.

ДОКАЗ. Према леми 5.3. ($\theta = \sqrt{D}$) постоји бесконачно много парова (x, y) целих бројева таквих да је

$$\left|x - y\sqrt{D}\right| < \frac{1}{y}.$$

Тада, за сваки такав пар целих бројева важи:

$$\begin{aligned}\left|x + y\sqrt{D}\right| &= \left|x - y\sqrt{D} + 2y\sqrt{D}\right| \leqslant \left|x - y\sqrt{D}\right| + 2|y|\sqrt{D}\\ &< \frac{1}{y} + 2y\sqrt{D},\end{aligned}$$

па и

$$\begin{aligned}\left|x^2 - Dy^2\right| &= \left|x - y\sqrt{D}\right| \left|x + y\sqrt{D}\right|\\ &< \frac{1}{y}\left(\frac{1}{y} + 2y\sqrt{D}\right) = 2\sqrt{D} + \frac{1}{y^2}\\ &\leqslant 2\sqrt{D} + 1.\end{aligned}$$

■

ТЕОРЕМА 5.4. *Дата је једначина*

$$(*) \qquad x^2 - Dy^2 = 1,$$

при чему је D природан број који није потпун квадрат. Тада важи:

а) *Једначина $(*)$ има бар једно решење у скупу природних бројева.*

б) *Ако је пар* (x, y) *природних бројева једно решење једначине* $(*)$, *тада су решења и парови* (x_n, y_n), $n \in \mathbb{N}$, *одређени са*

$$x_n + y_n\sqrt{D} = \left(x + y\sqrt{D}\right)^n.$$

в) *Ако су* (x, y) *и* (x', y') *два решења једначине* $(*)$, *тада важи:*

$$y < y' \;\Leftrightarrow\; x < x' \;\Leftrightarrow\; x + y\sqrt{D} < x' + y'\sqrt{D}.$$

г) *Ако је пар* (x_0, y_0) *природних бројева, такозвано* ***минимално решење*** *једначине* $(*)$, *такав да је* $y_0 \leqslant y$, *за свако друго решење* (x, y) *једначине* $(*)$, *онда су са*

$$x_n + y_n\sqrt{D} = \left(x_0 + y_0\sqrt{D}\right)^n$$

одређена сва решења (x_n, y_n) *једначине* $(*)$ *у скупу природних бројева.*

Доказ. а) Према леми 5.4. постоји цео број k, различит од нуле, такав да је $|k| < 1 + 2\sqrt{D}$ и једначина

$$x^2 - Dy^2 = k \tag{1}$$

има бесконачно много решења.

На (бесконачном) скупу парова целих бројева који су решења једначине (1) дефинишимо релацију еквиваленције $\sim$ на следећи начин:

$$(x_1, y_1) \sim (x_2, y_2) \Leftrightarrow x_1 \equiv x_2 \pmod{k} \wedge y_1 \equiv y_2 \pmod{k}.$$

Како је број каласа еквиваленције коначан (једнак k^2) а решења једначине (1) има бесконачно много, постоје бар два решења (x_1, y_1) и (x_2, y_2) ове једначине таква да важи:

$$x_1 \equiv x_2 \pmod{k},\; y_1 \equiv y_2 \pmod{k} \quad \text{и} \quad |y_1| \neq |y_2|.$$

Из $x_1^2 - Dy_1^2 = k$ и $x_2^2 - Dy_2^2 = k$, следи да је

$$k^2 = \left(x_1^2 - Dy_1^2\right)\left(x_2^2 - Dy_2^2\right) = \left(x_1x_2 - Dy_1y_2\right)^2 - D\left(x_1y_2 - x_2y_1\right)^2.$$

Пошто је

$$x_1x_2 - Dy_1y_2 \equiv x_1^2 - Dy_1^2 \equiv 0 \pmod{k}$$

и

$$x_1y_2 - x_2y_1 \equiv x_1y_2 - x_1y_2 \equiv 0 \pmod{k},$$

постоје цели бројеви X и Y такви да је $x_1x_2 - Dy_1y_2 = kX$ и $x_1y_2 - x_2y_1 = kY$. Сада имамо да је $X^2 - DY^2 = 1$. Остаје још да се провери да је $(X, Y) \neq (1, 0)$ и $(X, Y) \neq (-1, 0)$. Ако би било $(X, Y) = (1, 0)$ или $(X, Y) = (-1, 0)$, имали бисмо да је $x_1y_2 - x_2y_1 = 0$ и $x_1x_2 - Dy_1y_2 = \pm k$. Ако саберемо прву једначину, помножену са x_2, и другу, помножену са $-y_2$, добијамо да је $y_1\left(Dy_2^2 - x_2^2\right) = \pm k$ тј. $-ky_1 = \pm ky_2$, одакле следи да је $y_1 = \pm y_2$, што је немогуће због $|y_1| \neq |y_2|$. Пошто сваки од парова (X, Y), $(-X, Y)$, $(X, -Y)$, $(-X, -Y)$ представља решење дате једначине и бар један од њих је пар природних бројева овај део теореме је доказан.

б) Ако је $x^2 - Dy^2 = 1$ и $\left(x + y\sqrt{D}\right)^n = x_n + y_n\sqrt{D}$, тада је и $\left(x - y\sqrt{D}\right)^n = x_n - y_n\sqrt{D}$, одакле следи да је

$$\begin{aligned} x_n^2 - Dy_n^2 &= \left(x_n + y_n\sqrt{D}\right)\left(x_n - y_n\sqrt{D}\right) \\ &= \left(x + y\sqrt{D}\right)^n \left(x - y\sqrt{D}\right)^n \\ &= \left(x^2 - Dy^2\right)^n = 1. \end{aligned}$$

в) Пошто су x, y, x', y' природни бројеви важи следећи низ еквиваленција:

$$y < y' \Leftrightarrow y^2 < y'^2 \Leftrightarrow Dy^2 + 1 < Dy'^2 + 1 \Leftrightarrow x^2 < x'^2 \Leftrightarrow x < x'.$$

Ако је $x < x'$ и $y < y'$, тада је очигледно

$$x + y\sqrt{D} < x' + y'\sqrt{D}.$$

Обрнуто, ако је

$$x + y\sqrt{D} < x' + y'\sqrt{D},$$

онда је и

$$\frac{1}{x - y\sqrt{D}} < \frac{1}{x' - y'\sqrt{D}},$$

тј.

$$x' - y'\sqrt{D} < x - y\sqrt{D},$$

па је и

$$\left(x + y\sqrt{D}\right) + \left(x' - y'\sqrt{D}\right) < \left(x' + y'\sqrt{D}\right) + \left(x - y\sqrt{D}\right),$$

одакле следи да је $y < y'$.

Дакле, минимално решење (у скупу свих решења) дате једначине је пар (x_0, y_0) природних бројева такав да било x_0, било y_0 или пак $x_0 + y_0\sqrt{D}$ има најмању вредност.

г) Претпоставимо да постоји решење (x, y) које је различито од свих (x_n, y_n), $n \in \{0, 1, 2, 3, \dots\}$. Тада за неко n важи:

$$\begin{aligned}
& x_n + y_n\sqrt{D} < x + y\sqrt{D} < x_{n+1} + y_{n+1}\sqrt{D} \\
\Leftrightarrow \quad & \left(x_0 + y_0\sqrt{D}\right)^n < x + y\sqrt{D} < \left(x_0 + y_0\sqrt{D}\right)^{n+1} \\
\Leftrightarrow \quad & 1 < \left(x + y\sqrt{D}\right)\left(x_0 - y_0\sqrt{D}\right)^n < x_0 + y_0\sqrt{D}
\end{aligned}$$

Ако ставимо да је

$$x' + y'\sqrt{D} = \left(x + y\sqrt{D}\right)\left(x_0 - y_0\sqrt{D}\right)^n,$$

имамо да је

$$1 < x' + y'\sqrt{D} < x_0 + y_0\sqrt{D}.$$

Пошто је и

$$x' - y'\sqrt{D} = \left(x - y\sqrt{D}\right)\left(x_0 + y_0\sqrt{D}\right)^n,$$

добијамо да је $x'^2 - Dy'^2 = 1$, тј. пар (x', y') је решење дате једначине. Из $0 < x' - y'\sqrt{D}$, закључујемо да је $x' > 0$ и $y' > 0$, што је немогуће јер из $x' + y'\sqrt{D} < x_0 + y_0\sqrt{D}$ следи да (x_0, y_0) није минимално решење. ■

Ефективно, до решења једначине $x^2 - Dy^2 = 1$, долазимо тако што најпре одредимо најмањи природан број y_0 такав да је $Dy_0^2 + 1$ потпун квадрат (израчунавањем вредности израза $Dy^2 + 1$ редом за $y = 1$, $y = 2$,...); на тај начин долазимо до минималног решења.

Ево минималних решења Пелове једначине за $D \leqslant 17$:

D	(x_0, y_0)
2	$(3, 2)$
3	$(2, 1)$
5	$(9, 4)$
6	$(5, 2)$
7	$(8, 3)$
8	$(3, 1)$
10	$(19, 6)$
11	$(10, 3)$
12	$(7, 2)$
13	$(649, 180)$
14	$(15, 4)$
15	$(4, 1)$
17	$(33, 8)$

Примећујемо да већ за $D = 13$ треба извести дуго рачунање. За $D = 109$ минимално y за које је $Dy^2 + 1$ потпун квадрат је $y = 15\,140\,424\,455\,100$ што показује да је овај метод прилично непрактичан.

ПРИМЕР 5.10. *Основно решење једначине* $x^2 - 2y^2 = 1$ *је* $x_1 = 3$, $y_1 = 2$, *па су сва решења дате једначине у скупу природних бројева дата са*

$$x_n + y_n\sqrt{2} = \left(3 + 2\sqrt{2}\right)^n.$$

Рекурзивне релације којим се (x_n, y_n) *изражава преко* (x_{n-1}, y_{n-1}), *у овом случају су:*

$$x_n = 3x_{n-1} + 4y_{n-1}, \quad y_n = 2x_{n-1} + 3y_{n-1}, \quad n > 1.$$

Дакле,

$$x_2 = 3 \cdot 3 + 4 \cdot 2 = 17, \quad y_2 = 2 \cdot 3 + 3 \cdot 2 = 12;$$

$$x_3 = 3 \cdot 17 + 4 \cdot 12 = 99, \quad y_3 = 2 \cdot 17 + 3 \cdot 12 = 70;$$

$$x_4 = 3 \cdot 99 + 4 \cdot 70 = 577, \quad y_4 = 2 \cdot 99 + 3 \cdot 70 = 408;$$

$$\vdots$$

ПРИМЕР 5.11. *Једначина* $x^2 - (a^2 - 1)y^2 = 1$, $a \in \mathbb{N}$, *има основно решење* $(a, 1)$. *Такође,* $(2a^2 + 1, 2a)$ *је основно решење једначине* $x^2 - (a^2 + 1)y^2 = 1$, $a \in \mathbb{N}$.

Оставља се читаоцима да докажу да су сва решења једначине $x^2 - Dy^2 = 1$ дата са

$$\left.\begin{aligned} x_n &= \frac{\left(x_1 + y_1\sqrt{D}\right)^n + \left(x_1 - y_1\sqrt{D}\right)^n}{2} \\ y_n &= \frac{\left(x_1 + y_1\sqrt{D}\right)^n - \left(x_1 - y_1\sqrt{D}\right)^n}{2} \end{aligned}\right\}, \qquad n \in \mathbb{N},$$

где је (x_1, y_1) минимално решење дате једначине. Доказати, затим, везу између $n-$тог решења (x_n, y_n) и $n-1-$ог решења (x_{n-1}, y_{n-1}):

$$x_n = x_1 x_{n-1} + D y_1 y_{n-1} \quad \text{и} \quad y_n = y_1 x_{n-1} + x_1 y_{n-1}.$$

ПРИМЕР 5.12. *Такозвана* ***неīаīивна Пелова једначина*** $x^2 - Dy^2 = -1$ *нема увек решења у скуӣу ӣриродних бројева. Међуӣим, уколико ова једначина има решења* (x_0, y_0) *у скуӣу ӣриродних бројева, онда она има бесконачно мноīо решења* (x_n, y_n)*, ӣри чему је* $x_n + y_n\sqrt{D} = \left(x_0 + y_0\sqrt{D}\right)^{2n-1}$*,* $n \in \mathbb{N}$.

5.3. Задаци

191. Петар и Наташа станују у солитеру у којем на сваком спрату има по 10 станова. Станови почињу од првог спрата и нумерисани су бројевима $1, 2, \ldots$. Петар станује на спрату чији је број једнак броју стана у којем је Наташа. Збир бројева њихових станова је 239. Који је број стана у којем станује Петар?

Решење. Нека Петар станује на спрату $x+1$ $(x \geqslant 0)$. Тада је број његовог стана $10x + y$, где је $1 \leqslant y \leqslant 10$. Наташа станује у стану број $x+1$. Према услову задатка је $10x + y + x + 1 = 239$, односно $11x = 238 - y$. С обзиром на то да је $1 \leqslant y \leqslant 10$, једино целобројно решење ове једначине је $x = 21$, $y = 7$. Дакле, Петар станује у стану број 217.

192. У соби се налазе столице са 3 и са 4 ноге. Када на све столице седну људи, у соби је укупно 69 ногу. Колико у соби има столица са три ноге, а колико са четири?

Решење. Нека је x број столица са три, а y број столица са четири ноге. Према услову задатка, имамо да је

$$3x + 4y + 2(x + y) = 69, \quad \text{тј.} \quad 5x + 6y = 69.$$

Како су x и y ненегативни цели бројеви, имамо да $3 \mid x$, тј. $x = 3m$, за неко m. Сада имамо да је $5 \cdot 3m + 6y = 69$ тј. $5m + 2y = 23$. Из последње једначине закључујемо да је $5m = 23 - 2y$, тј. да $5 \mid 23 - 2y$. Дакле, $23 - 2y \in \{0, 5, 10, 15, 20\}$.

Случајеви $23 - 2y = 0$, $23 - 2y = 10$ и $23 - 2y = 20$ су немогући јер y мора бити цео број.

Дакле, $23 - 2y = 5$, тј. $y = 9$ или $23 - 2y = 15$, тј. $y = 4$.

Задатак има два решења: три столице са три ноге и девет столица са четири ноге или девет столица са три ноге и четири столице са четири ноге.

193. Дванаест хлебова подељено је на дванаест људи. Сваки мушкарац добио је по два хлеба, жена по пола хлеба, а свако дете по четвртину хлеба. Колико је било мушкараца, колико жена, а колико деце?

Решење. Нека је m број мушкараца, z број жена, а d број деце (m, z, d су ненегативни цели бројеви). Према условима задатка имамо да је

$$m + z + d = 12$$

и

$$2m + \frac{1}{2}z + \frac{1}{4}d = 12, \quad \text{тј.} \quad 8m + 2z + d = 48.$$

Из друге једначине најпре примећујемо да $2 \mid d$, тј. да је $d = 2k$, за неко k, па је

$$8m + 2z + 2k = 48, \quad \text{тј.} \quad 4m + z + k = 24.$$

Пошто је $z = 12 - m - 2k$, имамо да је

$$4m + (12 - m - 2k) + k = 24, \quad \text{тј.} \quad 3m - k = 12.$$

Из последње једнакости следи да $3 \mid k$. Како је $0 \leqslant d < 12$, имамо да је $0 \leqslant k < 6$, тј. $k = 0$ или $k = 3$.

Ако је $k = 0$, деце није било, док је било четири мушкарца и осам жена.

Ако је $k = 3$, било је шесторо деце, пет мушкараца и једна жена.

194. На колико начина се 380 динара може поделити двојици браће, тако да старији добија само новчанице од 50 динара, а млађи само новчанице од 20 динара?

Решење. Нека је x број новчаница од 50 динара које треба да добије старији брат, а y број новчаница од 20 динара које треба да добије млађи $(x, y \geqslant 0)$. Тада је

$$50x + 20y = 380, \quad \text{тј.} \quad 5x + 2y = 38.$$

Из последње једнакости следи да $2 \mid x$, па нека је $x = 2z$, за неко z. Тада је $5z + y = 19$. Дакле, $5z = 19 - y \in \{0, 5, 10, 15\}$.

За $z = 0$ имамо да је $x = 0$ и $y = 19$.

За $z = 1$ имамо да је $x = 2$ и $y = 14$.

За $z = 2$ имамо да је $x = 4$ и $y = 9$.

За $z = 3$ имамо да је $x = 6$ и $y = 4$.

Дакле, постоје четири могућности.

195. Наћи све целе бројеве x и y за које је

$$2x + 3y = 185 \quad \text{и} \quad xy > x + y.$$

Решење: $x = 91 + 3t,\ y = 1 - 2t,\ -30 < t < 0.$

196. Нека су a и b узајамно прости природни бројеви и n произвољан природан број. Доказати: ако је (x_0, y_0) решење једначине $ax + by = a^n + b^n$ онда је

$$\left[\frac{x_0}{b}\right] + \left[\frac{y_0}{a}\right] = \left[\frac{a^{n-1}}{b}\right] + \left[\frac{b^{n-1}}{a}\right].$$

Решење. Из задате једначине следи $by_0 \equiv b^n \pmod{a}$. Како су a и b узајамно прости можемо скратити са b: $y_0 \equiv b^{n-1} \pmod{a}$. Слично се доказује $x_0 \equiv a^{n-1} \pmod{b}$. Дакле, постоје цели бројеви r и s такви да је $x_0 = a^{n-1} + rb$ и $y_0 = b^{n-1} + sa$. Ако то уврстимо у задату једначину, добијамо $ab(r+s) = 0$, одакле је $s = -r$, тј. $x_0 = a^{n-1} + rb$ и $y_0 = b^{n-1} - ra$. Одатле је

$$\left[\frac{x_0}{b}\right] = r + \left[\frac{a^{n-1}}{b}\right] \quad \text{и} \quad \left[\frac{y_0}{a}\right] = -r + \left[\frac{b^{n-1}}{a}\right],$$

па следи тврђење задатка.

197. У скупу целих бројева решити једначину $x^2 - 5xy + 6y^2 = 3$.

Решење: $x^2 - 5xy + 6y^2 = 3 \Leftrightarrow (x-2y)(x-3y) = 3$
Анализом свих могућих случајева добијамо
$\mathcal{R} = \{(7,2), (-3,-2), (3,2), (-7,-2)\}$.

198. Решити у скупу природних бројева једначину

$$xyz + xy + yz + zx + x + y + z = 2\,000.$$

Решење. Како је

$$xyz + xy + yz + zx + x + y + z + 1 = (x+1)(y+1)(z+1),$$

једначина је еквивалентна са $(x+1)(y+1)(z+1) = 2\,001 = 3 \cdot 23 \cdot 29$.

199. Одредити целобројна решења једначине $p(x+y)=xy$, где је p дати прост број.

Решење. Очигледно је уређени пар $(0,0)$ решење дате једначине, а уређени пар (x,y) где је тачно један од бројева x и y једнак 0 није решење. Нека је зато $x\neq 0$ и $y\neq 0$. Из $p(x+y)=xy$ следи да $p\mid xy$, а пошто је p прост број то $p\mid x$ или $p\mid y$.

(1) $x=mp,\ m\in\mathbb{Z}, m\neq 0$. За $m=1$ добијамо $x=p$, тј. $p(p+y)=yp$, одакле је $p+y=y$. Контрадикција. Значи, $m\neq 1$. Из $p(mp+y)=mpy$ следи $y=\dfrac{mp}{m-1}$. Како је $(m-1,m)=1$ то $m-1\mid p$. Постоје следеће могућности:

(i) $m-1=1\Rightarrow m=2\Rightarrow x=2p\wedge y=2p$.

(ii) $m-1=-1\Rightarrow m=0$. Контрадикција.

(iii) $m-1=p\Rightarrow m=p+1\Rightarrow x=p(p+1)\wedge y=p+1$.

(iv) $m-1=-p\Rightarrow m=1-p\Rightarrow x=p(1-p)\wedge y=p-1$.

(2) Аналогно разматраном случају, када $p\mid y$ добијамо решења $x=p+1,\ y=p(p+1)$ и $x=p-1,\ y=p(1-p)$.

Дакле, скуп решења је:

$$\mathcal{R}=\{(0,0),(2p,2p),(p(p+1),p+1),(p+1,p(p+1)),(p(1-p),p-1),$$
$$(p-1,p(1-p))\}.$$

200. Решити у скупу природних бројева једначине:

(а) $x^2-y^2=31$; (б) $x^2-y^2=303$; (в) $x^3+x^2+x-3=0$.

Решење. (а) Пошто је 31 прост број и важи $x^2-y^2=(x-y)(x+y)$ имамо да је

$$x-y=1 \quad \text{и} \quad x+y=31$$

или

$$x-y=31 \quad \text{и} \quad x+y=1.$$

Решење првог система је $x = 16$, $y = 15$, док други систем нема решења у скупу природних бројева (што није тешко видети и без рачуна јер ако $x, y \in \mathbb{N}$ онда је $x + y > x - y$).

Дакле, једино решење дате једначине је $(16, 15)$.

(б) Пошто је $303 = 3 \cdot 101 = 1 \cdot 303$ (101 је прост број) имамо следеће могућности:

$$x - y = 3 \quad \text{и} \quad x + y = 101$$

или

$$x - y = 1 \quad \text{и} \quad x + y = 303.$$

Решавањем ових система добијамо два решења: $(52, 49)$ и $(152, 151)$.

(в) Пошто је једначина $x^3 + x^2 + x - 3 = 0$ еквивалентна са $x^3 + x^2 + x + 1 = 4$, тј. са $x^2(x + 1) + (x + 1) = 4$, односно са $(x + 1)(x^2 + 1) = 4 = 1 \cdot 4 = 2 \cdot 2$ имамо да је

$$x + 1 = 1 \quad \text{и} \quad x^2 + 1 = 4$$

или

$$x + 1 = 2 \quad \text{и} \quad x^2 + 1 = 2.$$

Дакле, једино решење је $x = 1$.

Исто решење се добија ако пођемо од $x(x^2 + x + 1) = 3 = 1 \cdot 3$.

201. Одредити све тројке (p, q, r) $(q \leqslant r)$ простих бројева за које важи $p^2 + qr = 1\,996^2$.

Решење. Дату једнакост можемо записати и овако:

$$qr = 1\,996^2 - p^2 = (1\,996 - p)(1\,996 + p).$$

Разликујемо три случаја:

1. $p = 3$: из $qr = 1\,993 \cdot 1\,999$ следи $q = 1\,993$ и $r = 1\,999$;

2. $p = 3k + 1$: тада $3 \mid 1\,996 - p$ па мора бити $q = 3$.
   Из $r = (665 - k)(1\,996 + p)$ следи $665 - k = 1$, па је $p = 1\,993$ и $r = 3\,989$;

3. $p = 3k + 2$: тада $3 \mid 1\,996 + p$ па је опет $q = 3$.
   Из $r = (1\,996 - p)(666 + k)$, како је $p \geqslant 2$, добијамо да је r сложен број, па овај случај не даје решење.

202. У скупу целих бројева решити једначине:
(1) $x^4 + y^4 = 6x^2 + 14y^2 - 53$;
(2) $x^2 + 4y^2 + z^4 = 2x - 20y - 23$.

Решење. (1) Једначина је еквивалентна са $(x^2 - 3)^2 + (y^2 - 7)^2 = 5$. Збир два квадрата једнак је 5, ако и само ако је један од тих квадрата једнак 4 а други 1, па разликујемо следеће случајеве:

$$\{(x^2 - 3)^2 = 1 \wedge (y^2 - 7)^2 = 4\} \vee \{(x^2 - 3)^2 = 4 \wedge (y^2 - 7)^2 = 1\}.$$

Решавајући добијене системе једначина, наравно у скупу целих бројева, добијамо да је скуп решења:
$\mathcal{R} = \{(2, 3), (2, -3), (-2, 3), (-2, -3)\}$.

(2) Једначина је еквивалентна са $(x - 1)^2 + (2y + 5)^2 + z^4 = 3$, што је, у скупу целих бројева могуће само ако су сви сабирци једнаки 1.

Скуп решења је:
$\mathcal{R} = \{(2, -2, 1), (2, -2, 1), (2, -3, 1), (2, -3, -1), (0, -2, 1),$
$(0, -2, -1), (0, -3, 1), (0, -3, -1)\}$.

203. У скупу целих бројева решити једначину $x^2 - xy + 2x - 3y = 6$.

Решење: $x^2 + 2x - 6 = 3y + xy \Leftrightarrow x^2 + 2x - 6 = (3 + x)y$. Пошто $x = -3$ не може бити решење дате једначине, због

$$x^2 + 2x - 6 = (x - 1)(x + 3) - 3 \quad \text{(дељење полинома)},$$

имамо да је
$$y = x - 1 - \frac{3}{x+3},$$
па су могуће вредности за $x+3$ бројеви из $\{-3,-1,1,3\}$. Четири случаја који могу да наступе дају да је скуп решења дате једначине $\mathcal{R} = \{(-2,-6),(-4,-2),(0,-2),(-6,-6)\}$.

204. У скупу природних бројева решити једначину
$$2x^2 - xy - y^2 + 2x + 7y = 84.$$

Решење: $(x,y) \in \{(6,1),(13,14)\}$.

205. Одредити све двоцифрене природне бројеве са особином да је њихова вредност једнака квадрату збира цифара.

Решење. Нека је тражени број $\overline{xy}$, при чему је $x \in \{1,2,\ldots,9\}$, $y \in \{0,1,\ldots,9\}$. Тада је $(x+y)^2 = 10x+y$. Како је $x+y \neq 0$ добијамо
$$x+y = \frac{10x+y}{x+y} = 1 + \frac{9x}{x+y}\,,$$
па $x+y$ може узимати вредности $1,3,9,x,3x,9x$. За добијене вредности је онда $x+y$ такође једнако, редом $1+9x, 1+3x, 1+x, 10, 4, 2$. Дакле, добијамо једначине $1+9x=1$, $1+3x=3$, $1+x=9$, $10=x$, $4=3x$ и $2=9x$. Од решења свих тих једначина, једино $x=8$ задовољава услове задатка. Тада је $y=1$, па је тражени број 81.

206. Решити једначину $y^4 = 1 + x(x+1)(x+2)(x+3)$ у скупу целих бројева.

Решење:
$$\begin{aligned}
& y^4 - x(x+1)(x+2)(x+3) = 1 \\
\Leftrightarrow\ & y^4 - (x^2+3x)(x^2+3x+2) = 1 \\
\Leftrightarrow\ & y^4 - (x^2+3x+1-1)(x^2+3x+1+1) = 1
\end{aligned}$$

$$\begin{aligned}
&\Leftrightarrow \quad y^4 - (x^2 + 3x + 1)^2 + 1 = 1 \\
&\Leftrightarrow \quad y^4 - (x^2 + 3x + 1)^2 = 0 \\
&\Leftrightarrow \quad (y^2 - x^2 - 3x - 1)(y^2 + x^2 + 3x + 1) = 0 \\
&\Leftrightarrow \quad x^2 + 3x + 1 - y^2 = 0 \vee x^2 + 3x + 1 + y^2 = 0.
\end{aligned}$$

Посматрајући дискриминанте $D_1 = 9-4+4y^2$ и $D_2 = 9-4-4y^2$ редом квадратних једначина (по x)

$$x^2 + 3x + 1 - y^2 = 0 \quad \text{и} \quad x^2 + 3x + 1 + y^2 = 0,$$

закључујемо, најпре, да мора бити $5 + 4y^2 \geqslant 0$ и $5 - 4y^2 \geqslant 0$. Услов $5+4y^2 \geqslant 0$ је увек задовољен. Такође, захтевамо да важи $5+4y^2 = k^2$, за неки цео број k. Решавајући у скупу целих бројева, једначину $k^2 - 4y^2 = 5$, тј. $(k-2y)(k+2y) = 5$ добијамо следеће случајеве:

$$\begin{aligned}
&k - 2y = 1,\ k + 2y = 5 \Rightarrow y = 1, \\
&k - 2y = 5,\ k + 2y = 1 \Rightarrow y = -1, \\
&k - 2y = -1,\ k + 2y = -5 \Rightarrow y = -1, \\
&k - 2y = -5,\ k + 2y = -1 \Rightarrow y = 1.
\end{aligned}$$

Из $5 - 4y^2 \geqslant 0$ следи да мора бити $|y| \leqslant \dfrac{\sqrt{5}}{2}$, $y \in \mathbb{Z}$, одакле закључујемо да $y \in \{-1, 0, 1\}$. Из $5 - 4y^2 = m^2$, $m \in \mathbb{Z}$, за $y = 0$ имамо да је $5 = m^2$, што је немогуће.

Дакле, $y = -1$ или $y = 1$.

За $y = -1$ из једначине $x^2 + 3x = 0$ добијамо да је $x = 0$ или $x = -3$, а из $x^2 + 3x + 2 = 0$ да је $x = -1$ или $x = -2$. Исте једначине (по x) добијамо и за $y = 1$.

Дакле, скуп решења дате једначине је: $\mathcal{R} = \{(0,1), (0,-1), (-1,1), (-1,-1), (-2,1), (-2,-1), (-3,1), (-3,-1)\}$.

207. Колико природних бројева има особину да је $n^2 + 3n + 24$ потпун квадрат целог броја?

Решење. Нека је $n^2 + 3n + 24 = m^2$. Тада добијамо квадратну једначину по n:

$$n^2 + 3n + 24 - m^2 = 0.$$

Да би n био цео број дискриминанта мора бити потпун квадрат, па је

$$9 - 4(24 - m^2) = k^2, \quad \text{тј.} \quad 4m^2 - k^2 = 87,$$

односно

$$(2m - k)(2m + k) = 87.$$

Могући случајеви су да $2m - k$ узима редом вредности:

$$1, 3, 29, 87, -1, -3, -29, -87,$$

а $2m + k$ редом вредности:

$$87, 29, 3, 1, -87, -29, -3, -1.$$

Одавде је $4m \in \{88, 32, -88, -32\}$, тј. $m \in \{22, 8, -22, -8\}$, па је $n \in \{5, -8, 20, -23\}$. Како n мора бити природан број, то имамо два решења: $n = 5$ или $n = 20$.

208. Колико има парова (m, n) целих бројева за које важи једнакост $m^3 + 6m^2 + 5m = 8n^3 + 36n^2 + 40n + 8$?

Решење. Оваквих парова нема. Лева страна дате једнакости може да се напише у еквивалентном облику $m(m + 1)(m + 5)$, а десна у облику $(2n + 1)(2n + 2)(2n + 6) - 4$, па је лева страна увек дељива са 3, а десна никада.

209. Доказати да једначине:
(1) $3x^2 + 5y^2 = 4\,444$;
(2) $15x^2 - 7y^2 = 9$;
(3) $5^x + 6^y = 234\,567$;
немају решења у скупу $\mathbb{Z}$.

Решење. (1) За сваки $n \in \mathbb{N}$ имамо $n^2 \equiv r \pmod{10}$, при чему $r \in \{0,1,4,5,6,9\}$. Дакле, ако је (x,y) једно решење дате једначине имамо: $3x^2 \equiv a \pmod{10}$, $a \in \{0,3,2,5,8,7\}$ и $5y^2 \equiv b \pmod{10}$, $b \in \{0,5\}$, па из таблице

$+_{10}$	0	5
0	0	5
2	2	7
3	3	8
5	5	0
7	7	2
8	8	3

закључујемо да је $3x^2 + 5y^2 \equiv c \pmod{10}$, $c \in \{0,2,3,5,7,8\}$, а важи $4\,444 \equiv 4 \pmod{10}$. Једначина, дакле, нема решења.

(2) Ако је (x,y) решење дате једначине закључујемо да $3 \mid y$, тј. да је $y = 3y_1$, за неко $y_1 \in \mathbb{Z}$. Сада једначина постаје $15x^2 - 63y_1^2 = 9$, тј. $5x^2 - 21y_1^2 = 3$, те $3 \mid x$, тј. $x = 3x_1$, $x_1 \in \mathbb{Z}$. Даље, једначина постаје $45x_1^2 - 21y_1^2 = 3$, тј. $15x_1^2 - 7y_1^2 = 1$, одакле следи да је $y_1^2 \equiv -1 \equiv 2 \pmod{3}$, што је немогуће јер за сваки $k \in \mathbb{Z}$, $k^2 \equiv 0$ или $1 \pmod{3}$. Дакле, ни ова једначина нема решења.

(3) Ако је $x < 0$ или $y < 0$, бар један од бројева 5^x или 6^y је мањи од 1. У сваком случају вредност израза $5^x + 6^y$ није цео број. Даље, за $x = 0$ добијамо да је $6^y = 234\,566$, што је немогуће јер $3 \mid 6^y$ али $3 \nmid 234\,566$. Слично, за $y = 0$ било би $5^x = 234\,566$, што је немогуће, јер је $5^x \equiv 5 \pmod{10}$, а $234\,566 \equiv 6 \pmod{10}$. Дакле, мора бити $x > 0$ и $y > 0$. Међутим, $5^x \equiv 5 \pmod{10}$ и $6^y \equiv 6 \pmod{10}$, па је $5^x + 6^y \equiv 1 \pmod{10}$, те једначина нема решења.

210. Доказати да једначина $x^2 + y^2 + z^2 = 2\,007$ нема решења у скупу целих бројева.

Решење. Квадрати целих бројева при дељењу са 4 дају остатак 0 (када је број паран) или 1 (када је број непаран).

Како је $2\,007 \equiv 3 \pmod 4$ то сва три броја x, y, z морају бити непарна, тј. $x = 2x_1 + 1$, $y = 2y_1 + 1$ и $z = 2z_1 + 1$, где су x_1, y_1, z_1 такође цели бројеви. Тада је

$$4x_1^2 + 4x_1 + 1 + 4y_1^2 + 4y_1 + 1 + 4z_1^2 + 4z_1 + 1 = 2\,007,$$

тј.

$$x_1(x_1 + 1) + y_1(y_1 + 1) + z_1(z_1 + 1) = 501.$$

Лева страна последње једначине је паран број, а десна непаран, па једначина нема решења у скупу целих бројева.

211. Одредити природне бројеве $x_1, x_2, \ldots, x_{1984}$ такве да је

$$x_1^2 + x_2^2 + \cdots + x_{1984}^2 = 2\,006.$$

Решење. Нека је $x_1 = x_2 = \cdots = x_k = 1$ и $x_{k+1} \geqslant 2, \ldots, x_{1984} \geqslant 2$. Тада је

$$k + x_{k+1}^2 + \cdots + x_{1984}^2 = 2\,006, \quad x_{k+1}^2 + \cdots + x_{1984}^2 \geqslant (1\,984 - k) \cdot 4,$$

па је $2\,006 \geqslant k + (1\,984 - k) \cdot 4$, одакле је $k \geqslant 1\,976$.

Дакле, $x_1 = x_2 = \cdots = x_{1976} = 1$, па је збир квадрата преосталих осам бројева

$$x_{1977}^2 + x_{1978}^2 + \cdots + x_{1984}^2 = 2\,006 - 1\,976 = 30.$$

Очигледно је да вредност сваког од ових осам бројева мора бити мања од 5. Нека је међу њима a јединица, b двојки, c тројки и d четворки. Тада је $a + b + c + d = 8$ и $a + 4b + 9c + 16d = 30$, па је $3b + 8c + 15d = 22$. Како је $3b + 15d = 22 - 8c$, то $22 - 8c$ мора бити дељиво са 3, а то је испуњено само за $c = 2$. Тада је $3b + 15d = 6$, одакле је очигледно $b = 2$ и $d = 0$. Сада се лако добија да је $a = 4$. Према томе,

$x_1 = x_2 = \cdots = x_{1976} = x_{1977} = x_{1978} = x_{1979} = x_{1980} = 1$,
$x_{1981} = x_{1982} = 2$, $x_{1983} = x_{1984} = 3$.

Дакле, решење дате једначине је било која пермутација скупа $\{1, 1, \ldots, 1, 2, 2, 3, 3\}$, где има тачно 1 980 јединица.

212. Доказати да једначина $x^2 + y^3 = z^2$ у скупу природних бројева има бесконачно много решења.

Решење. Да би (x, y, z) било решење, довољно је да задовољава нпр. $z - x = y$ и $z + x = y^2$. Одатле је $x = \dfrac{y^2 - y}{2}$ и $z = \dfrac{y^2 + y}{2}$. Пошто су y и y^2 увек исте парности, један бесконачан скуп решења је

$$\left\{ \left(\frac{n^2 - n}{2}, n, \frac{n^2 + n}{2} \right) : n \in \mathbb{N} \right\}.$$

213. Постоје ли цели бројеви x и yтакви да задовољавају једнакост $x^2 + x = y^4 + y^3 + y^2 + y$?

Решење. Множењем дате једначине са 4 и додавањем броја 1 левој и десној страни добија се $4x^2 + 4x + 1 = 4y^4 + 4y^3 + 4y^2 + 4y + 1$, па је

$$\begin{aligned}(2x+1)^2 &= 4y^4 + 4y^3 + 4y^2 + 4y + 1 = 4y^4 + 4y^3 + y^2 + 3y^2 + 4y + 1 \\ &= \left(2y^2 + y\right)^2 + (y+1)(3y+1)\end{aligned}$$

и

$$\begin{aligned}(2x+1)^2 &= 4y^4 + 4y^3 + 4y^2 + 4y + 1 \\ &= 4y^4 + y^2 + 4 + 4y^3 + 8y^2 + 4y - 5y^2 - 3 \\ &= \left(2y^2 + y + 2\right)^2 - 5y^2 - 3.\end{aligned}$$

Дакле,

$$\left(2y^2 + y\right)^2 + (y+1)(3y+1) = (2x+1)^2 = \left(2y^2 + y + 2\right)^2 - (5y^2 + 3).$$

Сада разликујемо две могућности:

1. $y = -1 \Rightarrow x^2 + x = 0 \Rightarrow x = 0 \vee x = -1$.
2. $y \in \mathbb{Z}, y \neq -1$. Тада је за $(y+1)(3y+1) > 0$ и $5y^2+3 > 0$, па је

$$\left(2y^2 + y\right)^2 < (2x+1)^2 < \left(2y^2 + y + 2\right)^2 .$$

Како између $\left(2y^2 + y\right)^2$ и $\left(2y^2 + y + 2\right)^2$ постоји само један потпун квадрат, $\left(2y^2 + y + 1\right)^2$, то је $(2x+1)^2 = \left(2y^2 + y + 1\right)^2$. Према томе,

$$\begin{aligned} 4y^4 + 4y^3 + 4y^2 + 4y + 1 &= (2x+1)^2 = \left(2y^2 + y + 1\right)^2 \\ &= 4y^4 + y^2 + 1 + 4y^3 + 4y^2 + 2y, \end{aligned}$$

па је $y^2 - 2y = 0$, одакле је $y = 0$ или $y = 2$. Ако је $y = 0$, онда је $x^2 + x = 0$, тј. $x = 0$ или $x = -1$. Ако је $y = 2$, онда је $x^2 + x = 30$, па је $x = 5$ или $x = 6$.

Дакле, скуп решења је:

$$\mathcal{R} = \{(0,-1), (-1,-1), (0,0), (-1,0), (5,2), (6,2)\}.$$

214. Решити једначину $x^2 + y^2 + z^2 = 2xyz$.

Решење. Нека је (x, y, z) једно решење дате једначине. Лако се види да је од бројева x, y, z тачно један паран или су сви парни. Међутим, уколико би наступио први случај, на пример, ако би било $x = 2x_1$, $y = 2y_1 + 1$, $z = 2z_1 + 1$, $x_1, y_1, z_1 \in \mathbb{Z}$, имали бисмо да је

$$4x_1^2 + 4y_1^2 + 4y_1 + 1 + 4z_1^2 + 4z_1 + 1 = 4x_1(2y_1+1)(2z_1+1),$$

тј.

$$\text{„десна страна“} \equiv 0 \pmod 4 \quad \text{а} \quad \text{„лева страна“} \equiv 2 \pmod 4.$$

Контрадикција. Дакле, сваки од бројева x, y, z мора бити паран, тј. $x = 2x_1$, $y = 2y_1$, $z = 2z_1$, $x_1, y_1, z_1 \in \mathbb{Z}$, па дата једначина постаје

$$x_1^2 + y_1^2 + z_1^2 = 4x_1y_1z_1.$$

Слично се може закључити да сваки од бројева x_1, y_1, z_1 мора бити паран, тј. $x_1 = 2x_2$, $y_1 = 2y_2$, $z_1 = 2z_2$, $x_2, y_2, z_2 \in \mathbb{Z}$, па дата једначина постаје

$$x_2^2 + y_2^2 + z_2^2 = 8x_2y_2z_2.$$

Настављајући овај поступак даље можемо наћи низове $x_1, x_2, \ldots$, $y_1, y_2, \ldots$, $z_1, z_2, \ldots$ целих бројева тако да важи:

$$x = 2x_1 = 2^2x_2 = 2^3x_3 = \cdots = 2^nx_n = \cdots$$

$$y = 2y_1 = 2^2y_2 = 2^3y_3 = \cdots = 2^ny_n = \cdots$$

$$z = 2z_1 = 2^2z_2 = 2^3z_3 = \cdots = 2^nz_n = \cdots$$

тј. за свако $n \in \mathbb{N}$, $2^n \mid x$, $2^n \mid y$, $2^n \mid z$, што је једино могуће у случају да је $x = y = z = 0$.

215. (Национална математичка олимпијада–регионална рунда, Бугарска 1997) Доказати да једначина

$$x^2 + y^2 + z^2 + 3(x + y + z) + 5 = 0$$

нема решења у скупу рационалних бројева.

Решење. Дата једначина може се написати у облику

$$(2x + 3)^2 + (2y + 3)^2 + (2z + 3)^2 = 7.$$

Она има решења у скупу рационалних бројева ако и само ако постоје цели бројеви a, b, c и m такви да је

$$a^2 + b^2 + c^2 = 7m^2.$$

Претпоставимо да такви бројеви постоје и нека је m најмање могуће. Ако је m паран број, $m = 2n$, тада је $a^2 + b^2 + c^2$ дељиво са 4 и лако се проверава да тада бројеви a, b, c морају бити парни, тј. $a = 2a_1$,

$b = 2b_1$, $c = 2c_1$ и $a_1^2 + b_1^2 + c_1^2 = 7n^2$, што је контрадикција са претпоставком о минималности m.
Ако је m непаран број, тада је $m^2 \equiv 1 \pmod 8$, па је

$$a^2 + b^2 + c^2 \equiv 7 \ (\mathrm{mod}\ 8),$$

што је немогуће.

216. (Национална математичка олимпијада–регионална рунда, Бугарска 1998) Доказати да једначина $x^2y^2 = z^2(z^2 - x^2 - y^2)$ нема решења у скупу природних бројева.

Решење. Претпоставимо супротно и посматрајмо решење (x, y, z) такво да је количник $\dfrac{xy}{z}$ (што је природан број) најмањи могућ.

Запишимо бројеве x, y, z у облику $x = dx_1$, $y = dy_1$ и $z = dz_1$, где је $d =$ НЗД(x, y, z). Онда је дата једначина еквивалентна са

$$x_1^2y_1^2 = z_1^2(z_1^2 - x_1^2 - y_1^2).$$

Нека је $u = (x_1, z_1)$, $v = (y_1, z_1)$, $x_1 = ut$, $y_1 = vw$. Пошто z_1 дели x_1y_1, то је $z_1 = uv$. Отуда је $(u^2 + w^2)(v^2 + t^2) = 2u^2v^2$.

Даље имамо $(u, w) = 1$, $(v, t) = 1$ пошто је $(x_1, y_1, z_1) = 1$, па је или $u^2 + w^2 = v^2$, $v^2 + t^2 = 2u^2$ или $u^2 + w^2 = 2v^2$, $v^2 + t^2 = u^2$. Не умањујући општост можемо претпоставити да важи први пар једнакости. Тада је лако видети да су v и u непарни цели бројеви. Даље из $u^2 + w^2 = v^2$ следи да је $u = m^2 - n^2$, $w = 2mn$, $v = m^2 + n^2$, где су m и n узајамно прости природни бројеви различите парности. Замењујући ове изразе за u и v у $v^2 + t^2 = 2u^2$ добијамо

$$t^2 + (2mn)^2 = (m^2 - n^2)^2,$$

па је $t = p^2 - q^2$, $mn = pq$, $m^2 - n^2 = p^2 + q^2$ за неке природне бројеве p и q. Према томе,

$$p^2q^2 = m^2(m^2 - p^2 - q^2)$$

одакле следи да је (p, q, m) решење дате једначине. Али,

$$\frac{pq}{m} = n < d(p^2 - q^2)2mn = \frac{xy}{z},$$

што је контрадикција.

217. Одредити све природне бројеве n такве да једначина

$$x^3 + y^3 + z^3 = nx^2y^2z^2$$

има решења у скупу природних бројева.

Решење. Нека је n природан број такав да је $x^3 + y^3 + z^3 = nx^2y^2z^2$ за неке x, y, z при чему је $x \leqslant y \leqslant z$. Тада је

$$z = nx^2y^2 - \frac{x^3 + y^3}{z^2}, \tag{1}$$

па пошто су n, x, y, z природни бројеви $\dfrac{x^3 + y^3}{z^2}$ је такође природан број, па је

$$x^3 + y^3 \geqslant z^2. \tag{2}$$

Пошто је $\dfrac{x}{z} \leqslant 1$ и $\dfrac{y}{z} \leqslant 1$, имајући у виду једнакост (1) добијамо $z \geqslant nx^2y^2 - (x + y)$ или

$$z^2 \geqslant (nx^2y^2 - (x + y))^2. \tag{3}$$

Формуле (2) и (3) имплицирају да је $n^2x^4y^4 < 2nx^2y^2(x+y) + x^3 + y^3$, а после дељења са nx^3y^3,

$$nxy < 2\left(\frac{1}{x} + \frac{1}{y}\right) + \frac{1}{nx^3} + \frac{1}{ny^3}. \tag{4}$$

Ако је $x \geqslant 2$, тада је десна страна последње неједнакости мања од 3, док лева страна није мања од 4. Дакле, $x = 1$. Сада, неједнакост (4) постаје

$$ny < 2 + \frac{2}{y} + \frac{1}{n} + \frac{1}{ny^3}. \tag{5}$$

Ако је $y \geqslant 4$ десна страна последње неједнакости је мања од 4, па је $y \leqslant 3$.

Раније смо видели да $\dfrac{x^3+y^3}{z^2}$ мора бити природан број. Пошто је $x = 1$, z^2 дели број $1 + y^3$. Последњи услов, заједно са $z \geqslant y$ и $y \leqslant 3$, нас доводи да тројки:

1. $x = 1, y = 1, z = 1;$

2. $x = 1, y = 2, z = 3.$

Прва тројка је решење једначине $x^3 + y^3 + z^3 = nx^2y^2z^2$, у случају $n = 3$, док је друга решење дате једначине ако је $n = 1$.

Дакле, 1 и 3 су једине вредности n за које дата једначина има решења у скупу природних бројева.

218. (Национална математичка олимпијада–регионална рунда, Бугарска 1999) Решити у скупу целих бројева једначину

$$x^3 = y^3 + 2y^2 + 1.$$

Решење. Очигледно је $x > y$. Поред тога, $x < y + 1$ ако и само ако је $(y+1)^3 > y^3 + 2y^2 + 1$ ако и само ако је $y(y+3) > 0$. За $y > 0$ или $y < -3$ једначина нема решења. Дакле, y може имати вредности 0, -1, -2 или -3. Сада се лако налазе решења: $\mathcal{R} = \{(-2,-3),(1,-2),(1,0)\}$.

219. (Национална математичка олимпијада–финална рунда, Бугарска 1999) Доказати да једначина $x^3 + y^3 + z^3 + t^3 = 1\,999$ има бесконачно много решења.

Решење. Лако се проверава да ако је n цео број, тада бројеви

$$x = 10 + 60n^3, \quad y = 10 - 60n^3, \quad z = -1, \quad t = -60n^2$$

задовољавају једначину.

220. Колико има парова (x, y) целих бројева за које важи $x \leqslant y$ и $(x + y + 1\,988)^2 = x^2 + y^2 + 1\,988^2$?

Решење:

$$\begin{aligned}
& (x + y + 1\,988)^2 = x^2 + y^2 + 1\,988^2 \\
\Leftrightarrow\quad & x^2 + y^2 + 1\,988^2 + 2xy + 2 \cdot x \cdot 1\,988 + 2 \cdot y \cdot 1\,988 = \\
& \quad = x^2 + y^2 + 1\,988^2 \\
\Leftrightarrow\quad & xy + x \cdot 1\,988 + y \cdot 1\,988 + 1\,988^2 = 1\,988^2 \\
\Leftrightarrow\quad & (x + 1\,988)(y + 1\,988) = 1\,988^2 = 2^4 \cdot 7^2 \cdot 71^2
\end{aligned}$$

Број $1\,988^2$ може се записати у облику производа два цела броја на $2 \cdot 5 \cdot 3 \cdot 3 = 90$ начина. Зато и дата једначина има укупно 90 решења. Постоје два решења код којих је $x = y$: $x = y = 0$ и $x = y = -3\,976$, а код осталих 88 решења у 44 случајева је $x < y$. Дакле, има 46 парова (x, y) целих бројева који задовољавају тражене услове.

221. Одредити природне бројеве $x < y < z$, такве да важи једнакост $2^x + 2^y + 2^z = 2\,336$.

Решење. Пошто је $2\,336 = 2^5 \cdot 73$ из $2^x(1 + 2^{y-x} + 2^{z-x}) = 2^5 \cdot 73$ следи да је $x = 5$ и $1 + 2^{y-x} + 2^{z-x} = 73$, тј. $2^{y-5} + 2^{z-5} = 72 = 2^3 \cdot 3^2$. Сада имамо да је $2^{y-5}(1 + 2^{z-y}) = 2^3 \cdot 3^2$, па је $y - 5 = 3$, тј. $y = 8$ и $1 + 2^{z-y} = 3^2$. Најзад, из $2^{z-8} = 8 = 2^3$, имамо да је $z - 8 = 3$, тј. $z = 11$.

222. Решити једначину $2^x - 3^y = 7$ у скупу целих бројева.

Решење. Из $2^x = 7 + 3^y$ следи да је $2^x > 7$, тј. $x \geqslant 3$. Слично, из $3^y = 2^x - 7$ следи да је $3^y \geqslant 1$, тј. да је $y \geqslant 0$.

Како је $x \geqslant 3$ то је $2^x \equiv 0 \pmod 4$, па је и $3^y + 7 \equiv 0 \pmod 4$. Из чињенице да је $3 \equiv -1 \pmod 4$ следи да је $(-1)^y + 7 \equiv 0 \pmod 4$, па y мора бити паран број, тј. $y = 2y_1$.

Уколико је $y = 0$ тада је $2^x = 8$, па је $x = 3$.

Нека је $y > 0$. Тада је $3^y \equiv 0 \pmod 3$, па и $2^x - 7 \equiv 0 \pmod 3$. Због $2 \equiv -1 \pmod 3$ је $(-1)^x \equiv 7 \equiv 1 \pmod 3$, одакле закључујемо да је и x паран број, тј. $x = 2x_1$.

Дакле, за $x > 3$ и $y > 0$ једначина гласи:

$$2^{2x_1} - 3^{2y_1} = 7 \Leftrightarrow \left(2^{x_1} - 3^{y_1}\right)\left(2^{x_1} + 3^{y_1}\right) = 7.$$

С обзиром на то да је $2^{x_1} > 0$ и $3^{y_1} > 0$ и да је $2^{x_1} + 3^{y_1} > 2^{x_1} - 3^{y_1}$ могућ је само следећи случај:

$$2^{x_1} + 3^{y_1} = 7 \ \wedge \ 2^{x_1} - 3^{y_1} = 1,$$

одакле је

$$2 \cdot 2^{x_1} = 8 \ \wedge \ 2 \cdot 3^{y_1} = 6,$$

па је $x_1 = 2$ и $y_1 = 1$, а $x = 2x_1 = 4$ и $y = 2y_1 = 2$.

Скуп решења је $\mathcal{R} = \{(3,0),(4,2)\}$.

223. Да ли постоје природни бројеви m и n такви да важи једнакост $3^n + 7^m = 8^n$?

Решење. За сваки природан број n и све целе бројеве a и b важи $a - b \mid a^n - b^n$. Дакле, ако би за неке природне бројеве m и n било $7^m = 8^n - 3^n$, из $5 \mid 8^n - 3^n$ $(5 = 8 - 3)$, следило би да $5 \mid 7^m$, што је немогуће јер је:

$7^1 \equiv 2 \pmod 5$, $\quad 7^2 \equiv 4 \pmod 5$, $\quad 7^3 \equiv 3 \pmod 5$,
$7^4 \equiv 1 \pmod 5$, $\quad 7^5 \equiv 2 \pmod 5$, $\quad 7^6 \equiv 4 \pmod 5, \ldots.$

224. (Републичко такмичење 1991, I разред) Наћи све просте бројеве p, q, r који задовољавају једначину $p^q + q^p = r$.

Решење. Нека је један од бројева p, q, r паран (иначе долазимо до очигледне контрадикције). Како је $r \neq 2$, онда је, на пример $q = 2$ (због симетрије p и q су „равноправни“) па је

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

Један од бројева p и r мора бити дељив са 3; иначе је остатак при дељењу леве стране са 3 једнак $(\pm 1)^2 + (-1)^p = 0$ (p–непаран), а остатак при дељењу десне стране са 3 је различит од 0. Како је $r \neq 3$, јер је $p \geqslant 3$, онда је $p = 3$, $r = 17$. Дакле, има два решења за тројку (p, q, r) и то су $(3, 2, 17)$ и $(2, 3, 17)$.

225. Наћи сва целобројна решења једначине:
(1) $x^2 + 2xy - 3y^2 = 1$;
(2) $x^2 + xy + y^2 = 1$;
(3) $x^3 - y^3 = 91$;
(4) $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{2}$;
(5) $(x + y)^2 = (x + 1)(y - 1)$;
(6) $x^y - 2^z = 1$.

Решење: (1) $(x, y) \in \{(1, 0), (-1, 0)\}$;
(2) $(x, y) \in \{(0, 1), (0, -1), (1, 0), (-1, 0), (1, -1), (-1, 1)\}$;
(3) $(x, y) \in \{(4, -3), (3, -4), (6, 5), (-5, -6)\}$;
(4) $(x, y) \in \{(-2, 1), (1, -2), (3, 6), (4, 4), (6, 3)\}$;
(5) $x = -1, y = 1$.

(6) Нека је (x, y, z) решење дате једначине. Лако се види да не може бити $y \leqslant 0$ и да је за $y = 1$ свака тројка $(2^z + 1, 1, z)$, $z \in \{0, 1, 2, \dots\}$, решење дате једначине. Нека је $y > 1$. Тада је $|x| > 1$, $z > 1$, а осим тога x је непаран број и важи

$$(x - 1)(x^{y-1} + x^{y-2} + \cdots + x + 1) = 2^z.$$

Како је $x^{y-1}+x^{y-2}+\cdots+x+1$ паран број, то је $y-1=2k+1$, где је k ненегативан цео број, па следи

$$(x-1)(x+1)(x^{y-2}+x^{y-4}+\cdots+1)=2^z.$$

Број $(x-1)(x+1)$ је степен двојке са природним експонентом, ако и само ако $x\in\{-3,3\}$. За $x=3$ добијамо $9^k+9^{k-1}+\cdots+1=2^{z-3}$, тј. $2^z=9^{k+1}-1=(3^{k+1}-1)(3^{k+1}+1)$, одакле следи $k=0$, $y=2$, $z=3$, тј. решење је тројка $(3,2,3)$. За $x=-3$ добијамо решење $(-3,2,3)$.

226. У скупу природних бројева решити једначине:
(1) $x!+2y=5\,555$;
(2) $x!+2=p^2$, где је p прост број.

Решење. (1) Ако је $x=1$ онда је и $x!=1$, па је $2y=5\,554$, тј. $y=2\,777$. Ако је $x\geqslant 2$, тада је $x!$ паран број, па је и $x!+2y$ паран број, а $5\,555$ је непаран број. Према томе, једино решење једначине је $(x,y)=(1,2\,777)$.

(2) За $x=1$ добија се $p^2=3$, па једначина нема решења. За $x=2$ добија се $p=2$. За $x\geqslant 3$ је $x!$ паран број, па је и број $x!+2$ такође паран. Међутим, прост број $p>2$ је непаран, па је и p^2 непаран. Значи једино решење је $(x,p)=(2,2)$.

227. Наћи све парове природних бројева m и n таквих да важи $m!+3=n^2$.

Решење. Ако је број $m!$ дељив са 3, тј. ако је $m\geqslant 3$, имаћемо да $3\mid m!+3$, па $3\mid n^2$, одакле следи да $9\mid n^2$, па и да $9\mid m!+3$. За $m=3$, $m!+3=9=3^2$, па је $n=3$. За $m=4$, $4!+3=27$ није потпун квадрат. Такође, за $m=5$, $5!+3=123$ није потпун квадрат. За $m\geqslant 6$, $m!+3=9\cdot(\cdots)+3$, па $9\nmid m!+3$.

Ако број $m!$ није дељив са 3, тада је $m=1$ или $m=2$. За $m=1$, $m!+3=4=2^2$, па је $n=2$. За $m=2$, $m!+3=7$ није потпун квадрат.

Дакле, имамо два решења $m = 1, n = 2$ и $m = 3, n = 3$.

228. (Национална математичка олимпијада–регионална рунда, Бугарска 2002) Наћи све тројке (x, y, z) природних бројева таквих да је

$$x! + y! = 15 \cdot 2^{z!}.$$

Решење. Ако је $x \geqslant 6$ и $y \geqslant 6$ тада је $x! + y!$ дељиво са 9, док $15 \cdot 2^{z!}$ није. Дакле, можемо претпоставити да је $y \leqslant x$ и $y \leqslant 5$. Тада је

$$\frac{x!}{y!} + 1 = \frac{15 \cdot 2^{z!}}{y!}.$$

Цео број $\dfrac{15 \cdot 2^{z!}}{y!}$ је непаран само ако је $z = 1$ и у том случају је $x = 4$ и $y = 3$. Ако је $z \geqslant 2$, тада је цео број $\dfrac{x!}{y!}$ непаран, одакле следи или да је $x = y$ или $x = y + 1$ и x непаран. У првом случају 15 дели $y!$, па је $y = 5$ и $z = 4!$, што је немогуће. У другом случају добијамо или да је $y = 2, x = 3$ или $y = 4, x = 5$, што је такође немогуће. Према томе, тражене тројке су $(4, 3, 1)$ и $(3, 4, 1)$.

229. Одредити природан број x тако да је $1! + 2! + \cdots + x!$ потпун квадрат неког природног броја.

Решење. Нека је $1! + 2! + \cdots + x! = y^2$. Разликујемо следеће могућности:

(i) $x = 1 \Rightarrow y^2 = 1! = 1 \Rightarrow y = 1$

(ii) $x = 2 \Rightarrow y^2 = 1! + 2! = 3$ – у овом случају нема целобројних решења

(iii) $x = 3 \Rightarrow y^2 = 1! + 2! + 3! = 9 \Rightarrow y = 3$

(iv) $x = 4 \Rightarrow y^2 = 1! + 2! + 3! + 4! = 33$ – у овом случају нема целобројних решења

(v) $x \geqslant 5 \Rightarrow y^2 = 1! + 2! + 3! + 4! + 5! + \cdots + x! = 33 + 5! + \cdots + x!$ бројеви $5!, 6!, \ldots, x!$ се завршавају цифром 0, па је у овом случају $y^2 = 33 + 10k$, тј. број y^2 се завршава цифром 3. Контрадикција.

Дакле, $x = 1$ или $x = 3$.

230. Постоје ли природни бројеви x, y, z такви да је $x! + y! = z!$?

Решење. Очигледно је да мора бити $x < z$ и $y < z$. Тада је

$$x! + y! = z! = z(z-1)\cdots(y+1)y(y-1)\cdots 2\cdot 1 = z(z-1)\cdots(y+1)y!,$$

одакле се добија

$$x! = z(z-1)\cdots(y+1)y! - y! = y!(z(z-1)\cdots(y+1) - 1).$$

Разликујемо следеће случајеве:

(i) $x < y \Rightarrow x! < y!$ – једначина нема решења.

(ii) $x = y \Rightarrow z(z-1)\cdots(y+1) - 1 = 1$, па је $z(z-1)\cdots(y+1) = 2$ што значи да је $z = 2$, а $x = y = 1$.

(iii) $x > y$ – тада је $x \geqslant 2$ и

$$x! = x(x-1)\cdots(y+1)y! = y!(z(z-1)\cdots(y+1) - 1),$$

па се после дељења са $y!$ добија

$$x(x-1)\cdots(y+1) = z(z-1)\cdots(y+1) - 1.$$

Очигледно је да мора бити $x > y + 1$. Тада је лева страна претходне једначине увек парна, а десна непарна, па једначина нема решења.

Дакле, једино решење је $x = y = 1$, $z = 2$.

231. Ако су x, y, z различити природни бројеви решити једначину

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = 1.$$

Решење. Не умањујући општост (због симетричности једначине) можемо претпоставити да је $x > y > z$. Тада је $\frac{1}{x} < \frac{1}{y} < \frac{1}{z}$, па је

$$\frac{3}{x} < \frac{1}{x} + \frac{1}{y} + \frac{1}{z} < \frac{3}{z},$$

одакле је $\frac{3}{x} < 1$ и $\frac{3}{z} > 1$, односно $x > 3$ и $z < 3$. Очигледно је да су x, y, z различити од 1, па је због $z < 3$ једина могућност $z = 2$. Тада је $\frac{1}{x} + \frac{1}{y} = \frac{1}{2}$. Како је

$$\frac{2}{x} < \frac{1}{x} + \frac{1}{y} < \frac{2}{y},$$

па је $\frac{1}{2} < \frac{2}{y}$, одакле је $y < 4$. Како је по претпоставци $y > z$ то је $y = 3$. Сада се лако добија $x = 6$.

Дакле, решење једначине је било која пермутација скупа $\{6, 3, 2\}$.

232. Доказати да једначина

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{1}{2\,007}$$

има коначан број решења у скупу природних бројева.

Решење. Сменом $x = 2\,007a$, $y = 2\,007b$, $z = 2\,007c$ једначина се своди на

$$\frac{1}{a} + \frac{1}{b} + \frac{1}{c} = 1.$$

233. (Зимско математичко такмичење, Бугарска 1999, 8. разред) Наћи све природне бројеве x и y такве да важи:

(а) $\dfrac{1}{x} - \dfrac{1}{y} = \dfrac{1}{3}$; (б) $\dfrac{1}{x} + \dfrac{1}{y} = \dfrac{1}{3} + \dfrac{1}{xy}$.

Решење. (а) Једначина је еквивалентна са $3y - 3x = xy$, одакле је $x = 3 - \dfrac{9}{y+3}$. Према томе, $y + 3 = 9$, па је $y = 6$ и $x = 2$.

(б) Нека је $x \leqslant y$. Тада је

$$\frac{1}{3} = \frac{1}{x} + \frac{1}{y} - \frac{1}{xy} \leqslant \frac{2}{x} - \frac{1}{xy} = \frac{2y-1}{xy} < \frac{2y}{xy} = \frac{2}{x},$$

па је $x < 6$.

За $x = 1$, $x = 2$ или $x = 3$ нема решења; $x = 4$ имплицира $y = 9$ и $x = 5$ имплицира $y = 6$. Иста аргументација користи се и за случај $x \geqslant y$.

Дакле, скуп решења је: $\mathcal{R} = \{(4,9), (5,6), (6,5), (9,4)\}$.

234. У скупу природних бројева решити једначину

$$\frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{u^2} = 1.$$

Решење. Слично као у претходном задатку можемо претпоставити да је $x \leqslant y \leqslant z \leqslant u$ и тада је $\dfrac{1}{u^2} \leqslant \dfrac{1}{z^2} \leqslant \dfrac{1}{y^2} \leqslant \dfrac{1}{x^2}$, па је

$$\frac{4}{u^2} \leqslant \frac{1}{x^2} + \frac{1}{y^2} + \frac{1}{z^2} + \frac{1}{u^2} = 1 \leqslant \frac{4}{x^2}\,.$$

Сличном анализом као у претходном задатку добијамо да је једино решење једначине $x = y = z = u = 2$.

235. Доказати да за сваки природан број $n > 1$ не постоји строго растући низ природних бројева $a_1, a_2, \ldots, a_n$ такав да је

$$\frac{1}{a_1^2} + \frac{1}{a_2^2} + \cdots + \frac{1}{a_n^2} = 1.$$

Решење. Сигурно је $a_1 \neq 1$, па из $a_1 < a_2 < \cdots < a_n$ следи да је $a_1 \geqslant 2, a_2 \geqslant 3, \ldots, a_n \geqslant n+1$, па је

$$\frac{1}{a_1^2} \leqslant \frac{1}{2^2},\ \frac{1}{a_2^2} \leqslant \frac{1}{3^2},\ \ldots,\ \frac{1}{a_n^2} \leqslant \frac{1}{(n+1)^2}\,.$$

Сада је

$$\begin{aligned}
\frac{1}{a_1^2} + \frac{1}{a_2^2} + \cdots + \frac{1}{a_n^2} &\leqslant \frac{1}{2^2} + \frac{1}{3^2} + \cdots + \frac{1}{(n+1)^2} \\
&\leqslant \frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n(n+1)} \\
&= 1 - \frac{1}{2} + \frac{1}{2} - \frac{1}{3} + \cdots + \frac{1}{n} - \frac{1}{n+1} = 1 - \frac{1}{n} < 1,
\end{aligned}$$

па једначина нема решења.

236. (Зимско математичко такмичење, Бугарска 2002, 9. разред) Нађи све природне бројеве n такве да једначина

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \cdots + \frac{1}{x_n^2} = \frac{n+1}{x_{n+1}^2}$$

има решење у скупу природних бројева.

Решење. Ако је $n = 1$, једначина постаје $2 = \dfrac{x_2^2}{x_1^2}$ и, пошто је $\sqrt{2}$ ирационалан број, једначина нема решења у скупу природних бројева.

Ако је $n = 2$ имамо

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} = \frac{3}{x_3^2},$$

односно $(x_2x_3)^2 + (x_1x_3)^2 = 3(x_1x_2)^2$, тј. $a^2 + b^2 = 3c^2$ за $a = x_2x_3$, $b = x_1x_3$ и $c = x_1x_2$. Пошто су квадрати целих бројева конгруентни

0 или 1 по модулу 3, закључујемо да су a и b дељиви са 3. Нека је $a = 3a_1$ и $b = 3b_1$. После замене и скраћивања закључујемо да је и c дељиво са 3. Нека је $c = 3c_1$. Онда добијамо $a_1^2 + b_1^2 = 3c_1^2$. На исти начин се показује да су a_1, b_1 и c_1 дељиви са 3 итд. Према томе, за свако $m \in \mathbb{N}$ су бројеви a, b и c дељиви са 3^m, што је могуће само ако је $a = b = c = 0$. Контрадикција, јер је $a = x_2x_3 \neq 0$.

Покажимо сада да за $n \geqslant 3$ дата једначина има решења у скупу $\mathbb{N}$. Довољно је доказати да то важи за $n = 3$. Наиме, ако је

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} = \frac{4}{x_4^2},$$

тада је

$$\frac{1}{x_1^2} + \frac{1}{x_2^2} + \frac{1}{x_3^2} + \underbrace{\frac{1}{x_4^2} + \cdots + \frac{1}{x_4^2}}_{n-3} = \frac{n+1}{x_4^2}.$$

Да бисмо нашли решење за $n = 3$, уочимо једнакост

$$\frac{1}{15^2} + \frac{1}{20^2} = \frac{1}{12^2}.$$

Сада је

$$\left(\frac{1}{15^2} + \frac{1}{20^2}\right)\frac{1}{12^2} = \frac{1}{(12^2)^2},$$

одакле добијамо

$$\frac{1}{(15 \cdot 12)^2} + \frac{1}{(20 \cdot 15)^2} + \frac{1}{(20 \cdot 20)^2} = \frac{1}{(12^2)^2} = \frac{4}{(2 \cdot 12^2)^2}.$$

237. У скупу троуглова чије су дужине страница узастопни природни бројеви, одредити оне чија је површина природан број.

Решење. Нека су $n-1, n, n+1$ дужине страница троугла $(n > 1)$. По Хероновом обрасцу добијамо да је

$$P = \frac{n}{2}\sqrt{3\left(\left(\frac{n}{2}\right)^2 - 1\right)}.$$

Нека је $\dfrac{n}{2} = x$, $P = x\sqrt{3(x^2-1)}$. Из услова $P \in \mathbb{N}$ следи да мора бити $x^2 - 1 = 3y^2$, за неки природан број y. Решења последње (Пелове) једначине у скупу природних бројева су (x_n, y_n), где је

$$x_n : 2, 7, 26, 97, \ldots$$

$$y_n : 1, 4, 15, 56, \ldots$$

Како је $n = 2x$ $(x > 0, n > 2)$ имамо да $n \in \{4, 14, 52, 194, \ldots\}$, па су дужине страница троугла:

$$(3,4,5);\ (13,14,15);\ (51,52,53);\ (193,194,195);\ \ldots$$

238. Доказати да једначина:

(1) $x^2 - 2y^2 = -1$;

(2) $x^2 - 2y^2 = -7$;

(3) $x^2 - 2y^2 = 7$

има бесконачно много решења у скупу природних бројева.

Решење. (1) Није тешко видети да је пар $(1,1)$ решење дате једначине. Формулом

$$x_n + y_n\sqrt{2} = \left(1+\sqrt{2}\right)^{2n-1}, \quad n \in \mathbb{N},$$

дато је бесконачно много решења дате једначине. Заиста, из

$$x_n+y_n\sqrt{2} = \left(1+\sqrt{2}\right)^{2n-1} \quad \text{и} \quad x_n-y_n\sqrt{2} = \left(1-\sqrt{2}\right)^{2n-1}, \quad n \in \mathbb{N},$$

следи

$$\begin{aligned} x_n^2 - 2y_n^2 &= \left(x_n + y_n\sqrt{2}\right)\left(x_n - y_n\sqrt{2}\right) \\ &= \left(1+\sqrt{2}\right)^{2n-1}\left(1-\sqrt{2}\right)^{2n-1} = -1. \end{aligned}$$

(2) Пошто је пар $(1,2)$ решење дате једначине, бесконачно много решења (x_n, y_n), $n \in \mathbb{N}$, добијамо из

$$x_n + y_n\sqrt{2} = \left(1+2\sqrt{2}\right)\left(3+2\sqrt{2}\right)^n, \quad n \in \mathbb{N},$$

јер је $(3,2)$ решење једначине $x^2 - 2y^2 = 1$.

239. Нека је D природан број који није потпун квадрат и m цео број различит од нуле. Ако једначина $x^2 - Dy^2 = m$ има решења у скупу целих бројева, доказати да их има бесконачно много.

Решење. Нека је пар (x', y') једно решење дате једначине, тј. нека је $x'^2 - Dy'^2 = m$. Нека је, даље, са

$$x_n + y_n\sqrt{D} = \left(x_1 + y_1\sqrt{D}\right)^n, \quad n \in \mathbb{N},$$

дат низ (x_n, y_n), $n \in \mathbb{N}$, решења једначине $x^2 - Dy^2 = 1$ ((x_1, y_1) је минимално решење последње једначине). Тада није тешко доказати, да

$$x_n' + y_n'\sqrt{D} = \left(x' + y'\sqrt{D}\right)\left(x_1 + y_1\sqrt{D}\right)^n, \quad n \in \mathbb{N},$$

даје бесконачан низ $({x'}_n, {y'}_n)$, $n \in \mathbb{N}$, решења једначине $x^2 - Dy^2 = m$.

240. За дати природан број n наћи пар природних бројева (x, y) за које важи $x^2 - 5y^2 = 1\,996^n$.

Решење. Приметимо да је

$$1\,996 = 49^2 - 5 \cdot 9^2 = \left(49 - 9\sqrt{5}\right)\left(49 + 9\sqrt{5}\right).$$

Даље,

$$\begin{aligned}\left(49 - 9\sqrt{5}\right)^n &= 49^n - \binom{n}{1}49^{n-1} \cdot 9\sqrt{5} + \binom{n}{2}49^{n-2}\left(9\sqrt{5}\right)^2 \\ &\quad - \cdots + (-1)^n\left(9\sqrt{5}\right)^n,\end{aligned}$$

$$\begin{aligned}\left(49 + 9\sqrt{5}\right)^n &= 49^n + \binom{n}{1}49^{n-1} \cdot 9\sqrt{5} + \binom{n}{2}49^{n-2}\left(9\sqrt{5}\right)^2 \\ &\quad + \cdots + \left(9\sqrt{5}\right)^n.\end{aligned}$$

Одатле је $1\,996^n = \left(49 - 9\sqrt{5}\right)^n\left(49 + 9\sqrt{5}\right)^n = x^2 - 5y^2$, где је

$$\begin{aligned}x &= 49^n + \binom{n}{2}49^{n-2}\left(9\sqrt{5}\right)^2 + \cdots \\ y &= \binom{n}{1}49^{n-1} \cdot 9 + \binom{n}{3}49^{n-3} \cdot 9^3 \cdot 5 + \cdots\end{aligned}$$

241. Ако је p прост број облика $4k+1$, $k \in \mathbb{N}$, онда једначина $x^2 - py^2 = -1$ има решења у скупу природних бројева.

Решење. Нека је (x', y') минимално решење једначине $x^2 - py^2 = 1$. Дакле, $x'^2 - py'^2 = 1$. Докажимо да је y' паран број. Заиста, ако би y' био непаран број, онда бисмо имали $y'^2 \equiv 1 \pmod{4}$, па би било

$x'^2 = py'^2 + 1 \equiv 1 + 1 \equiv 2 \pmod 4$, што је немогуће. Дакле, $y' = 2y_0$, за неки природан број y_0. Из $x'^2 - 1 = 4py_0^2$ следи да је:

$$(1) \begin{cases} x' - 1 = 2pu^2 \\ x' + 1 = 2v^2 \end{cases} \quad \text{или} \quad (2) \begin{cases} x' - 1 = 2u^2 \\ x' + 1 = 2pv^2 \end{cases}$$

за неке природне бројеве u и vтакве да је $y_0 = uv$. Из (1) добијамо да је $2v^2 - 2pu^2 = 2$, тј. $v^2 - pu^2 = 1$, што је немогуће због $u \leqslant uv = y_0 < 2y_0 = y'$. Дакле, важи (2), одакле следи да је $u^2 - pv^2 = -1$.

242. Ако је D природан број облика $4k + 3$, $k \in \mathbb{N}$, доказати да једначина $x^2 - Dy^2 = -1$ нема решења у скупу природних бројева.

Решење. Квадрати природних бројева при дељењу са 4 могу давати остатак 0 или 1. Дакле, ако би дата једначина имала решења (x, y), имали бисмо да је

$$Dy^2 \equiv 0 \pmod 4 \quad \text{или} \quad Dy^2 \equiv 3 \pmod 4,$$

док је

$$x^2 + 1 \equiv 1 \pmod 4 \quad \text{или} \quad x^2 + 1 \equiv 2 \pmod 4.$$

243. Доказати да за произвољан цео број k једначина

$$x^2 - (k^2 - 1)y^2 = -1$$

нема решења у скупу целих бројева.

244. Доказати да једначине:

$$x^2 - 3y^2 = 2, \quad x^2 - 5y^2 = 2 \quad \text{и} \quad x^2 - 7y^2 = 3$$

немају решење у скупу природних бројева.

245. Доказати да постоји бесконачно много природних бројева n таквих да једначина

$$(x + y + z)^3 = n^2xyz$$

има решење у скупу природних бројева.

Решење. Потражимо решења (x, y, z) дате једначине таква да је $z = k(x+y)$, где је k природан број. Тада дату једначину можемо записати у облику

$$((x+y)+k(x+y))^3 = n^2xyk(x+y),$$

тј.

$$(k+1)^3(x+y)^2 = n^2kxy. \tag{$*$}$$

Ако једначина $(*)$ има решење за неке n и k онда је то случај и са задатом једначином. Нека је $n = 3k+3$. Тада се $(*)$ може записати у облику

$$(k+1)(x+y)^2 = 9kxy.$$

Довољно је доказати да последња једначина има решење (x, y) за бесконачно много k, или еквивалентно, да квадратна једначина по t ($t = \frac{x}{y}$)

$$(k+1)(t+1)^2 - 9kt = 0, \quad \text{тј. } (k+1)t^2 - (7k-2)t + (k+1) = 0$$

има позитивно рационално решење за бесконачно много k. Последње тврђење важи ако и само ако је дискриминанта

$$D = (7k-2)^2 - 4(k+1)^2 = 9k(5k-4)$$

потпун квадрат за бесконачно много k. Стављајући да је $k = u^2$ проблем се своди на доказивање да једначина

$$5u^2 - 4 = v^2$$

има бесконачно много решења (u, v) у скупу целих бројева, што је тачно према задатку 239.

246. (Национална математичка олимпијада–финална рунда, Бугарска 2001) Дата је једначина

$$(p+2)x^2-(p+1)y^2+px+(p+2)y=1,$$

где је p фиксиран прост број облика $4k+3$. Доказати да важи:

(а) ако је (x_0, y_0) решење једначине, $x_0, y_0 \in \mathbb{N}$, тада $p \mid x_0$;

(б) дата једначина има бесконачно много решења (x_0, y_0), где су $x_0, y_0 \in \mathbb{N}$.

Решење. (а) Обележимо $y-1=z$ и запишимо једначину у облику

$$(*) \qquad x^2=(z-x)((p+1)(z+x)+p).$$

Ако су $z-x$ и $(p+1)(z+x)+p$ узајамно прости онда су они потпуни квадрати, што је немогуће јер је број $(p+1)(z+x)+p$ облика $4k+3$. Нека је q заједнички делилац посматраних бројева. Из $(*)$ следи да $q \mid x$, а затим и да $q \mid z$. Пошто $q \mid (p+1)(z+x)+p$ имамо да $q \mid p$, тј. да је $q=p$, одакле следи тврђење.

(б) Довољно је доказати да једначина $(*)$ има бесконачно много решења у скупу природних бројева. Нека је $x=px_1$ и $z=pz_1$. Тада је

$$x_1^2=(z_1-x_1)((p+1)(z_1+x_1)+1),$$

па постоје природни бројеви a и b такви да је $z_1-x_1=a^2$, $x_1=ab$ и $(p+1)(z_1+x_1)+1=b^2$. Сада следи

$$(**) \qquad (p+2)b^2-(p+1)(a+b)^2=1.$$

Нека је

$$\left(\sqrt{p+2}+\sqrt{p+1}\right)^{2k+1}=m_k\sqrt{p+2}+n_k\sqrt{p+1}$$

за било које $k=0,1,\ldots$, где су m_k и n_k природни бројеви. Тада је очигледно

$$\left(\sqrt{p+2}-\sqrt{p+1}\right)^{2k+1}=m_k\sqrt{p+2}-n_k\sqrt{p+1}$$

и после множења добијамо да је

$$(p+2)m_k^2 - (p+1)n_k^2 = 1,$$

тј. $b = m_k$ и $a + b = n_k$ су решења једначине $(**)$. Према томе, $x = pm_k(n_k - m_k)$ и $z = pn_k(n_k - m_k)$ су решења једначине $(*)$. Тврђење (б) следи из чињенице да су оба низа $m_1, m_2, \ldots$ и $n_1, n_2, \ldots$ строго растућа.

5.4. Конгруенције вишег реда

Нека је

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0, \quad a_n \neq 0$$

полином са целобројним коефицијентима. За изабрани цео број m, ако је $a_n \not\equiv 0 \pmod{m}$, кажемо да је конгруенција

$$P(x) \equiv 0 \ (\mathrm{mod}\ m)$$

реда n по модулу m.

За $n = 1$ имамо линеарне конгруенције облика $ax \equiv b \pmod{m}$, чије је решавање еквивалентно решавању линеарне Диофантове једначине $ax - my = b$.

Конгруенције вишег реда су конгруенције реда $n \geqslant 2$. Решење те конгруенције је сваки број x за који је $m \mid P(x)$.

Број решења једнак је броју класа остатака по модулу m које задовољавају конгруенцију. Број решења конгруенције вишег реда не мора бити једнак реду конгруенције, може бити мањи, али може бити и већи.

Пример 5.13. *Конгруенција* $x^2 + x - 1 \equiv 2 \pmod 4$ *нема решења. Лако се проверава да ниједан од бројева из потпуног система остатака* $\{0, 1, 2, 3\}$ *не задовољава конгруенцију.*

Конгруенција $x^2+x-1 \equiv 1 \pmod 4$ *има два решења: задовољавају је бројеви* 1 *и* 2 *из потпуног система остатака по модулу* 4.

Конгруенција $x^2 - 1 \equiv 0 \pmod{24}$ *има осам решења. Њу задовољавају следећи бројеви из потпуног система остатака по модулу* 24*:* 1, 5, 7, 11, 13, 17, 19 *и* 23.

Теорема 5.5. *Ако у полиному са целобројним коефицијентима*

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$$

прост број p *не дели* a_n*, тада конгруенција*

$$P(x) \equiv 0 \pmod p$$

има највише n *различитих решења.*

Доказ. Доказаћемо теорему индукцијом по n. За $n = 1$ тврђење важи. Наиме, линеарна конгруенција $a_1x + a_0 \equiv 0 \pmod m$ има решење ако и само ако $(a_1, m) \mid a_0$ (видети Линеарне Диофантове једначине – страна 150). Ако је x_0 решење те конгруенције, тада није тешко видети да она има $d = (a_1, m)$ решења:

$$x_0, x_0 + \frac{m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}\,.$$

Линеарна конгруенција $a_1x + a_0 \equiv 0 \pmod p$ има јединствено решење јер је по претпоставци $(a_1, p) = 1$.

Претпоставимо да тврђење важи за полиноме степена мањег од n. Претпоставимо да за неки полином $P(x) = a_nx^n + \cdots + a_0$ степена $n > 1$ тврђење не важи. Тада конгруенција $P(x) \equiv 0 \pmod p$ има бар

$n+1$ решења неконгруентних по модулу p. Нека су то $x_1, x_2, \ldots, x_{n+1}$. Тада је

$$P(x) - P(x_1) = a_n(x^n - x_1^n) + \cdots + a_1(x - x_1) = (x - x_1)Q(x),$$

где је $Q(x) = a_n x^{n-1} + \cdots$ полином са целобројним коефицијентима, па добијамо

$$(x - x_1)Q(x) \equiv P(x) - P(x_1) \pmod{p},$$

одакле, због $P(x_1) \equiv 0 \pmod{p}$, добијамо конгруенцију

$$(x - x_1)Q(x) \equiv P(x) \pmod{p}.$$

Замењујући у последњој конгруенцији x редом са $x_2, \ldots, x_{n+1}$ добијамо конгруенције:

$$\begin{aligned} (x_2 - x_1)Q(x_2) &\equiv 0 \pmod{p}, \\ &\vdots \\ (x_{n+1} - x_1)Q(x_{n+1}) &\equiv 0 \pmod{p}, \end{aligned}$$

односно, након скраћивања редом са $x_2 - x_1, \ldots, x_{n+1} - x_1$ (скраћивање је могуће јер су решења $x_1, x_2, \ldots, x_{n+1}$ по паровима неконгруентна по модулу p, тј. све посматране разлике су узајамно просте са p – видети теорему 4.3. 1.):

$$Q(x_2) \equiv 0 \pmod{p}, \ \ldots, \ Q(x_{n+1}) \equiv 0 \pmod{p}.$$

То значи да конгруенција $Q(x) \equiv 0 \pmod{p}$, која је реда $n-1$, има n решења, што је у контрадикцији са индукцијском претпоставком. Тиме је тврђење доказано. ■

5.4.1. Квадратне конгруенције

Посебно ћемо се позабавити најједноставнијим обликом конгруенција другог реда (квадратних конгруенција).

Посматраћемо једначине облика

$$(*) \qquad x^2 \equiv a \pmod{p}, \quad (a,p)=1, \;\; p - \text{непаран прост број.}$$

Ако је x_1 неко решење једначине $(*)$, тада је и $-x_1$ њено решење различито (по модулу p) од x_1.

Наравно, решења једначине $(*)$ тражимо у скупу $\{0, 1, \ldots, p-1\}$, јер ако је x_0 решење, тада је и сваки број из његове класе конгруенције по модулу p такође решење једначине $(*)$.

Теорема 5.6. *У сведеном систему остатака $\{1, 2, \ldots, p-1\}$ по модулу p има тачно $\dfrac{p-1}{2}$ бројева који су конгруентни квадратима целих бројева по модулу p.*

Доказ. Квадратима целих бројева по модулу p конгруентни су бројеви

$$1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

Међу тим бројевима нема конгруентних по модулу p. Наиме, ако би постојали бројеви r и s такви да важи

$$r^2 \equiv s^2 \pmod{p} \quad \text{и} \quad 0 < r < s \leqslant \frac{p-1}{2},$$

тада би важило $r^2 - s^2 \equiv 0 \pmod{p}$, тј. $(r-s)(r+s) \equiv 0 \pmod{p}$, одакле следи $p \mid r-s$ или $p \mid r+s$. Контрадикција. ■

ТЕОРЕМА 5.7. (***Ојлеров критеријум***) *Ако је p непаран прост број и ако је $(a,p)=1$, тада једначина $(*)$ има два или ниједно решење, зависно од тога да ли је $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ или $a^{\frac{p-1}{2}} \equiv -1 \pmod p$.*

ДОКАЗ. Према Малој Фермаовој теореми је $a^{p-1} \equiv 1 \pmod p$, односно

$$\left(a^{\frac{p-1}{2}}-1\right)\left(a^{\frac{p-1}{2}}+1\right) \equiv 0 \ (\mathrm{mod}\ p).$$

Како не могу оба чиниоца на левој страни последње конгруенције бити дељива са p (јер би тада и њихова разлика, 2, била дељива са p), то важи једна и само једна од конгруенција:

$$a^{\frac{p-1}{2}} \equiv 1 \ (\mathrm{mod}\ p), \quad a^{\frac{p-1}{2}} \equiv -1 \ (\mathrm{mod}\ p).$$

Ако једначина $(*)$ има решење x, тада важи

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \ (\mathrm{mod}\ p).$$

Важи и обрнуто, ако је $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, тада једначина $(*)$ има решење, а већ смо напоменули да једначина $(*)$ не може имати тачно једно решење. ■

ПРИМЕР 5.14. *Једначина $x^2 \equiv 5 \pmod{29}$ има два решења ($x_1 \equiv 11$, $x_2 \equiv 18$) јер је $5^{\frac{29-1}{2}} = 5^{14} \equiv 1 \pmod{29}$, док једначина $x^2 \equiv 3 \pmod{29}$ нема решења јер је $3^{\frac{29-1}{2}} = 3^{14} \equiv -1 \pmod{29}$.*

ДЕФИНИЦИЈА 5.1. *Нека је p непаран прост број и $(a,p)=1$.* ***Лежандров симбол*** *броја a у односу на p, у ознаци $\left(\dfrac{a}{p}\right)$ је*

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & x^2 \equiv a \ (\mathrm{mod}\ p) \ \textit{има два решења} \\ -1, & x^2 \equiv a \ (\mathrm{mod}\ p) \ \textit{нема решења} \end{cases}.$$

Пример 5.15. $\left(\dfrac{7}{19}\right) = +1$, $\left(\dfrac{5}{17}\right) = -1$.

Према дефиницији 5.1. и теореми 5.7. важи:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p.$$

Теорема 5.8. (***Гаусов критеријум***) *Нека је p непаран прост број и a цео број узајамно прост са p. Тада је*

$$\left(\frac{a}{p}\right) = (-1)^k,$$

при чему је k број оних елемената скупа $S = \left\{a, 2a, \ldots, \dfrac{p-1}{2}a\right\}$ чији је најмањи по апсолутној вредности остатак при дељењу са p негативан.

Доказ. Сваки елемент скупа S конгруентан је тачно једном броју сведеног система остатака по модулу p:

$$-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2},$$

односно, сваком броју sa из S одговара број $(-1)^{k_s} r_s$, такав да важи $sa \equiv (-1)^{k_s} r_s \pmod p$, где је $1 \leqslant r_s \leqslant \dfrac{p-1}{2}$ и k_s једнако 0 или 1, при чему је $k_s = 1$ ако и само ако је најмањи по апсолутној вредности остатак броја sa при дељењу са p негативан.

Ако су sa и ta, $s \neq t$, два броја скупа S, тада је $r_s \neq r_t$. Заиста, ако би било $r_s = r_t$, тј.

$$sa \equiv (-1)^{k_s} r_s \pmod p \quad \text{и} \quad ta \equiv (-1)^{k_t} r_s \pmod p,$$

имали бисмо да је $sa \equiv \pm ta \pmod{p}$, тј. да $p \mid (s \mp t)a$. Међутим, како је $1 \leqslant s \leqslant \dfrac{p-1}{2}$, $1 \leqslant t \leqslant \dfrac{p-1}{2}$, $s \neq t$, следи да је $0 < |s \pm t| \leqslant \dfrac{p-1}{2}$, па $p \nmid s \pm t$, тј. $p \mid a$ супротно претпоставци теореме.

Дакле, сваком елементу sa скупа S одговара тачно један број r_s скупа $\left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$, па је

$$r_1 r_2 \cdots r_{\frac{p-1}{2}} = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}.$$

Означимо последњи производ са P. Множењем конгруенција:

$$\begin{aligned} 1 \cdot a &\equiv (-1)^{k_1} r_1 \pmod{p} \\ 2 \cdot a &\equiv (-1)^{k_2} r_2 \pmod{p} \\ &\vdots \\ \frac{p-1}{2} \cdot a &\equiv (-1)^{k_{\frac{p-1}{2}}} r_{\frac{p-1}{2}} \pmod{p} \end{aligned}$$

добијамо да је

$$P \cdot a^{\frac{p-1}{2}} \equiv (-1)^{k_1 + k_2 + \cdots + k_{\frac{p-1}{2}}} \cdot P \pmod{p},$$

па како је P узајамно просто са p, да је

$$a^{\frac{p-1}{2}} \equiv (-1)^{k_1 + k_2 + \cdots + k_{\frac{p-1}{2}}} \pmod{p}.$$

Према Ојлеровом критеријуму (теорема 5.7.) је

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p},$$

па је

$$\left(\frac{a}{p}\right) \equiv (-1)^{k_1 + k_2 + \cdots + k_{\frac{p-1}{2}}} \pmod{p}.$$

Лева и десна страна последње конгруенције су по апсолутној вредности једнаке 1, па пошто су конгруентне по модулу p следи да је

$$\left(\frac{a}{p}\right) = (-1)^{k_1+k_2+\cdots+k_{\frac{p-1}{2}}} = (-1)^k,$$

при чему је k једнако броју целих бројева k_s једнаких 1, тј. броју оних елемената скупа S чији је најмањи по апсолутној вредности остатак при дељењу са p негативан. ■

Особине Лежандровог симбола дајемо у следећој теореми.

Теорема 5.9. *Нека је p непаран прост број.*

(1) *Ако су a и b цели бројеви узајамно прости са p такви да је $a \equiv b \pmod{p}$, тада је $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

(2) *Ако су $a_1, a_2, \ldots, a_n$ цели бројеви такви да је $(a_i, p) = 1$, $i = 1, 2, \ldots, n$, при чему је p непаран прост број, тада је*

$$\left(\frac{a_1 a_2 \cdots a_n}{p}\right) = \left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)\cdots\left(\frac{a_n}{p}\right).$$

(3) *Ако је a цео број узајамно прост са непарним простим бројем p, тада важи $\left(\frac{a^2}{p}\right) = 1$.*

(4) $\left(\frac{-1}{p}\right) = \begin{cases} +1, & \text{ако је } p \equiv 1 \pmod{4} \\ -1, & \text{ако је } p \equiv 3 \pmod{4} \end{cases}.$

(5) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

Доказ. Тврђења под (1), (2) и (3) лако се доказују. То остављамо читаоцима да сами ураде.

(4) Према Ојлеровом критеријуму имамо да је

$$\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

И лева и десна страна последње конгруенције по апсолутној вредности једнаке су јединици, па оне могу бити конгруентне по модулу p $(p > 2)$, једино ако су једнаке, тј. ако је

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

Број $(-1)^{\frac{p-1}{2}}$ једнак је $+1$ или -1, ако је $p \equiv 1 \pmod 4$ или $p \equiv 3 \pmod 4$, редом.

(5) Ако је $p = 8n + 1$ или $p = 8n + 7$, тада је $\dfrac{p^2 - 1}{8}$ паран број, а ако је $p = 8n + 3$ или $p = 8n + 5$, $\dfrac{p^2 - 1}{8}$ је непаран број, па треба доказати да је

$$\left(\frac{2}{p}\right) = \begin{cases} +1, & \text{ако је } p \equiv 1 \pmod 8 \text{ или } p \equiv 7 \pmod 8 \\ -1, & \text{ако је } p \equiv 3 \pmod 8 \text{ или } p \equiv 5 \pmod 8 \end{cases}.$$

Према Гаусовом критеријуму имамо да је $\left(\dfrac{2}{p}\right) = (-1)^k$, при чему је k број елемената скупа $\left\{1 \cdot 2, 2 \cdot 2, \ldots, \dfrac{p-1}{2} \cdot 2 = p - 1\right\}$, тј. скупа $S = \{2, 4, 6, \ldots, p - 1\}$ парних бројева мањих од $p - 1$ чији је најмањи по апсолутној вредности остатак при дељењу са p негативан. Најмањи по апсолутној вредности остатак при дељењу неког броја из S са p је негативан ако је тај број већи од $\dfrac{p}{2}$. Пошто парних природних бројева мањих или једнаких $\dfrac{p}{2}$ има $\left[\dfrac{p}{4}\right]$, следи да је $k = \dfrac{p-1}{2} - \left[\dfrac{p}{4}\right]$. Сада,

– ако је $p = 8n + 1$, имамо $k = 4n - 2n = 2n$,

– ако је $p = 8n + 3$, имамо $k = (4n + 1) - 2n = 2n + 1$,

– ако је $p = 8n + 5$, имамо $k = (4n + 2) - (2n + 1) = 2n + 1$,

– ако је $p = 8n + 7$, имамо $k = (4n + 3) - (2n + 1) = 2(n + 1)$,

па је $\left(\dfrac{2}{p}\right) = (-1)^k$ једнако 1, ако је прост број p облика $8n + 1$ или $8n + 7$, док је једнако -1, ако је p облика $8n + 3$ или $8n + 5$. ∎

Пример 5.16. *Покажимо да постоји цео број x такав да $79 \mid x^2 - 2$. Како је $79 = 8 \cdot 9 + 7$, то је $\left(\dfrac{2}{79}\right) = 1$, па постоји цео број x такав да $79 \mid x^2 - 2$.*

Теорема 5.10. (***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:*

$$(**) \qquad x^2 \equiv p \pmod{q}, \qquad x^2 \equiv q \pmod{p}$$

решива, а друга није. Ако p и q нису оба облика $4k + 3$, тада су или обе једначине $(**)$ решиве или ниједна, или еквивалентно, за непарне и различите просте бројеве p и q важи:

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = \begin{cases} -1, & \text{ако је } p \equiv 3 \pmod{4} \text{ и } q \equiv 3 \pmod{4} \\ +1, & \text{ако је } p \equiv 1 \pmod{4} \text{ или } q \equiv 1 \pmod{4} \end{cases},$$

тј.

$$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}.$$

Доказ. Према Гаусовом критеријуму није тешко закључити да је

$$\left(\frac{p}{q}\right) = (-1)^{\sum_{s=1}^{\frac{p-1}{2}} \left[\frac{qs}{p}\right]} \quad \text{и} \quad \left(\frac{q}{p}\right) = (-1)^{\sum_{s=1}^{\frac{q-1}{2}} \left[\frac{ps}{q}\right]},$$

па је

$$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\sum\limits_{s=1}^{\frac{p-1}{2}}\left[\frac{qs}{p}\right]+\sum\limits_{s=1}^{\frac{q-1}{2}}\left[\frac{ps}{q}\right]}.$$

Сличним поступком као у задатку 287 може се доказати да је

$$\sum_{s=1}^{\frac{p-1}{2}}\left[\frac{qs}{p}\right]+\sum_{s=1}^{\frac{q-1}{2}}\left[\frac{ps}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}\pmod 2,$$

одакле директно следи тврђење теореме. ■

На крају, навешћемо једну доста важну теорему теорије бројева:

ТЕОРЕМА 5.11. (***Лаīранж***) *Сваки īриродан број се може īредсīавиīи као збир чеīири квадраīа целих бројева.*

ДОКАЗ. Приметимо најпре да за реалне бројеве a_i, b_i $(i=1,2,3,4)$ важи:

$$(1)\qquad \left(a_1^2+a_2^2+a_3^2+a_4^2\right)\left(b_1^2+b_2^2+b_3^2+b_4^2\right)=c_1^2+c_2^2+c_3^2+c_4^2,$$

где је:

$$\begin{aligned} c_1&=a_1b_1+a_2b_2+a_3b_3+a_4b_4, & c_2&=a_1b_2-a_2b_1+a_3b_4-a_4b_3,\\ c_3&=a_1b_3-a_3b_1+a_4b_2-a_2b_4, & c_4&=a_1b_4-a_4b_1+a_2b_3-a_3b_2.\end{aligned}$$

Према томе, довољно је доказати да тврђење теореме важи за све просте бројеве. За $p=2$ тврђење очигледно важи.

Нека је p непаран прост број. Видели смо већ да међу бројевима

$$(2)\qquad 0^2,\ 1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2$$

не постоје два која су конгруентна по модулу p. То исто важи и за бројеве:

$$(3) \qquad -1-0^2,\ -1-1^2,\ -1-2^2,\ \ldots,\ -1-\left(\frac{p-1}{2}\right)^2.$$

Како бројева (2) и (3) има укупно $p+1$, то морају постојати два који су конгруентни по модулу p. Један од њих мора бити из једног, а други из другог скупа. Дакле, постоје цели бројеви a и b, $0 \leqslant a, b \leqslant \dfrac{p-1}{2}$ такви да је $a^2 \equiv -1-b^2 \pmod{p}$, тј. $a^2+b^2+1=pm$, где је

$$m=\frac{1}{p}(a^2+b^2+1) \leqslant \frac{1}{p}\left[2\left(\frac{p-1}{2}\right)^2+1\right]=\frac{p^2-2p+3}{2p}<\frac{p}{2}.$$

Дакле, за сваки непаран прост број p постоји $m \in \mathbb{Z}$, $1 \leqslant m < \dfrac{p}{2}$, тако да важи

$$mp=a^2+b^2+1^2+0^2,$$

тј. да се број mp може представити као збир четири квадрата. Нека је m_0 најмањи број за који постоји представљање облика

$$(4) \qquad m_0p=a_1^2+a_2^2+a_3^2+a_4^2, \quad 1 \leqslant m_0 < \frac{p}{2}.$$

Ако докажемо да је $m_0=1$, то ће значити да се сваки непаран прост број може представити као збир четири квадрата целих бројева.

Доказаћемо најпре да је m_0 непаран број. Претпоставимо супротно да је $m_0=2m_1$. Тада међу бројевима a_1, a_2, a_3, a_4 мора бити паран број непарних, па би се они могли нумерисати тако да $2 \mid a_1 \pm a_2$ и $2 \mid a_3 \pm a_4$. Тада је

$$\begin{aligned} m_1p &= \frac{1}{2}\left(a_1^2+a_2^2+a_3^2+a_4^2\right) \\ &= \left(\frac{a_1+a_2}{2}\right)^2+\left(\frac{a_1-a_2}{2}\right)^2+\left(\frac{a_3+a_4}{2}\right)^2+\left(\frac{a_3-a_4}{2}\right)^2, \end{aligned}$$

што је у контрадикцији са избором m_0. Дакле, број m_0 је непаран.

Нека су r_i остаци при дељењу a_i са m_0 и то најмањи по апсолутној вредности, тј. $|r_i| < \dfrac{m_0}{2}$. Тада је

$$r_1^2 + r_2^2 + r_3^2 + r_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m_0},$$

тј.

$$r_1^2 + r_2^2 + r_3^2 + r_4^2 = m_0 t, \tag{5}$$

где је

$$0 \leqslant t = \frac{1}{m}\left(r_1^2 + r_2^2 + r_3^2 + r_4^2\right) < \frac{1}{m_0} \cdot 4 \left(\frac{m_0}{2}\right)^2 = m_0.$$

Множењем релација (4) и (5), користећи (1), добијамо

$$m_0^2 pt = \left(a_1^2 + a_2^2 + a_3^2 + a_4^2\right)\left(r_1^2 + r_2^2 + r_3^2 + r_4^2\right) = c_1^2 + c_2^2 + c_3^2 + c_4^2,$$

где је $c_1 = a_1r_1 + a_2r_2 + a_3r_3 + a_4r_4 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m_0}$, $c_2 = a_1r_2 - a_2r_1 + a_3r_4 - a_4r_3 \equiv a_1a_2 - a_2a_1 + a_3a_4 - a_4a_3 \equiv 0 \pmod{m_0}$, и слично за c_3 и c_4. Значи, бројеви c_1, c_2, c_3 и c_4 су дељиви са m_0. Сада добијамо

$$pt = \left(\frac{c_1}{m_0}\right)^2 + \left(\frac{c_2}{m_0}\right)^2 + \left(\frac{c_3}{m_0}\right)^2 + \left(\frac{c_4}{m_0}\right)^2.$$

На основу избора броја m_0 следи да је $t = 0$, па је и $r_i = 0$, односно $a_i \equiv 0 \pmod{m_0}$. Тада важи

$$m_0^2 \mid a_1^2 + a_2^2 + a_3^2 + a_4^2 = m_0 p,$$

одакле следи да $m_0 \mid p$. Због услова $1 \leqslant m_0 < \dfrac{p}{2}$, следи да мора бити $m_0 = 1$, што је и требало доказати. ■

5.5. Задаци

247. Нека је $p > 2$ прост број и a, b цели бројеви. Наћи услове под којима конгруенција $x^2 + ax + b \equiv 0 \pmod p$ има решења.

Решење. Како је $(4, p) = 1$, конгруенција $x^2 + ax + b \equiv 0 \pmod p$ има решења ако и само ако $4x^2 + 4ax + 4b \equiv 0 \pmod p$ има решења, тј. $(2x + a)^2 \equiv a^2 - 4b \pmod p$ има решења.

Нека је $D = a^2 - 4b$.

1. Ако D није конгруентно квадрату природног броја по модулу p, дата конгруенција нема решења.

2. Ако је $a^2 \equiv 4b \pmod p$, дата конгруенција има тачно једно решење (у скупу $\{0, 1, \ldots, p-1\}$).

3. Ако је $D \not\equiv 0 \pmod p$ и D је конгруентно квадрату природног броја по модулу p, дата конгруенција има два решења.

248. Ако је p прост број облика $4n + 1$ и конгруенција $x^2 \equiv a \pmod p$ има решење, тада и конгруенција $x^2 \equiv -a \pmod p$ има решење. Важи и обрнуто: ако постојање решења конгруенције $x^2 \equiv a \pmod p$ повлачи постојање решења конгруенције $x^2 \equiv -a \pmod p$, непаран прост број p је облика $4n + 1$. Доказати.

Решење. Нека је $p = 4n + 1$ и нека конгруенција $x^2 \equiv a \pmod p$ има решење, нпр. $c^2 \equiv a \pmod p$. Према Вилсоновој теореми важи:

$$-a = a(-1) \equiv a(p-1)! = a \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \ldots \cdot (p-1) \pmod p.$$

Како је $p - k \equiv -k \pmod p$ за $k = 1, 2, \ldots, \dfrac{p-1}{2}$, то је

$$-a \equiv a \cdot \left[1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right] \cdot \left[(-1) \cdot (-2) \cdot \ldots \cdot \left(-\frac{p-1}{2}\right)\right] \pmod p$$

и како је број фактора у свакој од средњих заграда једнак $\dfrac{p-1}{2} = 2n$, дакле, паран, то је

$$-a \equiv a \cdot \left(1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right)^2 \equiv \left(c \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}\right)^2 \pmod{p},$$

тј. конгруенција $x^2 \equiv -a \pmod{p}$ има решења.

Обрнуто, нека је $b^2 \equiv a \pmod{p}$ и $c^2 \equiv -a \pmod{p}$, $0 < b < p$ и $0 < c < p$. Тада добијамо:

$$c^{p-1} \equiv \left(c^2\right)^{\frac{p-1}{2}} \equiv (-a)^{\frac{p-1}{2}} = (-1)^{\frac{p-1}{2}} a^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} b^{p-1} \pmod{p}.$$

Према Малој Фермаовој теореми је $b^{p-1} \equiv c^{p-1} \equiv 1 \pmod{p}$, па је $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, одакле непосредно следи да је $\dfrac{p-1}{2} = 2n$, тј. $p = 4n+1$.

249. Конгруенција $P(x) \equiv 0 \pmod{p}$ реда n, $n > p$, где је p прост број еквивалентна је конгруенцији $R(x) \equiv 0 \pmod{p}$, где је $R(x)$ остатак при дељењу $P(x)$ са $x^p - x$. Доказати.

Решење. Нека је $Q(x)$ полином такав да је

$$P(x) = (x^p - x)Q(x) + R(x).$$

Онда је дата конгруенција еквивалентна конгруенцији

$$(x^p - x)Q(x) + R(x) \equiv 0 \pmod{p},$$

односно, на основу Мале Фермаове теореме, конгруенцији

$$R(x) \equiv 0 \pmod{p}.$$

250. Решити следећу конгруенцију

$$x^7 - 3x^6 + x^5 - x^3 + 4x^2 - 4x + 2 \equiv 0 \pmod{5}.$$

Решење. Дељењем леве стране конгруенције са $x^5 - x$ добија се остатак $x^2 - 3x + 2$, па је на основу задатка 249 дата конгруенција еквивалентна са конгруенцијом $x^2 - 3x + 2 \equiv 0 \pmod 5$, чија решења налазимо провером свих елемената потпуног система остатака по модулу 5. Решења су 1 и 2.

251. Нека су $P(x)$, $Q(x)$ и $R(x)$ полиноми са целобројним коефицијентима такви да је $P(x) = Q(x)R(x)$ и p прост број. Ако је број решења конгруенције $P(x) \equiv 0 \pmod p$ једнак степену полинома $P(x)$, онда и свака од конгруенција

$$Q(x) \equiv 0 \pmod p \quad \text{и} \quad R(x) \equiv 0 \pmod p$$

има онолико решења колики је степен полинома на левој страни конгруенције. Доказати.

Решење. Степен полинома $P(x)$ једнак је збиру степена полинома $Q(x)$ и $R(x)$. Ниједна од конгруенција $Q(x) \equiv 0 \pmod p$ и $R(x) \equiv 0 \pmod p$ не може имати више решења него што је степен одговарајућег полинома, јер би у супротном сви коефицијенти тог полинома били дељиви са p, па би то важило и за полином $P(x)$. Ако би нека од тих конгруенција имала мање решења од степена одговарајућег полинома, онда би и број решења конгруенције $P(x) \equiv 0 \pmod p$ био мањи од степена полинома $P(x)$.

252. Доказати да свака од конгруенција

$$x^{\frac{p-1}{2}} \equiv 1 \pmod p, \quad x^{\frac{p-1}{2}} \equiv -1 \pmod p,$$

где је $p > 2$ прост број, има тачно $\dfrac{p-1}{2}$ решења.

Решење. На основу Мале Фермаове теореме конгруенција

$$x^{p-1} - 1 \equiv 0 \pmod p,$$

има $p-1$ решења, а како је

$$x^{p-1}-1=\left(x^{\frac{p-1}{2}}-1\right)\left(x^{\frac{p-1}{2}}+1\right)$$

то тврђење следи на основу задатка 251.

253. Нека је p непаран прост број. Доказати да једначина

$$x^2+1\equiv 0 \pmod p$$

има решења ако и само ако је $p\equiv 1 \pmod 4$.

254. Да ли постоји цео број x такав да $127 \mid x^2+1$?

255. Да ли конгруенција $x^2\equiv 6 \pmod{19}$ има решења?

Решење. Одредимо најмање по апсолутној вредности остатке бројева $6s$, $1\leqslant s\leqslant 9$, при дељењу са 19 и пребројимо колико је негативних:

$$\begin{array}{lll}
6\cdot 1\equiv 6 \ (\mathrm{mod}\ 19), & \underline{6\cdot 2\equiv -7 \ (\mathrm{mod}\ 19)}, & \underline{6\cdot 3\equiv -1 \ (\mathrm{mod}\ 19)},\\
6\cdot 4\equiv 5 \ (\mathrm{mod}\ 19), & \underline{6\cdot 5\equiv -8 \ (\mathrm{mod}\ 19)}, & \underline{6\cdot 6\equiv -2 \ (\mathrm{mod}\ 19)},\\
6\cdot 7\equiv 4 \ (\mathrm{mod}\ 19), & \underline{6\cdot 8\equiv -9 \ (\mathrm{mod}\ 19)}, & \underline{6\cdot 9\equiv -3 \ (\mathrm{mod}\ 19)}.
\end{array}$$

Пошто је 6 негативних остатака, према Гаусовом критеријуму следи да је $\left(\dfrac{6}{19}\right)=(-1)^6=1$, што значи да конгруенција $x^2\equiv 6 \pmod{19}$ има два решења.

⌜ *Напомена.* Видети теорему 5.8. и њен доказ. ⌟

256. 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?

Решење. Приметимо најпре да су бројеви $113, 521, 619$ прости.

1) Применом теорема 5.9. и 5.10. имамо да је:

$$
\begin{aligned}
\left(\frac{68}{113}\right) &= \left(\frac{2}{113}\right)^2\left(\frac{17}{113}\right) && \text{према 5.9. } (2)\text{, јер је } 68 = 2^2\cdot 17\\
&= \left(\frac{113}{17}\right) && \text{јер је } \left(\frac{2}{113}\right)^2 = 1 \text{ и према 5.10.}\\
& && \left(\frac{17}{113}\right)\left(\frac{113}{17}\right) = (-1)^{\frac{17-1}{2}\cdot\frac{113-1}{2}} = 1\\
&= \left(\frac{11}{17}\right) && \text{према 5.9. } (1) \text{ јер је } 113 \equiv 11 \pmod{17}\\
&= \left(\frac{17}{11}\right) && \text{према 5.10. је } \left(\frac{11}{17}\right)\left(\frac{17}{11}\right) = 1\\
&= \left(\frac{6}{11}\right) && \text{јер је } 17 \equiv 6 \pmod{11}\\
&= \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) && \text{јер је } 6 = 2\cdot 3\\
&= -\left(\frac{3}{11}\right) && \text{према 5.9. } (5)\\
& && \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = -1\\
&= \left(\frac{11}{3}\right) && \text{јер је } \left(\frac{3}{11}\right)\left(\frac{11}{3}\right) = -1\\
&= \left(\frac{2}{3}\right) && \text{јер је } 11 \equiv 2 \pmod{3}\\
&= -1,
\end{aligned}
$$

одакле следи да дата конгруенција нема решења.

2) Из једнакости

$$\left(\frac{310}{521}\right) = \left(\frac{2}{521}\right)\left(\frac{5}{521}\right)\left(\frac{31}{521}\right)$$

$$\begin{aligned} &= \left(\frac{521}{5}\right)\left(\frac{521}{31}\right) \\ &= \left(\frac{1}{5}\right)\left(\frac{25}{31}\right) = \left(\frac{5^2}{31}\right) = 1 \end{aligned}$$

следи да дата конгруенција има два решења.

3) Из једнакости

$$\begin{aligned} \left(\frac{-174}{619}\right) &= \left(\frac{-1}{619}\right)\left(\frac{2}{619}\right)\left(\frac{3}{619}\right)\left(\frac{29}{619}\right) \\ &= \left(\frac{3}{619}\right)\left(\frac{29}{619}\right) = -\left(\frac{619}{3}\right)\left(\frac{619}{29}\right) \\ &= -\left(\frac{1}{3}\right)\left(\frac{10}{29}\right) = -\left(\frac{2}{29}\right)\left(\frac{5}{29}\right) \\ &= \left(\frac{29}{5}\right) = \left(\frac{2^2}{5}\right) = 1, \end{aligned}$$

следи да дата конгруенција има два решења.

257. (Мала олимпијада 1980) Нека су a, b, c цели бројеви и m природан број већи од 1. Ако је

$$a^n + bn + c \equiv 0 \pmod{m},$$

за сваки природан број n, доказати да је $b^2 \equiv 0 \pmod{m}$. Да ли мора бити $b \equiv 0 \pmod{m}$?

Решење. Из претпоставке задатка, за $n = 1$, $n = 2$ и $n = 3$, добијамо редом:

$$\begin{aligned} a + b + c &\equiv 0 \pmod{m}, \\ a^2 + 2b + c &\equiv 0 \pmod{m}, \\ a^3 + 3b + c &\equiv 0 \pmod{m}. \end{aligned}$$

Из прве две од тих релација следи

$$a^2 - a + b \equiv 0 \pmod{m}, \tag{1}$$

а из последње две

$$a^3 - a^2 + b \equiv 0 \pmod{m}., \tag{2}$$

Из (1) и (2) сада добијамо

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

и

$$b^2 \equiv [a(a-1)]^2 \equiv a\left[a(a-1)^2\right] \pmod{m},$$

па је $b^2 \equiv 0 \pmod{m}$.

Пример $m = 4$, $a = 3$, $b = 2$ и $c = 3$ показује да не мора бити $b \equiv 0 \pmod{m}$.

6. Разни задаци

258. Доказати да $641 \mid 2^{32}+1$.

Решење. Како је $641 = 5^4 + 2^4 = 5 \cdot 2^7 + 1$ и како важи

$$5 \cdot 2^7 + 1 \mid (5 \cdot 2^7)^4 - 1 = 5^4 \cdot 2^{28} - 1$$

и

$$5^4 + 2^4 \mid (5^4 + 2^4)2^{28} = 5^4 \cdot 2^{28} + 2^{32},$$

то $641 \mid (5^4 \cdot 2^{28} + 2^{32}) - (5^4 \cdot 2^{28} - 1)$.

259. Који је највећи двоцифрен прост број који је фактор броја $\binom{200}{100}$?

Решење:
$$\binom{200}{100} = \frac{200 \cdot 199 \cdots 102 \cdot 101}{100 \cdot 99 \cdots 2 \cdot 1}.$$

Првих 7 двоцифрених простих бројева у опадајућем поретку су 97, 89, 83, 79, 73, 67. Сваки од ових бројева се појављује једанпут у имениоцу и једанпут у бројиоцу (у бројевима 194, 178, 166, 158, 146, 142, 134), што значи да $\binom{200}{100}$ неће имати ове просте бројеве као факторе. Међутим, број 61 (следећи највећи прост број) јавља се као фактор једанпут у имениоцу, али два пута у бројиоцу–у бројевима 122 и 183, тако да $\binom{200}{100}$ има као фактор број 61, и то је тражени број.

260. Познато је да је $f(n) = n^2 - n + 41$ прост број ако $n \in \{1, 2, \ldots, 40\}$. Доказати:

(1) $f(n)$, $n \in \mathbb{N}$, никада није потпун квадрат, осим за $n = 41$;

(2) За сваки природан број n постоји природан број m такав да важи $f(m) = f(n)f(n+1)$;

(3) $f(1\,722)$ је најмањи у низу бројева $f(n)$, $n \in \mathbb{N}$, који је производ четири не обавезно различита проста фактора.

Решење. (1) Ако је $n < 41$, $f(n)$ је прост број па се не може представити у облику квадрата природног броја.

За $n = 41$ је $f(41) = 41^2$, а за $n > 41$ важе неједнакости:

$$(n-1)^2 < n^2 - n + 41 < n^2,$$

тј. $f(n)$ се налази између квадрата два узастопна природна броја, чиме је доказ завршен.

(2) Како је

$$\begin{aligned} f(n)f(n+1) &= (n^2 - n + 41)((n+1)^2 - (n+1) + 41) \\ &= n^4 + 81n^2 + 1\,681 \\ &= f(m) = m^2 - m + 41, \end{aligned}$$

имамо да је

$$m^2 - m = m(m-1) = n^4 + 81n^2 + 1\,640 = (n^2 + 41)(n^2 + 40).$$

Из последњих једнакости налазимо да је $m = n^2 + 41$, тако да је

$$f(n)f(n+1) = f(n^2 + 41).$$

(3) Према (2) имамо да је за $n = 41$,

$$\begin{aligned} f(41^2 + 41) &= f(1\,722) = f(41)f(42) \\ &= f(0)f(1)f(1)f(2) \\ &= 41 \cdot 41 \cdot 41 \cdot 43, \end{aligned}$$

одакле закључујемо да се $f(1\,722)$ може представити у облику производа четири проста броја. Истовремено се види да је $f(1\,722)$

најмањи број у низу бројева $f(n)$, $n \in \mathbb{N}$, са четири фактора који су прости бројеви, јер за $n > 1$ функција f монотоно расте.

261. (Чешко–словачка математичка олимпијада – финална рунда, 2003) Наћи највећи број узастопних петоцифрених бројева међу којима нема палиндрома.

Решење. Међу следећих 109 узастопних петоцифрених бројева

$$10\,902,\ 10\,903,\ \ldots,\ 10\,999,\ 11\,000,\ \ldots,\ 11\,009,\ 11\,010$$

нема палиндрома. Најмањи и највећи петоцифрени палиндроми су редом 10 001 и 99 999. Пре броја 10 001 је само један петоцифрен број, а иза броја 99 999 нема више петоцифрених бројева. Показаћемо да после било ког петоцифреног палиндрома x, $x \neq 99\,999$, постоји други петоцифрен палиндром облика $x + 100$ или $x + 110$ или $x + 11$. Означимо $x = \overline{abcba}$. Ако је $c \neq 9$, тада је број $x + 100 = \overline{ab(c+1)ba}$ палиндром. Ако је $c = 9 \neq b$, број $x + 110 = \overline{a(b+1)0(b+1)a}$ је палиндром, и коначно ако је $c = b = 9$ (наравно, $a \neq 9$) број $x + 11 = \overline{(a+1)000(a+1)}$ је палиндром.

Према томе, највећи могући број узастопних петоцифрених бројева међу којима нема палиндрома је 109.

262. (Национална математичка олимпијада–финална рунда, Бугарска 1998) Нека су m и n природни бројеви такви да је број

$$A = \frac{(m+3)^n + 1}{3m}$$

цео. Доказати да је A непаран број.

Решење. Претпоставимо супротно да је A паран број, тј. да је $(m+3)^n+1 = 6km$. Тада је m паран број. Штавише, $3 \mid m^n+1$, одакле следи да је $m = 3t+2$ и да је n непаран број. Тада је $3^n + 1 = 4 \cdot S$, где је S непаран број ($8 \nmid 3^n+1$) и $3^n+1 \equiv 4 \pmod 6$. Нека је $m = 2^\alpha m_1$, где је $\alpha \geqslant 1$ и m_1 непаран број. Тада $2^\alpha \mid 3^n+1$, одакле је $\alpha \leqslant 2$, и $m_1 = 6t_1+1$. Пошто $m = 2^\alpha(6t_1+1)$ има облик $3t+2$, а $1 \leqslant \alpha \leqslant 2$ видимо да је $\alpha = 1$. Онда је $m = 12t_1+2$ и из $(m+3)^n+1 = 6km$ следи да $4 \mid 5^n+1$, што је немогуће.

263. (Зимско математичко такмичење, Бугарска 1999, 10. разред) Нека је A скуп природних бројева без нуле у децималном запису. Познато је да ако $a = \overline{a_1a_2\dots a_k} \in A$, тада $b = \overline{b_1b_2\dots b_k}$ (где је b_j, $1 \leqslant j \leqslant k$, остатак при дељењу $3a_j$ са 10) такође припада скупу A и збир цифара броја b једнак је збиру цифара броја a.

(а) Доказати да је збир цифара сваког k-цифреног броја из A једнака $5k$.

(б) За дати природан број k, наћи најмањи k-цифрени број који може бити елемент скупа који има исте особине као скуп A.

Решење. (а) Нека је $a = \overline{a_1a_2\dots a_k} \in A$ и S збир његових цифара. Посматрајмо бројеве $b = \overline{b_1b_2\dots b_k}$, $c = \overline{c_1c_2\dots c_k}$ и $d = \overline{d_1d_2\dots d_k}$, где је b_j остатак при дељењу $3a_j$ са 10, c_j остатак при дељењу $3b_j$ са 10 и d_j остатак при дељењу $3c_j$ са 10, $1 \leqslant j \leqslant k$. Тада $b, c, d \in A$ и

$$(*)\qquad S = \sum_{j=1}^{k} a_j = \sum_{j=1}^{k} b_j = \sum_{j=1}^{k} c_j = \sum_{j=1}^{k} d_j.$$

За свако фиксирано j важи $a_j+b_j+c_j+d_j = 20$. Тада из $(*)$ следи $4S = \sum_{j=1}^{k}(a_j+b_j+c_j+d_j) = 20k$, тј. $S = 5k$.

(б) Показаћемо да је у случају $k = 2t$ тражени природан број једнак $a = \overline{a_1a_2\dots a_{2t}}$, где је $a_1 = a_2 = \dots = a_t = 1$, $a_{t+1} = a_{t+2} = \dots = a_{2t} = 9$, а у случају $k = 2t+1$ је $b = \overline{b_1b_2\dots b_{2t+1}}$, где је $b_1 = \dots = b_t = 1$, $b_{t+1} = 5$, $b_{t+2} = \dots = b_{2t+1} = 9$. Лако се проверава да a и b могу бити елементи скупа који има тражене особине.

Нека је $k = 2t$. Претпоставимо да постоји $c = \overline{c_1c_2\dots c_{2t}}$ такво да је $c < a$. Пошто нема нула међу цифрама броја c то је $c_1 = c_2 = \dots = c_t = 1$. Из (а) следи да је збир цифара броја c једнак $5k = 10t$, што имплицира $c_{t+1} = c_{t+2} = \cdots = c_{2t} = 9$. Одатле следи $c = a$, што је контрадикција.

Нека је $k = 2t + 1$. Претпоставимо да постоји $c = \overline{c_1 c_2 \ldots c_{2t+1}}$ такво да је $c < b$. Пошто нема нула међу цифрама броја c то је $c_1 = c_2 = \cdots = c_t = 1$. Из (а) следи да је збир цифара броја c једнак $5k = 10t + 5$, што имплицира да је $c_{t+1} \geqslant 5$. Пошто је $c < b$ то је $c_{t+1} = 5$, па је и $c_{t+2} = c_{t+3} = \cdots = c_{2t+1} = 9$. Одатле следи $c = b$, што је контрадикција.

264. (Зимско математичко такмичење, Бугарска 1997, 10. разред) Наћи број свих природних бројева $\overline{a_1 a_2 \cdots a_{2n}}$ таквих да важи:

(1) ниједна од цифара a_i није једнака нули;

(2) збир $a_1 a_2 + a_3 a_4 + \cdots + a_{2n-1} a_{2n}$ је паран број.

Решење. Означимо тражени број са A_n. Производ $a_{2i-1} a_{2i}$ је паран ако је бар једна од цифара a_{2i-1} и a_{2i} парна. Према томе, постоји $5 \cdot 4 + 4 \cdot 5 + 4 \cdot 4 = 56$ избора за a_{2i-1} и a_{2i} тако да је $a_{2i-1} a_{2i}$ паран број. Слично, $a_{2i-1} a_{2i}$ је непарно када су обе цифре a_{2i-1} и a_{2i} непарне. Дакле, постоји $5 \cdot 5 = 25$ избора за a_{2i-1} и a_{2i} тако да је $a_{2i-1} a_{2i}$ непаран број. Број бројева $\overline{a_1 a_2 \cdots a_{2n}}$ таквих да су i сабирака $a_{2k-1} a_{2k}$ непарни је $\binom{n}{i} 25^i 56^{n-i}$. Према томе,

$$A_n = \sum_{i=0}^{n} \binom{n}{2i} 25^{2i} 56^{n-2i}.$$

Обележимо

$$B_n = \sum_{i=0}^{n} \binom{n}{2i+1} 25^{2i+1} 56^{n-2i-1}.$$

Тада је

$$A_n + B_n = \sum_{i=0}^{n} \binom{n}{i} 25^i 56^{n-i} = (56 + 25)^n = 81^n$$

и

$$A_n - B_n = \sum_{i=0}^{n} (-1)^n \binom{n}{i} 25^i 56^{n-i} = (56-25)^n = 31^n.$$

Сада се лако добија $A_n = \dfrac{81^n + 31^n}{2}$.

265. (Национална математичка олимпијада–друга рунда, Румунија 2003, 9. разред) Наћи све $n \in \mathbb{N}$, $n \geqslant 2$ и цифре $a_1, a_2, \ldots, a_n$, тако да је

$$\sqrt{\overline{a_1 a_2 \ldots a_n}} - \sqrt{\overline{a_1 a_2 \ldots a_{n-1}}} = a_n.$$

Решење. Нека је $x = \overline{a_1 a_2 \ldots a_{n-1}} \in \mathbb{N}$. Тада је

$$\overline{a_1 a_2 \ldots a_n} = 10x + a_n \quad \text{и} \quad \sqrt{10x + a_n} - \sqrt{x} = a_n,$$

тј.

$$10x + a_n = x + a_n^2 + 2a_n\sqrt{x}.$$

Последња једначина се може записати у облику

$$9x = a_n(a_n + 2\sqrt{x} - 1).$$

Како је $a_n \leqslant 9$, добијамо $x \leqslant a_n + 2\sqrt{x} - 1$, односно

$$(\sqrt{x} - 1)^2 \leqslant a_n \leqslant 9,$$

што имплицира $\sqrt{x} \leqslant 4$ или $x \leqslant 16$.

Поред тога, $a_n \neq 0$ (јер би у супротном било $x = 0$) и

$$\sqrt{x} = \frac{9x + a_n - a_n^2}{2a_n}$$

је рационалан број, па x мора бити потпун квадрат. Како је

$$\sqrt{10x + a_n} = a_n + \sqrt{x},$$

то и $10x + a_n$ мора бити потпун квадрат. Разматрајући могуће случајеве $x = 1, 4, 9, 16$ налазимо да је $x = 16$, $a_n = 9$ и $n = 3$. Тада је $\sqrt{169} - \sqrt{16} = 9$.

266. (Зимско математичко такмичење, Бугарска 1999, 11. разред) Наћи најмањи природан број n такав да је збир квадрата свих његових делилаца (укључујући 1 и n) једнак $(n+3)^2$.

Решење. Јасно је да n мора имати најмање три делиоца. Нека су $1 < d_1 < d_2 < \cdots < d_k < n$ његови делиоци различити од 1 и n. Тада је

$$(*) \qquad d_1^2 + d_2^2 + \cdots + d_k^2 = 6n + 8.$$

Нека је $n = p^\alpha$, где је p прост број. Тада из $(*)$ следи

$$p^2 + p^4 + \cdots + p^{2\alpha-2} = 6p^\alpha + 8,$$

па $p \mid 8$, одакле следи $p = 2$. Онда је

$$1 + p^2 + p^4 + \cdots + p^{2\alpha-4} = 6p^{\alpha-2} + 2,$$

што је немогуће.

Према томе, $k \neq 1, 3, 5$, јер би у тим случајевима број делилаца броја n био једнак $3, 5, 7$, тј. $n = p^2$, $n = p^4$ или $n = p^6$, где је p прост број. Претпоставимо зато да је $k \geqslant 6$. Како је $d_i d_{k-i} = n$, из $(*)$ следи да је $(d_{k-1} - d_1)^2 + (d_{k-2} - d_2)^2 + (d_{k-3} - d_3)^2 \leqslant 8$. Међутим, ова неједнакост је немогућа јер су $d_{k-1} - d_1$, $d_{k-2} - d_2$ и $d_{k-3} - d_3$ различити природни бројеви (ако би било $d_{k-1} - d_1 = d_{k-2} - d_2 = A$ тада би важило $d_1(A + d_1) = d_2(A + d_2)$, тј. $d_1 = d_2$). Према томе, или је $k = 2$ или је $k = 4$.

Претпоставимо да је $k = 4$. Онда n има 6 делилаца, па је $n = pq^2$, где су p и q различити прости бројеви (случај $n = p^5$ је већ анализиран). Тада из $(*)$ следи

$$(**) \qquad p^2 + q^2 + q^4 + p^2q^2 = 6pq^2 + 8.$$

Ако је $q \geqslant 5$, тада је $q^4+p^2q^2 \geqslant 2pq^3 \geqslant 10pq^2 > 6pq^2+8$. Према томе $q=2$ или $q=3$. Директном провером видимо да је у оба случаја једнакост $(**)$ немогућа.

Коначно, нека је $k=2$ и $n=pq$, где су $p<q$ прости бројеви такви да важи
$$p^2+q^2=6pq+8.$$
Како $q \mid p^2-8$, то је у случају $p \leqslant 17$ једино могуће за $p=7$. Тада је $q=41$ и $n=287$. За $p>17$ је $n=pq>17^2=289>287$, па је најмањи тражени број n једнак 287.

267. (Национална математичка олимпијада–регионална рунда, Бугарска 2001) Наћи све тројке природних бројева (a,b,c) таквих да је $a^3+b^3+c^3$ дељиво са a^2b, b^2c и c^2a.

Решење. Ако је $d=$ НЗД(a,b,c), лако се види да је и тројка $\left(\frac{a}{d},\frac{b}{d},\frac{c}{d}\right)$ такође решење проблема. Зато је довољно наћи све тројке (a,b,c) такве да је НЗД$(a,b,c)=1$.

Нека је $s=(a,b)$. Претпоставимо да је $s>1$. Ако је p прост делилац од s, онда p дели a, p дели b и p дели $a^3+b^3+c^3$. Одатле следи да p дели c^3, па p дели и c. Контрадикција са НЗД$(a,b,c)=1$.

Према томе, $(a,b)=1$ и аналогно $(a,c)=(b,c)=1$. Из
$$a^2 \mid a^3+b^3+c^3, \quad b^2 \mid a^3+b^3+c^3, \quad c^2 \mid a^3+b^3+c^3$$
и
$$(a^2,b^2)=(a^2,c^2)=(b^2,c^2)=1$$
следи да $a^2b^2c^2 \mid a^3+b^3+c^3$, па је $a^3+b^3+c^3 \geqslant a^2b^2c^2$.

Не умањујући општост можемо претпоставити да је $a \leqslant b \leqslant c$. Тада важи:
$$3c^3 \geqslant a^3+b^3+c^3 \geqslant a^2b^2c^2 \;\Rightarrow\; c \geqslant \frac{a^2b^2}{3}.$$

Претпоставимо да је $a > 1$. Тада је

$$\frac{a^2b^2}{3} > b^2 \geqslant b^2 + a(a-b) = a^2 - ab + b^2,$$

па је

$$c > a^2 - ab + b^2. \tag{1}$$

С друге стране, пошто је $b \geqslant a \geqslant 2$ то је $b^2 \geqslant 2b \geqslant a + b$ и пошто је $c > b^2$, то је

$$c > a + b. \tag{2}$$

Сада из (1) и (2) добијамо

$$\frac{(a^2 - ab + b^2)(a+b)}{c^2} < 1 \ \Leftrightarrow \ \frac{a^3 + b^3}{c^2} < 1,$$

што је немогуће, јер је $\dfrac{a^3+b^3}{c^2}$ цео број.

Према томе, $a = 1$. У том случају је $1 + b^3 + c^3$ дељиво са b^2c^2. Размотримо следеће случајеве:

1. Ако је $b = c$, лако је видети да је $b = c = 1$. Дакле, тројка $(1, 1, 1)$ је решење задатка.
2. Ако је $b = 1$, добијамо исто решење као у случају 1.
3. Ако је $b = 2$, тада је $c = 3$. Тројка $(1, 2, 3)$ је решење задатка.

Претпоставимо сада да је $c > b \geqslant 3$. Пошто је $1 + b^3 + c^3 \geqslant b^2c^2$, следи да је $2c^3 > 1 + b^3 + c^3$, одакле добијамо да је $2c > b^2$, тј. $c > \dfrac{b^2}{2}$. Из $2c > b^2$ следи да је $2c > b^2 - b + 1$, тј.

$$\frac{b^2 - b + 1}{c} < 2. \tag{3}$$

Када је $b \geqslant 5$ важи неједнакост $\dfrac{c}{2} > \dfrac{b^2}{4} > b+1$, одакле следи

$$\frac{b+1}{c} < \frac{1}{2}. \tag{4}$$

Множећи (3) и (4) добијамо да је $\dfrac{b^3+1}{c^2} < 1$, што је немогуће јер је број $\dfrac{b^3+1}{c^2}$ цео. Непосредном провером може се показати да за $b = 3$ или $b = 4$ нема нових решења.

Према томе, сва решења задатка су тројке (k, k, k) и $(k, 2k, 3k)$ (и њихове пермутације) за произвољан природан број k.

268. (III селекционо такмичење за ЈБМО, Румунија 2003) Дат је скуп од 2 003 природна броја. Показати да се могу наћи два елемента тог скупа таква да њихов збир није делилац збира преосталих елемената.

Решење. Нека су $a_1 < a_2 < \cdots < a_{2003}$ елементи датог скупа. Претпоставимо супротно тврђењу, тј. да збир било која два елемента датог скупа дели збир преосталих елемената. Тада сваки од бројева $a_1+a_{2003}, a_2+a_{2003}, \dots, a_{2002}+a_{2003}$ дели збир $S = a_1+a_2+\cdots+a_{2003}$, јер важи $a+b \mid S-a-b$ ако и само ако $a+b \mid S$. Према томе, $S = k_i(a_i+a_{2003})$ за све $i = 1, 2, \dots, 2\,002$, где су k_i различити цели бројеви. Како је

$$a_i + a_{2003} < S < 2\,003a_{2003} < 2\,003(a_i + a_{2003}),$$

следи да је $k_i \in \{2, 3, \dots, 2\,002\}$, за све $i = 1, 2, \dots, 2\,002$. Тада на основу Дирихлеовог принципа постоје индекси $i \neq j$, такви да је $k_i = k_j$. Контрадикција.

269. Нека су задати бројеви m, n, r, s, такви да је $0 \leqslant r < m$ и $0 \leqslant s < n$. Ако је r остатак при дељењу неког броја са m, а s остатак при дељењу тог броја са n, извести поступак за одређивање остатка при дељењу тог броја са $[m,n]$?

Решење. Нека је a цео број такав да је $a = pm + r$ и $a = qn + s$, за неке целе бројеве p и q. Одредимо остатак који се добија при дељењу броја a са $[m,n]$.

Како је $\left(\dfrac{m}{(m,n)}, \dfrac{n}{(m,n)}\right) = 1$, одредимо целе бројеве α и β (користећи, на пример, Еуклидов алгоритам) тако да је

$$\alpha\frac{m}{(m,n)} + \beta\frac{n}{(m,n)} = 1.$$

Сабирањем једнакости

$$\frac{\beta n}{(m,n)}a = \frac{\beta mn}{(m,n)}p + \frac{\beta n}{(m,n)}r$$

и

$$\frac{\alpha m}{(m,n)}a = \frac{\alpha mn}{(m,n)}q + \frac{\alpha m}{(m,n)}s,$$

добијамо

$$a = (\beta p + \alpha q)\,[m,n] + \frac{\beta n}{(m,n)}r + \frac{\alpha m}{(m,n)}s,$$

(јер је $(m,n)\cdot[m,n] = mn$) одакле следи да је

$$a \equiv \frac{\beta nr}{(m,n)} + \frac{\alpha ms}{(m,n)} \pmod{[m,n]}.$$

Дакле, тражени остатак једнак је остатку који се добија при дељењу броја $\dfrac{\beta nr}{(m,n)} + \dfrac{\alpha ms}{(m,n)}$ са $[m,n]$.

270. (Савезно такмичење 1977, I разред) Нека су a, b и c природни бројеви и $a^2 + b^2 = c^2$. Доказати да је број abc дељив са 60.

Решење. Како је $60 = 2^2 \cdot 3 \cdot 5$, довољно је доказати да је бар један од бројева a, b, c дељив са 4 или да су два парна, да је бар један дељив са 3 и бар један дељив са 5.

Приметимо најпре да a и b не могу оба бити непарни бројеви, јер би у том случају важило $a^2 + b^2 \equiv 2 \pmod 4$, па $a^2 + b^2$ не би могао да буде једнак квадрату целог броја c.

Ако су и a и b парни бројеви, онда $4 \mid abc$.

Ако је један од бројева a, b паран а други непаран, на пример, $a = 2k$ и $b = 2n + 1$, $k, n \in \mathbb{N}$, онда је c непаран, тј. $c = 2m + 1$, $m \in \mathbb{N}$. Из $a^2 + b^2 = c^2$ следи $k^2 = m(m + 1) - n(n + 1)$, па како $2 \mid m(m+1) - n(n+1)$, имамо да $2 \mid k^2$, тј. $2 \mid k$. Пошто је $a = 2k$, то $4 \mid a$, па $4 \mid abc$.

Квадрат целог броја при дељењу са 3 даје остатак 0 или 1. Ако ни један од бројева a и b није дељив са 3, онда је $a^2 + b^2 \equiv 2 \pmod 3$, што је немогуће јер $c^2 \not\equiv 2 \pmod 3$. Дакле, бар један од бројева a, b је дељив са 3, па $3 \mid abc$.

Ако је цео број дељив са 5 и његов квадрат је дељив са 5. Ако цео број није дељив са 5, његов квадрат даје остатак 1 или 4 при дељењу са 5. Ако ни један од бројева a, b, c није дељив са 5, онда је :

$$a^2 + b^2 \equiv 0 \text{ или } 2 \text{ или } 3 \pmod 5, \quad c^2 \equiv 1 \text{ или } 4 \pmod 5.$$

Контрадикција. Дакле, бар један од бројева a, b, c је дељив са 5, па $5 \mid abc$.

271. Два играча играју следећу игру. Први изговори било који природан број, други додаје том броју 54 или 77 и изговара добијени збир. У наставку играчи наизменично додају било који од бројева 54 или 77 и изговарају збир тог броја са претходним збиром. Други играч постиже победу ако било који од играча изговори број чији је остатак при дељењу са 100 прост број. Може ли први да онемогући победу другом играчу?

Решење. Не. Наиме, стратегија другог играча је следећа: нека први на почетку изабере број n. Други бира рецимо 54. Затим у сваком следећем потезу бира број који први играч није бирао у истом потезу. Тако се након k-тог потеза добија број $n+54+77k+54k = n+54+131k$. Постојање броја k таквог да $n+54+131k \equiv p \pmod{100}$, где је $p < 100$ прост, следи из чињенице да је $(100, 131) = 1$, јер то значи да постоје $k, l \in \mathbb{Z}$ такви да важи $131 \cdot k + 100 \cdot l = 1$. Одавде је $131k \cdot (p-n-54) \equiv p-n-54 \pmod{100}$, па, штавише, за свако p имамо по једно такво k. Тиме је доказ завршен.

272. (Пролећно математичко такмичење, Бугарска 1998, 11. разред) Наћи све природне бројеве n такве да ако су a и b природни бројеви за које n дели a^2b+1 тада n дели a^2+b.

Решење. Очигледно је да је $n = 1$ једно решење. Нека $n \geqslant 2$ задовољава услове задатка и нека је a природан број узајамно прост са n. Тада постоји природан број b такав да је a^2b+1 дељив са n. Тада n дели a^2+b и једнакост $a^4-1 = a^2(a^2+b)-(a^2b+1)$ показује да n дели a^4-1.

Нека је $n = 2^\alpha k$, где је k непаран број и $\alpha \geqslant 0$. Претпоставимо да је $k \geqslant 3$. Тада су n и $k-2$ узајамно прости и зато $2^\alpha k$ дели $(k-2)^4-1$, одакле $k \mid 15$. Дакле, $n = 2^\alpha \cdot 3^\beta \cdot 5^\gamma$, где је $\alpha \geqslant 0$ и $0 \leqslant \beta, \gamma \leqslant 1$. Даље закључујемо да n дели 11^4-1, па је $\alpha \leqslant 4$. Ако је $n = 2^\alpha$, тада 2^α дели 3^4-1 и опет добијамо $\alpha \leqslant 4$. Дакле, n је делилац броја $2^4 \cdot 3 \cdot 5 = 240$.

Обрнуто, нека је n делилац броја 240. Тада n задовољава услове задатка. Заиста, ако 3 дели a^2b+1, тада 3 дели a^4-1 па $3 \mid a^2+b$. Аналогно, ако 5 дели a^2b+1 тада 5 дели a^2+b. Треба показати да исто важи за $2, 4, 8$ и 16. Претпоставимо да 2^k дели a^2b+1, где је $1 \leqslant k \leqslant 3$. Онда је a непаран број, па је a^2-1 дељиво са 8. Тада мора бити $b+1$ дељиво са 2^k, па је и a^2+b дељиво са 2^k. Ако 16 дели a^2b+1 тада је a непаран број и лако је видети да је тада $a^2 \equiv 1 \pmod{16}$ или $a^2 \equiv 9 \pmod{16}$. То имплицира $b \equiv 15 \pmod{16}$ или

$b \equiv 7 \pmod{16}$, респективно, и даље да је $a^2 + b$ дељиво са 16.

Дакле, одговор је: сви делиоци броја 240.

273. (Мала олимпијада 1982) Нека је p прост број већи од 2. За $k \in \{1, 2, \ldots, p-1\}$ нека је r_k остатак при дељењу броја k^p са p^2. Доказати да је

$$r_1 + r_2 + \cdots + r_{p-1} = \frac{p^3 - p^2}{2}.$$

Решење. За $k \in \{1, 2, \ldots, p-1\}$,

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

па $p^2 \mid k^p + (p-k)^p$, одакле следи да $p^2 \mid r_k + r_{p-k}$. Међутим, како је $r_k < p^2$ и $r_{p-k} < p^2$, то је $r_k + r_{p-k} = p^2$, па је

$$\begin{aligned} r_1 + r_2 + \cdots + r_{p-1} &= (r_1 + r_{p-1}) + (r_2 + r_{p-2}) + \cdots + \left(r_{\frac{p-1}{2}} + r_{\frac{p+1}{2}}\right) \\ &= \frac{p-1}{2} p^2. \end{aligned}$$

274. (Републичко такмичење 2000, III разред) Дати су природни бројеви q, n и r, $0 < r \leqslant n$. Доказати да $r!$ дели број

$$\left(q^n - 1\right)\left(q^n - q\right) \cdots \left(q^n - q^{r-1}\right).$$

Решење. Тврђење ће бити доказано, ако се докаже да је за произвољан прост број p, највећи степен N броја p који дели $r!$ мањи или једнак од највећег степена M броја p који дели број

$$\left(q^n - 1\right)\left(q^n - q\right) \cdots \left(q^n - q^{r-1}\right).$$

На основу задатка 83 је

$$N=\left[\frac{r}{p}\right]+\left[\frac{r}{p^2}\right]+\left[\frac{r}{p^3}\right]+\cdots.$$

Разликујемо два случаја:

1. p дели q. Како је

$$\begin{aligned}(q^n-1)(q^n-q)\dots(q^n-q^{r-1})&=(q^n-1)(q^{n-1}-1)\dots(q^{n-r+1}-1)\\&\quad\times q^{1+2+\cdots+(r-1)},\end{aligned}$$

овај број је дељив са $q^{1+2+\cdots+(r-1)}=q^{\frac{r(r-1)}{2}}$, дакле и са $p^{\frac{r(r-1)}{2}}$, па је

$$M\geqslant\frac{r(r-1)}{2}\geqslant\frac{r}{p-1}=\frac{r}{p}+\frac{r}{p^2}+\frac{r}{p^3}+\cdots\geqslant N$$

јер је

$$\frac{1}{p-1}=\frac{1}{p\left(1-\dfrac{1}{p}\right)}=\frac{1}{p}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right)$$

(користимо да је $[x]\leqslant x$; неједнакост $\dfrac{r(r-1)}{2}\geqslant\dfrac{r}{p-1}$ је еквивалентна са $(r-1)(p-1)\geqslant 2$ и није задовољена једино у тривијалним случајевима $r=1$ или $r=2$, $p=2$, који се непосредно проверавају).

2. p не дели q. Према Ојлеровој теореми важи $p^k\mid q^{\varphi(p^k)}-1$, па и $p^k\mid q^{np^{k-1}(p-1)}-1$, за све природне бројева k и n. То значи да међу бројевима $q^n-1, q^{n-1}-1,\dots,(q^{n-r+1}-1)$ сваки $(p-1)-$ви је дељив са p, сваки $p(p-1)-$ ви са p^2, сваки $p^2(p-1)-$ ви са $p^3\dots.$ Зато у производу

$$(q^n-1)(q^{n-1}-1)\cdots(q^{n-r+1}-1)\cdot q^{1+2+\cdots+(r-1)}$$

међу првих r фактора има бар $\left[\dfrac{r}{p-1}\right]$ дељивих са p, бар $\left[\dfrac{r}{p(p-1)}\right]$ дељивих са $p^2\ldots$, те је

$$\begin{aligned} M &\geqslant \left[\frac{r}{p-1}\right] + \left[\frac{r}{p(p-1)}\right] + \left[\frac{r}{p^2(p-1)}\right] + \cdots \\ &\geqslant \left[\frac{r}{p}\right] + \left[\frac{r}{p^2}\right] + \left[\frac{r}{p^3}\right] + \cdots = N. \end{aligned}$$

275. (Мала олимпијада 1995) Нека је n природан број који у свом бинарном запису има тачно $1\,995$ јединица. Доказати да је број $n!$ дељив са 2^{n-1995}.

Решење. Нека је

$$(*) \qquad n = 2^{l_1} + 2^{l_2} + \cdots + 2^{l_k}, \quad l_1 > l_2 > \cdots > l_k \geqslant 0.$$

Довољно је доказати да важи тврђење

$$\left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] + \left[\frac{n}{8}\right] + \cdots = n - k.$$

(У нашем случају је $k = 1\,995$.)

Доказ тврђења изводимо математичком индукцијом по n. За $n = 1 = 2^0$, тврђење важи. Нека тврђење важи за све бројеве мање од n. Размотримо број n облика $(*)$.

Ако је $l_k > 0$, онда означимо

$$m = \frac{n}{2} = \frac{2^{l_1} + 2^{l_2} + \cdots + 2^{l_k}}{2}\,.$$

Бинарни запис броја n завршава се нулом, а у бинарном запису броја m има такође k јединица. Тада на основу индуктивне хипотезе тврђење важи за број m, па добијамо

$$\begin{aligned} \left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] + \left[\frac{n}{8}\right] + \cdots &= m + \left[\frac{m}{2}\right] + \left[\frac{m}{4}\right] + \left[\frac{m}{8}\right] + \cdots \\ &= m + m - k = n - k. \end{aligned}$$

Ако је $l_k = 0$, онда означимо

$$m = \frac{n-1}{2} = \frac{2^{l_1} + 2^{l_2} + \cdots + 2^{l_{k-1}}}{2}\,.$$

Бинарни запис броја n завршава се јединицом, а у бинарном запису броја m има $k-1$ јединица. Тада на основу индуктивне хипотезе тврђење важи за број m, па добијамо

$$\begin{aligned}\left[\frac{n}{2}\right] + \left[\frac{n}{4}\right] + \left[\frac{n}{8}\right] + \cdots &= m + \left[\frac{m}{2}\right] + \left[\frac{m}{4}\right] + \left[\frac{m}{8}\right] + \cdots \\ &= m + m - (k-1) = n - k.\end{aligned}$$

276. Решити једначину $\dfrac{1}{\{x\}} = [x] + 2\,003.$

Решење. Ако је x решење дате једначине, из $\{x\} > 0$ следи да је $[x] + 2\,003 > 0$, тј. $[x] > -2\,003$. Нека је $[x] = k$ и $\{x\} = \alpha$. Приметимо, најпре да је α рационалан број, тј. да је $\alpha = \dfrac{p}{q}$, за неки цео број p и неки природан број $q > 1$ тако да је $(p, q) = 1$. Дакле, имамо

$$\frac{q}{p} = k + 2\,003, \quad k, p, q \in \mathbb{Z}, \quad q > 1, \quad (p, q) = 1,$$

одакле добијамо да је $p = 1$, $q = k + 2\,003$ и $k > -2\,002$ (због $q > 1$).

Није тешко проверити да, за свако $k \geqslant -2\,001$, број

$$x = k + \frac{1}{k + 2\,003}$$

задовољава дату једначину, па једначина има бесконачно много решења.

277. Доказати да за сваки природан број n важи једнакост

$$[\sqrt{n} + \sqrt{n+1}] = [\sqrt{4n+2}].$$

Решење. За сваки природан број n имамо да важи:

$$\begin{aligned}
\sqrt{n}+\sqrt{n+1} &= \sqrt{\left(\sqrt{n}+\sqrt{n+1}\right)^2}\\
&= \sqrt{2n+1+2\sqrt{n(n+1)}}\\
&= \sqrt{2n+1+\sqrt{4n^2+4n}}\\
&< \sqrt{2n+1+\sqrt{4n^2+4n+1}}\\
&= \sqrt{4n+2},
\end{aligned}$$

па је $\left[\sqrt{n}+\sqrt{n+1}\right] \leqslant [4n+2]$.

Докажимо да не постоји природан број m такав да важи неједнакост

$$\sqrt{n}+\sqrt{n+1} < m \leqslant \sqrt{4n+2}.$$

Заиста, ако би такав број постојао, тада би важила и неједнакост

$$2n+1+2\sqrt{n(n+1)} < m^2 \leqslant 4n+2,$$

тј.

$$2\sqrt{n^2+n} < \left(m^2-2n-1\right) \leqslant 2n+1,$$

односно, после квадрирања

$$4(n^2+n) < \left(m^2-2n-1\right)^2 \leqslant 4n^2+4n+1.$$

Из последње неједнакости следи да је

$$\left(m^2-2n-1\right)^2 = 4n^2+4n+1 = (2n+1)^2\,,$$

или

$$m^2-2n-1 = 2n+1,$$

одакле је $m^2 = 4n + 2$, што је немогуће, зато што квадрат природног броја при дељењу са 4 никада не даје остатак 2.

278. (Пролећно математичко такмичење, Бугарска 1997, 8. разред) Нађи све природне бројеве n такве да постоји цео број x за који је $499 \cdot (1\,997^n + 1) = x^2 + x$.

Решење. Нека је n решење проблема. Онда је

$$(2x + 1)^2 = 1\,996 \cdot 1\,997^n + 1\,997,$$

па је $(2x + 1)^2$ дељиво са $1\,997$. Пошто је $1\,997$ прост број, следи да је $(2x + 1)^2$ дељиво са $1\,997^2$. Како је и $1\,996 \cdot 1\,997^n + 1\,997$ дељиво са $1\,997^2$ то је $n = 1$. Напоменимо да у овом случају $x = 998$ и $x = -999$ задовољавају услове задатка.

279. (Зимско математичко такмичење, Бугарска 1997, 9. разред) Нека су $\alpha \neq \beta$ корени једначине $x^2 + px + q = 0$. За сваки природан број n означимо

$$a_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}\,.$$

(а) Нађи све $p, q \in \mathbb{Z}$ такве да за свако $n \in \mathbb{N}$ важи

$$a_{n+1}a_{n+2} - a_n a_{n+3} = (-1)^n.$$

(б) Доказати да за такве p и q за све $n \in \mathbb{N}$ важи $a_n + a_{n+1} = a_{n+2}$ и ако $3 \mid n$, да је тада a_n паран број.

Решење. Како су α и β корени једначине $x^2 + px + q = 0$ то је $\alpha + \beta = -p$ и $\alpha\beta = q$. Према томе

$$\begin{aligned}(-1)^n &= \frac{\alpha^{n+1} - \beta^{n+1}}{\alpha - \beta} \cdot \frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta} - \frac{\alpha^n - \beta^n}{\alpha - \beta} \cdot \frac{\alpha^{n+3} - \beta^{n+3}}{\alpha - \beta} \\ &= \frac{1}{(\alpha - \beta)^2}\left[-(\alpha + \beta)(\alpha\beta)^{n+1} + (\alpha^3 + \beta^3)(\alpha\beta)^n\right]\end{aligned}$$

$$\begin{aligned} &= \frac{1}{p^2-4q}\left(pq^{n+1}-p(p^2-3q)q^n\right) \\ &= \frac{q^n}{p^2-4q}\left(-p^3+4pq\right) = -pq^n. \end{aligned}$$

За $n=1$ и $n=2$ важи $pq=1$ и $pq^2=-1$, одакле се добија $p=-1$ и $q=-1$. Директна провера показује да $p=-1$ и $q=-1$ задовољавају $pq^n=(-1)^{n+1}$ за све $n\in\mathbb{N}$. Такође, $\alpha\neq\beta$.

(б) Пошто су α и β корени једначине $x^2-x-1=0$, то је $\alpha^2=\alpha+1$ и $\beta^2=\beta+1$, па је

$$\begin{aligned} a_n+a_{n+1} &= \frac{\alpha^n-\beta^n}{\alpha-\beta}+\frac{\alpha^{n+1}-\beta^{n+1}}{\alpha-\beta} = \frac{\alpha^n(1+\alpha)-\beta^n(1+\beta)}{\alpha-\beta} \\ &= \frac{\alpha^n\alpha^2-\beta^n\beta^2}{\alpha-\beta} = \frac{\alpha^{n+2}-\beta^{n+2}}{\alpha-\beta} = a_{n+2}. \end{aligned}$$

Пошто је $a_1=\dfrac{\alpha-\beta}{\alpha-\beta}=1$ и $a_2=\dfrac{\alpha^2-\beta^2}{\alpha-\beta}=\alpha+\beta=1$, то индукцијом из

$$a_n+a_{n+1}=a_{n+2} \tag{$*$}$$

следи да је $a_n\in\mathbb{Z}$ за све $n\in\mathbb{N}$. Из $(*)$ следи

$$a_{n+3}=a_{n+2}+a_{n+1}=a_{n+1}+a_n+a_{n+1}=2a_{n+1}+a_n.$$

Како је $a_3=a_1+a_2=2$ паран број то се индукцијом лако може показати да је a_n паран број за $n=3k$.

280. Доказати да постоји бесконачно много простих бројева p таквих да једначина (по x и y) $x^2+x+1=py$ има целобројно решење.

Решење. Претпоставимо да постоји коначно много простих бројева који могу бити чиниоци бројева облика x^2+x+1, $x\in\mathbb{Z}$, и нека су $p_1, p_2, \ldots, p_k$ сви такви прости бројеви. Међутим, број

$$(p_1 p_2 \cdots p_k)^2 + p_1 p_2 \cdots p_k + 1$$

није дељив ниједним од бројева $p_1, p_2, \ldots, p_k$.

281. (Национална математичка олимпијада–регионална рунда, Бугарска 1997) Наћи све природна бројеве a, b, c такве да су корени једначина:

$$\begin{aligned} x^2 - 2ax + b &= 0 \\ x^2 - 2bx + c &= 0 \\ x^2 - 2cx + a &= 0 \end{aligned}$$

природни бројеви.

Решење. Нека су $\{x_1, x_2\}, \{x_3, x_4\}$ и $\{x_5, x_6\}$ корени прве, друге и треће једначине респективно и нека су сви они природни бројеви. Претпоставимо да је $x_i \geqslant 2$ за $i = 1, 2, \ldots, 6$. Тада је:

$$\begin{aligned} 2a &= x_1 + x_2 \leqslant x_1 x_2 = b, \\ 2b &= x_3 + x_4 \leqslant x_3 x_4 = c, \\ 2c &= x_5 + x_6 \leqslant x_5 x_6 = a. \end{aligned}$$

Онда је $2(a+b+c) \leqslant a+b+c$, што је немогуће. Према томе, бар један од бројева x_i је једнак 1. Не умањујући општост претпоставимо да је $x_1 = 1$. Тада је $1 - 2a + b = 0$. Ако је $x_i \geqslant 2$ за $i = 3, 4, 5, 6$, тада је

$$2(b+c) = (x_3 + x_4) + (x_5 + x_6) \leqslant x_3 x_4 + x_5 x_6 = c + a,$$

односно $2(2a - 1 + c) \leqslant c + a$, одакле је $c \leqslant 2 - 3a < 0$, што је немогуће.

Према томе, бар један од бројева x_3, x_4, x_5, x_6 је једнак 1. Ако је то x_3, тада је $1 - 2b + c = 0$. Ако би важило $x_5 \geqslant 2$ и $x_6 \geqslant 2$, тада би добили $2c = x_5 + x_6 \leqslant a$, односно $2(2b-1) \leqslant \dfrac{b+1}{2}$, тј. $7b \leqslant 5$, што је контрадикција.

Дакле, бар један од бројева x_5, x_6 једнак је 1, па је $1 - 2c + a = 0$. На основу претходног је

$$0 = (1 - 2a + b) + (1 - 2b + c) + (1 - 2c + a) = 3 - (a + b + c)$$

одакле следи да је $a = b = c = 1$. Јасно је да ови бројеви задовољавају услове задатка.

282. (Савезно такмичење 1978, IV разред) Нека је $n \in \mathbb{N}$. Означимо са p_k број ненегативних целобројних решења (x, y) једначине

$$kx + (k+1)y = n - k + 1.$$

Израчунати збир $\displaystyle\sum_{k=1}^{n+1} p_k$.

Решење. Дату једначину можемо написати у облику

$$k(x + y + 1) + y = n + 1,$$

односно $ka + b = n + 1$, при чему је $0 \leqslant b = y < x + y + 1 = a$. Обрнуто, сваком решењу једначине $ka + b = n + 1$, уз дате услове, одговара тачно једно решење полазне једначине.

Дакле, треба наћи укупан број тројки (k, a, b), где су a и b ненегативни, а k позитиван цео број, $k \leqslant n + 1$, за које важи $ka + b = n + 1$ и $b < a$. Како сваком $k \in \{1, 2, \ldots, n + 1\}$ одговара тачно једно представљање броја $n + 1$ у наведеном облику (теорема 2.3.), то је тражена сума једнака $n + 1$.

283. Ако је полупречник круга непаран прост број, тада се око њега могу описати тачно два неподударна примитивна Питагорина троугла. Доказати.

Решење. Ако је $a = m^2 - n^2$, $b = 2mn$ и $c = m^2 + n^2$ примитивна Питагорина тројка, полупречник уписаног круга одговарајућег троугла је

$$r = \frac{1}{2}(a + b - c) = \frac{1}{2}(m^2 - n^2 + 2mn - m^2 - n^2) = n(m - n).$$

Како је полупречник непаран прост број p то постоје две могућности:

1. $n = 1,\ m = p + 1 \Rightarrow a = p^2 + 2p,\ b = 2(p + 1),\ c = p^2 + 2p + 2.$
2. $n = p,\ m = p + 1 \Rightarrow a = 2p + 1,\ b = 2p(p + 1),\ c = 2p^2 + 2p + 2.$

284. (Мала олимпијада 1973) Дужине страница правоугаоника једнаке су непарним природним бројевима. Доказати да у том правоугаонику не постоји тачка чије је растојање од сваког темена једнако природном броју.

Решење. Нека су непарни бројеви a и b дужине страница датог правоугаоника. Претпоставимо да унутар тог правоугаоника постоји тачка T чије је растојање од сваког темена једнако целом броју. Нека су x_1 и x_2 растојања тачке T од страница дужине b, а y_1 и y_2 растојања те тачке од страница дужине a. Тада је $a = x_1 + x_2$, $b = y_1 + y_2$, а бројеви $d_{ij} = \sqrt{x_i^2 + y_j^2}$, $i, j \in \{1, 2\}$, су цели.

Уведимо следеће ознаке: $a_i = abx_i$, $b_j = aby_j$, $i, j \in \{1, 2\}$, и

$$A_1 = a_1 - a_2, \quad A_2 = a_1 + a_2, \quad B_1 = b_1 - b_2, \quad B_2 = b_1 + b_2.$$

Тада је:

$$\begin{aligned}
A_1 &= ab(x_1 - x_2) = b\left(x_1^2 - x_2^2\right) = b\left[\left(x_1^2 + y_1^2\right) - \left(x_2^2 + y_1^2\right)\right]\\
A_2 &= ab(x_1 + x_2) = a^2 b\\
B_1 &= ab(y_1 - y_2) = a\left(y_1^2 - y_2^2\right) = a\left[\left(x_1^2 + y_1^2\right) - \left(x_1^2 + y_2^2\right)\right]\\
B_2 &= ab(y_1 + y_2) = ab^2,
\end{aligned}$$

па следи да су A_1 и B_1 цели, а A_2 и B_2 непарни бројеви.

Претпоставимо да је сваки од бројева a_1, a_2, b_1, b_2 цео. Како су A_2 и B_2 непарни бројеви, то је тачно један од бројева a_1, a_2 и тачно један од бројева b_1, b_2 непаран. Нека су, нпр. a_1 и b_1 непарни бројеви. Тада је $a_1^2 \equiv 1 \pmod 4$, и $b_1^2 \equiv 1 \pmod 4$, па је $a_1^2 + b_1^2 = (d_{11}ab)^2 \equiv 2 \pmod 4$, што је немогуће. Према томе, бар један од бројева a_1, a_2, b_1, b_2 није цео.

Како је $2a_1 = A_1 + A_2, 2a_2 = A_2 - A_1, 2b_1 = B_1 + B_2, 2b_2 = B_2 - B_1$, то је бар један од бројева $2a_1, 2a_2, 2b_1, 2b_2$ непаран. Нека је, нпр. $2a_1$ непаран број. Тада је $(2a_1)^2 + (2b_1)^2 = 4\,(a_1^2 + b_1^2) = 4a^2b^2d_{11}^2$, одакле следи $(2b_1)^2 = 4a^2b^2d_{11}^2 - (2a_1)^2 \equiv -1 \pmod 4$, што је немогуће.

Дакле, не могу сви d_{ij}, $i, j \in \{1, 2\}$, бити цели.

285. За тачку P са целобројним координатама у правоуглом Декартовом координатном систему у равни кажемо да је ***видљива*** из координатног почетка O ако не постоји тачка са целобројним координатама на дужи OP.

Доказати да је тачка (m, n) са целобројним координатама видљива из координатног почетка ако и само ако су m и n узајамно прости бројеви.

286. Доказати да за задати природан број n постоје цели бројеви a и b такви да тачке $(a + r, b + s)$, $0 < r \leqslant n$, $0 < s \leqslant n$ нису видљиве из координатног почетка.

Решење. Нека је

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots$$

низ простих бројева. Формирајмо табелу $n \times n$ на следећи начин:

$$\begin{array}{llll}
p_1 & p_2 & \cdots & p_n \\
p_{n+1} & p_{n+2} & \cdots & p_{2n} \\
p_{2n+1} & p_{2n+2} & \cdots & p_{3n} \\
\vdots & \vdots & \ddots & \vdots \\
p_{n^2-n+1} & p_{n^2-n+2} & \cdots & p_{n^2}
\end{array}$$

Нека је m_i производ елемената $i-$те врсте, а M_j производ елемената $j-$те колоне горње табеле, $i,j=1,2,\dots,n$. Посматрајмо следеће системе конгруенција:

$$(I)\quad \begin{cases} x\equiv -1 \pmod{m_1}\\ x\equiv -2 \pmod{m_2}\\ \quad\vdots\\ x\equiv -n \pmod{m_n}\end{cases} \qquad (II)\quad \begin{cases} y\equiv -1 \pmod{M_1}\\ y\equiv -2 \pmod{M_2}\\ \quad\vdots\\ y\equiv -n \pmod{M_n}\end{cases}$$

Бројеви $m_1,m_2,\dots,m_n$ су узајамно прости у паровима. Према Кинеској теореми о остацима систем (I) има решење $x=a$ (јединствено по модулу $m_1m_2\cdots m_n$). Слично, пошто су бројеви $M_1,M_2,\dots,M_n$ узајамно прости у паровима систем (II) има решење $y=b$ (јединствено по модулу $M_1M_2\cdots M_n$).

Посматрајмо сада тачке $(a+r,b+s)$, $r,s\in\{1,2,\dots,n\}$. Да бисмо показали да тачка $(a+r,b+s)$ није видљива из координатног почетка, довољно је показати да њене координате $a+r$ и $b+s$ нису узајамно прости бројеви.

$r-$та конгруенција система (I) може се записати у облику

$$a+r\equiv 0 \pmod{m_r},$$

а $s-$та конгруенција система (II) у облику

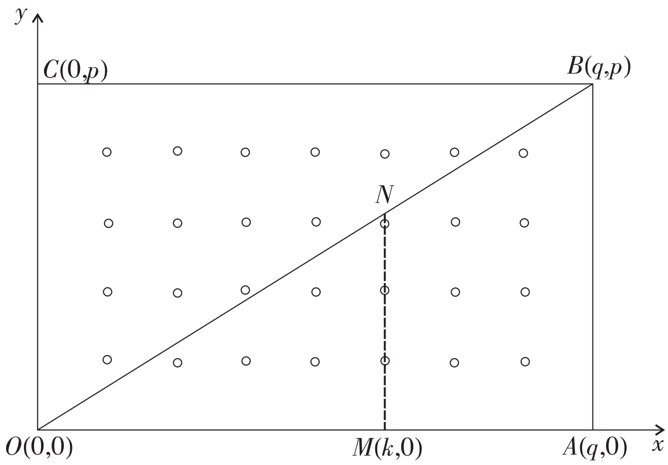
$$b+s\equiv 0 \pmod{M_s}.$$

Сада имамо да је $a+r$ дељиво са m_r, а $b+s$ дељиво са M_s. Пошто $r-$та врста и $s-$та колона наше табеле имају заједнички елемент, то је тај елемент заједнички делилац бројева m_r и M_s, тј. бројеви $a+r$ и $b+s$ нису узајамно прости. Дакле, тачка $(a+r,b+s)$ није видљива из координатног почетка.

287. (Гаус) Ако су p и q узајамно прости природни бројеви, тада је

$$\left[\frac{p}{q}\right]+\left[\frac{2p}{q}\right]+\cdots+\left[\frac{(q-1)p}{q}\right]=\left[\frac{q}{p}\right]+\left[\frac{2q}{p}\right]+\cdots+\left[\frac{(p-1)q}{p}\right]$$
$$=\frac{(p-1)(q-1)}{2}.$$

Решење. Уочимо све тачке (x,y) са целобројним координатама за које је $1\leqslant x\leqslant q-1$ и $1\leqslant y\leqslant p-1$. Ове тачке припадају унутрашњости правоугаоника $OABC$, чије су дужине страница $OA=q$ и $OC=p$, и њихов број је $(p-1)(q-1)$, при чему се на дијагонали OB не налази ни једна тачка од ових тачака.



Наиме, за све тачке (x',y') дијагонале OB важи $\dfrac{x'}{y'}=\dfrac{OA}{AB}=\dfrac{q}{p}$, но како су p и q узајамно прости, то не постоје цели позитивни бројеви $x'<q$ и $y'<p$ за које је $\dfrac{x'}{y'}=\dfrac{q}{p}$. Приметимо даље да је број целобројних тачака које имају апсцису једнаку k $(0<k<q)$ и које се налазе испод дијагонале OB једнак целом делу дужине дужи MN.

Како је $MN = \dfrac{OM}{OA} \cdot AB = \dfrac{kp}{q}$, то је тај број једнак $\left[\dfrac{kp}{q}\right]$. Дакле збир

$$\left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{(q-1)p}{q}\right]$$

једнак је броју свих целобројних тачака које су смештене испод дијагонале OB.

Због симетрије у односу на центар правоугаоника $OABC$ број целобројних тачака изнад дијагонале OB је једнак броју целобројних тачака испод дијагонале OB и износи $\dfrac{(p-1)(q-1)}{2}$. Дакле имамо да је

$$\left[\frac{p}{q}\right] + \left[\frac{2p}{q}\right] + \cdots + \left[\frac{(q-1)p}{q}\right] = \frac{(p-1)(q-1)}{2}.$$

Слично се доказује да је

$$\left[\frac{q}{p}\right] + \left[\frac{2q}{p}\right] + \cdots + \left[\frac{(p-1)q}{p}\right] = \frac{(p-1)(q-1)}{2}.$$

288. Нека је $f : [a,b] \overset{1\cdot 1}{\underset{\text{na}}{\longrightarrow}} [c,d]$ растућа бијекција интервала $[a,b]$ на интервал $[c,d]$. Доказати да важи једнакост

$$\sum_{a<m\leqslant b} [f(m)] + \sum_{c<n\leqslant d} \left[f^{-1}(n)\right] = [b]\cdot[d] - [a]\cdot[c] + K,$$

где је K број тачака са целобројним координатама које леже на графику функције f над $(a,b]$.

289. Нека је $f : [a,b] \overset{1\cdot 1}{\underset{\text{na}}{\longrightarrow}} [c,d]$ опадајућа бијекција интервала $[a,b]$ на интервал $[c,d]$ ($f(a)=d$ и $f(b)=c$). Доказати да важи једнакост

$$\sum_{a<m\leqslant b} [f(m)] - \sum_{c<n\leqslant d} \left[f^{-1}(n)\right] = [b]\cdot[d] - [a]\cdot[c]\,.$$

290. (Савезно такмичење 1998, II разред) Нека је n природан број већи од 1. Ако је

$$S_1 = \left[\sqrt{n}\right] + \left[\sqrt{2n}\right] + \cdots + \left[\sqrt{(n-1)n}\right]$$

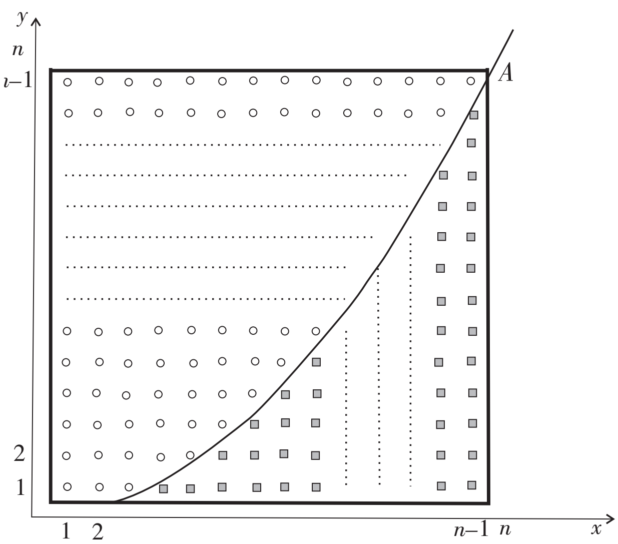
и

$$S_2 = \left[\frac{1}{n}\right] + \left[\frac{4}{n}\right] + \cdots + \left[\frac{(n-1)^2}{n}\right],$$

доказати да је $S_1 + S_2 \geqslant (n-1)^2$, при чему једнакост важи ако и само ако број n није дељив квадратом неког природног броја већег од 1.

Решење. Нека је

$$A = \{(x, y) \mid 1 \leqslant x < n, 1 \leqslant y < n, x^2 = ny\}.$$



Докажимо најпре да скуп A садржи тачке са целобројним координатама ако и само ако је n дељив неким потпуним квадратом.

Заиста, ако је n дељив неким потпуним квадратом, тј. ако је $n = p^2q$, за неке природне бројеве p, q веће од 1, тачка $\left(\dfrac{n}{p}, q\right)$ припада скупу A, јер је $1 \leqslant \dfrac{n}{p},\, q < n,\ \left(\dfrac{n}{p}\right)^2 = nq$ и $\dfrac{n}{p},\, q \in \mathbb{N}$.

С друге стране, ако n није дељив потпуним квадратом, онда је $n = p_1p_2\cdots p_k$, где су p_1, p_2, ..., p_k међусобно различити прости бројеви. У овом случају не постоје цели бројеви x, y такви да је $1 \leqslant x, y < n$ и $x^2 = ny$, јер ако би такви постојали, за свако $i \in \{1, 2, \ldots, k\}$ бисмо имали:

$$p_i \mid n \Rightarrow p_i \mid x^2 \Rightarrow p_i^2 \mid x^2 \Rightarrow p_i^2 \mid ny \Rightarrow p_i \mid y$$

па би било $y = p_1p_2\cdots p_ky'$, за неко $y' \in \mathbb{N}$, тј. $y \geqslant n$, супротно чињеници да је $y < n$.

Нека је a број тачака са целобројним координатама које припадају скупу A.

Број елемената скупа

$$A_1 = \{(x, y) \mid 1 \leqslant x, y < n, x, y \in \mathbb{N},\, x^2 \leqslant ny\}$$

(„бројимо их слева на десно, од $y-$осе до графика A, укључујући евентуално и тачке скупа A“) је

$$S_1 = \left[\sqrt{1 \cdot n}\right] + \left[\sqrt{2 \cdot n}\right] + \cdots + \left[\sqrt{(n-1)n}\right].$$

Број елемената скупа

$$A_2 = \{(x, y) \mid 1 \leqslant x, y < n, x, y \in \mathbb{N},\, x^2 \geqslant ny\}$$

(„бројимо их одоздо на горе, од $x-$осе до графика A, укључујући евентуално и тачке скупа A“) је

$$S_2 = \left[\frac{1}{n}\right] + \left[\frac{4}{n}\right] + \cdots + \left[\frac{(n-1)^2}{n}\right].$$

Пошто скуп тачака (x, y) чије су координате природни бројеви x и y за које важи $1 \leqslant x, y < n$ има $(n-1)^2$ елемената, следи да је $S_1 + S_2 = (n-1)^2 + a$.

Како је $a \geqslant 0$, имамо најпре да је

$$S_1 + S_2 \geqslant (n-1)^2,$$

а такође и да у последњој формули важи знак једнакости ако и само ако је $a = 0$, тј. ако и само ако n није дељив потпуним квадратом.

291. Доказати да у скупу целих бројева важи:

(1) $a - c \mid ab + cd \Rightarrow a - c \mid ad + bc$

(2) Ако $n \mid a + b + c + d + e$ и $n \mid a^2 + b^2 + c^2 + d^2 + e^2$, тада важи $n \mid a^5 + b^5 + c^5 + d^5 + e^5 - 5abcde$, где је n произвољан непаран број.

Решење. (1) $(ab + cd) - (ad + bc) = (a - c)(b - d)$.

(2) Нека је P полином чији су корени a, b, c, d, e. Тада је

$$P(x) = (x - a)(x - e)(x - c)(x - d)(x - e),$$

тј.

$$P(x) = x^5 + px^4 + qx^3 + rx^2 + sx + t,$$

при чему је (према Виетовим формулама): $p = -(a + b + c + d + e)$, $q = ab + ac + ad + ae + bc + bd + be + cd + ce + de, \dots, t = -abcde$.

Како је $P(a) + \cdots + P(e) = 0$, тј.

$$\begin{aligned} &a^5 + \cdots + e^5 + p(a^4 + \cdots + e^4) + q(a^3 + \cdots + e^3) \\ &\quad + r(a^2 + \cdots + e^2) + s(a + \cdots + e) + 5t = 0 \end{aligned}$$

имамо да је

$$\begin{aligned} a^5 + \cdots + e^5 - 5abcde = &-p(a^4 + \cdots + e^4) - q(a^3 + \cdots + e^3) \\ &-r(a^2 + \cdots + e^2) - s(a + \cdots + e). \end{aligned}$$

Из претпоставке задатка директно следи да

$$n \mid 2q = (a + \cdots + e)^2 - (a^2 + \cdots + e^2),$$

а пошто је n непаран број, $n \mid q$, одакле једноставно следи тврђење задатка.

292. (ИМО 2001) Нека су a, b, c, d цели бројеви, такви да је $a > b > c > d > 0$. Претпоставимо и да је

$$ac + bd = (b + d + a - c)(b + d - a + c).$$

Доказати да $ab + cd$ није прост број.

Решење. Једнакост $ac + bd = (b + d + a - c)(b + d - a + c)$ је еквивалентна са

$$a^2 - ac + c^2 = b^2 + bd + d^2. \tag{1}$$

Ако последњу једнакост помножимо са ac и трансформишемо, добићемо:

$$(ac + bd)(a^2 - ac + c^2) = (ab + cd)(ad + bc). \tag{2}$$

Даље, приметимо да важи $(a - d)(b - c) > 0$ и $(a - b)(c - d) > 0$ одакле следи

$$ab + cd > ac + bd, \tag{3}$$

$$ac + bd > ad + bc. \tag{4}$$

Ако би број $ab + cd$ био прост, тада користећи неједнакост (3), из једнакости (2) добијамо да $ac + bd \mid ad + bc$, што је у контрадикцији са (4).

293. (БМО 2001) Нека је n природан број. Доказати да је, ако су a и b цели бројеви већи од 1 такви да је $2^n - 1 = ab$, број $ab-(a-b)-1$ облика $k \cdot 2^{2m}$, где је k непаран, а m природан број.

Решење. Будући да је a непаран број, довољно је посматрати степен двојке у изразу $a(ab-(a-b)-1)$. Тада имамо:

$$\begin{aligned} a(ab-(a-b)-1) &= 2^n a - 2a - a^2 + ab \\ &= 2^n a + 2^n - (a+1)^2 \\ &= 2^n(a+1) - (a+1)^2. \end{aligned}$$

Нека је $a+1 = 2^m q$, при чему је q непаран и $m < n$. Тада је

$$\begin{aligned} 2^n(a+1)-(a+1)^2 &= 2^{n+m}q - 2^{2m}q^2 \\ &= 2^{2m}\left(2^{n-m}q - q^2\right) = 2^{2m}k. \end{aligned}$$

294. Доказати да за свако $n \in \mathbb{N}$ постоји природан број a_n такав да су $a_n, 2a_n, \ldots, na_n$ потпуни степени, тј. бројеви облика m^k, где су m и k природни бројеви и $k > 1$.

Решење. Доказаћемо индукцијом по n.

За $n = 1$ можемо узети $a_1 = 4$.

Претпоставимо сада да постоји $a_{n-1} \in \mathbb{N}$ такав да је за свако $i \in \{1, \ldots, n-1\}$, $ia_{n-1} = m_i^{k_i}$.

Нека је $k = [k_1, \ldots, k_{n-1}]$. Дефинишимо a_n са $a_n = a_{n-1}(na_{n-1})^k$. Тада је за свако $i \in \{1, \ldots, n-1\}$,

$$ia_n = ia_{n-1}(na_{n-1})^k = m_i^{k_i}(na_{n-1})^k = \left(m_i(na_{n-1})^{\frac{k}{k_i}}\right)^{k_i}$$

и

$$na_n = na_{n-1}(na_{n-1})^k = (na_{n-1})^{k+1}.$$

295. Доказати да су бројеви $2^m - 1$ и $2^n - 1$ узајамно прости ако и само ако су m и n узајамно прости.

Решење. Нека је $D(m,n) = (2^n - 1, 2^m - 1)$. Нека је нпр. $n > m$. Тада имамо:

$$\begin{aligned} D(m,n) &= ((2^n-1)-(2^m-1), 2^m-1) \\ &= \big(2^m(2^{n-m}-1), 2^m-1\big) \\ &= \big(2^{n-m}-1, 2^m-1\big) \\ &= D(m, n-m). \end{aligned}$$

Применом Еуклидовог алгоритма за добијање највећег заједничког делиоца бројева m и n добијамо:

$$\begin{aligned} D(m,n) &= D(m,n-m) = \cdots = D(m,r_1) \\ &= D(m-r_1, r_1) = \cdots = D(r_2, r_1) = \cdots = D(r_k, 0). \end{aligned}$$

Међутим, $D(r_k, 0) = (2^{r_k} - 1, 2^0 - 1) = 2^{r_k} - 1$. Коначно: m и n су узајамно прости ако и само ко је $r_k = 1$, а то је еквивалентно са

$$(2^n - 1, 2^m - 1) = 2^1 - 1 = 1,$$

тј. са чињеницом да су $2^m - 1$ и $2^n - 1$ узајамно прости.

296. Ако су m и n природни бројеви, доказати да је

$$(2^m - 1, 2^n - 1) = 2^{(m,n)} - 1.$$

297. Наћи све природне бројеве n за које је $2^n - 1$ дељиво са n.

Решење. Претпоставимо да $n \mid 2^n - 1$. Како је $2^n - 1$ непаран број и $n \mid 2^n - 1$, n је непаран број. За $n = 1$ услов је очигледно испуњен. Нека је сада $n \geqslant 3$. Нека је p најмањи прост фактор од n. С обзиром на то да је n непаран број не мањи од 3, p је такође непаран број не мањи од 3. Из услова задатка следи $p \mid 2^n - 1$, а на основу Мале Фермаове теореме $p \mid 2^{p-1} - 1$. На основу задатка 296 је

$$(2^n - 1, 2^{p-1} - 1) = 2^{(n,p-1)} - 1.$$

Из $p \mid 2^n - 1$ и $p \mid 2^{p-1} - 1$ следи $p \mid 2^{(n,p-1)} - 1$. Међутим, $(n, p-1) = 1$, јер је p најмањи прост фактор од n. Дакле, $p \mid 1$, а то је контрадикција, јер је $p \geqslant 3$.

298. (ИМО 1990) Одреди све природне бројеве $n > 1$ за које важи $n^2 \mid 2^n + 1$.

Решење. Ако је n паран број, онда број $2^n + 1$ није дељив са n^2.

Претпоставимо да за неки непаран број $n \geqslant 3$ важи $n \mid 2^n + 1$ и нека је p најмањи прост делилац броја n. Тада је p такође непаран број и важи

$$p \mid (2^n + 1)(2^n - 1) = 2^{2n} - 1. \tag{1}$$

На основу Мале Фермаове теореме добијамо и следећу релацију:

$$p \mid 2^{p-1} - 1. \tag{2}$$

С обзиром на то да је најмањи прост делилац броја n једнак p следи

$$(2n, p-1) = 2. \tag{3}$$

На основу задатка 296 из релација (1), (2) и (3) закључујемо да $p \mid 2^2 - 1 = 3$, тј. $p = 3$. Према томе, $n = 3m$ за неки природан број m. Ако је $m = 1$, онда је $n = 3$ и с обзиром на то да је $\dfrac{2^3 + 1}{3^2} = 1$, то следи да је $n = 3$ једно решење задатка.

Докажимо да других решења нема. Означимо са q најмањи прост делилац броја m. Размотримо прво случај $q = 3$. Тада је $n = 3^k \cdot m_1$, где је $k \geqslant 2$, а бројеви m_1 и 3 су узајамно прости. Ако је број $2^n + 1$ дељив са n^2, онда је он дељив и са 3^{2k}. Користећи чињеницу да је n непаран број, добијамо:

$$\begin{aligned} 2^n + 1 &= 1 + (-1 + 3)^n = 1 + \sum_{i=0}^{n} \binom{n}{i} (-1)^{n-i} 3^i \\ &= 1 + (-1) + 3n - \binom{n}{2} 3^2 + \cdots + 3^n. \end{aligned}$$

Из ове једнакости следи да је број $3n = 3^{k+1}m_1$ дељив са 3^{k+2}, што је у контрадикцији са условом да су m_1 и 3 узајамно прости бројеви. Размотримо сада случај $q \geqslant 5$. С обзиром на то да су бројеви $2^{2n}-1$ и $2^{q-1}-1$ дељиви са q, то на основу претходног задатка следи да је број $2^{(2n,q-1)}-1$ дељив са q. При томе, $d = (2n, q-1) = (6m, q-1) \in \{2, 6\}$, јер је q најмањи прост делилац броја m. Не може бити $d = 2$ јер тада број $2^2 - 1 = 3$ није дељив са $q \geqslant 5$. За $d = 6$ добијамо $2^d - 1 = 2^6 - 1 = 63$, одакле следи да је $q = 7$. Из услова да је број $2^3 - 1$ дељив са 7, следи да је број $2^n - 1 = 2^{3m} - 1$ дељив са 7, а број $2^n + 1 = (2^n - 1) + 2$ није дељив са 7, па према томе ни са n. Тиме је доказ завршен.

299. Одредити природан број n такав да је збир $1+2+3+\cdots+n$ троцифрен број чије су све цифре једнаке.

Решење. Нека је n природан број и $a \in \{1, 2, 3, \ldots, 9\}$ цифра таква да је

$$1 + 2 + 3 + \cdots + n = \overline{aaa} = a \cdot 100 + a \cdot 10 + a = 111a,$$

тј.

$$\frac{n(n+1)}{2} = 111a,$$

односно

$$n(n+1) = 222a = 2 \cdot 3 \cdot 37 \cdot a.$$

Дакле, треба наћи цифру a такву да се број $2\cdot 3\cdot 37\cdot a$ може представити као производ два узастопна природна броја. Није тешко видети да је $a = 6$, па је $n = 36$.

300. Одредити све двоцифрене бројеве који су једнаки збиру куба цифре десетица и квадрата цифре јединица.

Решење. Нека је тражени број $\overline{ab}$, при чему важи $a \in \{1, 2, \ldots, 9\}$, $b \in \{0, 1, \ldots, 9\}$. Према условима задатка тада је $10a + b = a^3 + b^2$.

Како је $\overline{ab} = 10a + b \leqslant 99$, то је и $a^3 + b^2 \leqslant 99$, па је $1 \leqslant a \leqslant 4$. Трансформацијом дате једначине добија се $10a - a^3 = b^2 - b$, односно $a(10 - a^2) = b(b-1)$, па је $a(10 - a^2)$ паран број, а то значи да је и a паран број. Како је $a(10 - a^2) \geqslant 0$, то је $10 - a^2 \geqslant 0$, па је $a \leqslant 3$. Једино решење је $a = 2$, а тада је $b(b-1) = 12$, па је $b = 4$. Дакле, тражени број је $24 = 2^3 + 4^2$.

301. Одредити све природне бројеве који су 33 пута већи од збира својих цифара.

Решење. Нека је тражени број $\overline{a_{n-1} \ldots a_1 a_0}$, $a_0^2 + \cdots + a_{n-1}^2 \neq 0$, $a_i \in \{0, 1, \ldots, 9\}$ $(i = 0, 1, \ldots, n-1)$. Тада је

$$\begin{aligned} & a_{n-1} \cdot 10^{n-1} + \cdots + 10a_1 + a_0 = 33(a_{n-1} + \cdots + a_1 + a_0) \\ \Leftrightarrow \quad & a_{n-1}\left(10^{n-1} - 33\right) + \cdots + a_2\left(10^2 - 33\right) = 23a_1 + 32a_0. \end{aligned}$$

Лева страна последње неједнакости није мања од $10^{n-1} - 33$, а десна није већа од $23 \cdot 9 + 32 \cdot 9 = 495$, па је та једнакост могућа само за $n \leqslant 3$. Једноцифрених и двоцифрених бројева који задовољавају дати услов нема. За $n = 3$ добијамо

$$\overline{a_2 a_1 a_0} = 100a_2 + 10a_1 + a_0 = 33(a_2 + a_1 + a_0),$$

одакле следи да $3 \mid \overline{a_2 a_1 a_0}$, па онда важи и $3 \mid a_2 + a_1 + a_0$. Сада закључујемо да и $9 \mid \overline{a_2 a_1 a_0}$, а самим тим и $9 \mid a_2 + a_1 + a_0$. Према томе, $a_2 + a_1 + a_0 \in \{9, 18, 27\}$. Провером се показује да једино случај $a_2 + a_1 + a_0 = 18$ даје број 594 који задовољава услове задатка.

302. Одредити све двоцифрене бројеве чији се збир цифара не мења када се ти бројеви помноже са сваким од бројева 2, 3, 4, 5, 6, 7, 8, 9.

303. Доказати да се природан број n може представити у облику збира неколико (бар два) узастопних природних бројева ако и само ако n није степен двојке.

Решење. ($\rightarrow$) Број који може да се представи у задатом облику изгледа овако:

$$\begin{aligned} n &= m + (m+1) + \cdots + (m+k-1) \\ &= km + (1 + 2 + \cdots + (k-1)) \\ &= km + \frac{k(k-1)}{2} = \frac{k(2m+k-1)}{2}\,. \end{aligned}$$

Како су k и $2m+k-1$ различите парности, и оба већа од 1, закључујемо да n садржи непаран чинилац већи од 1, па не може бити степен двојке.

($\leftarrow$) Нека је $n = 2^p q$, где је $q > 1$ непаран број. Можемо, за $m = 2^p$ и $q = 2k+1$, записати:

$$n = (m-k) + (m-k+1) + \cdots + (m+k).$$

Могуће је наравно и да је $m - k \leqslant 0$. У том случају из записа избацујемо првих $k-m$ (негативних) бројева, нулу и следећих $k-m$ бројева (који су позитивни).

304. Доказати да број који се у декадном запису пише коришћењем једино цифара 2 и 6 није разлика квадрата два цела броја.

Решење. Нека је c број који се у декадном запису пише коришћењем једино цифара 2 и 6. Очигледно је c паран број. Ако постоје цели бројеви a и b такви да је $a^2 - b^2 = c$, онда они не могу бити различите парности јер би тада разлика њихових квадрата била непаран природан број. Дакле, имамо два случаја:

1. $a = 2m$ и $b = 2n$, за неке m и n. Тада је $a^2 - b^2 = 4(m^2 - n^2)$, па $4 \mid c$;

2. $a = 2m+1$ и $b = 2n+1$, за неке m и n. Тада је $a^2 - b^2 = 4(m^2 + m - n^2 - n)$, па, поново $4 \mid c$.

Међутим, двоцифрени завршетак броја c је: 22, 26, 62 или 66, тј. $4 \nmid c$.

Дакле, не постоје цели бројеви a и b такви да је $a^2 - b^2 = c$.

305. Доказати да збир квадрата пет узастопних целих бројева не може бити потпун квадрат.

Решење. Број

$$(n-2)^2 + (n-1)^2 + n^2 + (n+1)^2 + (n+2)^2 = 5n^2 + 10 = 5(n^2+2)$$

је дељив са 5, али није са 25, јер су једино 1, 2 и 3 могући остаци при дељењу броја n^2+2 са 5, па број $5(n^2+2)$ не може бити потпун квадрат.

306. (ЈБМО 2003) Нека је n позитиван цео број. Број A се састоји од $2n$ цифара и свака од њих је 4, број B се састоји од n цифара и свака од њих је 8. Доказати да је $A + 2B + 4$ потпун квадрат.

Решење:

$$\begin{aligned}
A + 2B + 4 &= \underbrace{444\ldots44}_{2n} + 2 \cdot \underbrace{888\ldots88}_{n} + 4 = \\
&= 4 \cdot \underbrace{111\ldots11}_{2n} + 2 \cdot 8 \cdot \underbrace{111\ldots11}_{n} + 4 = \\
&= 4 \cdot \frac{1}{9} \cdot \underbrace{999\ldots99}_{2n} + 2 \cdot 8 \cdot \frac{1}{9} \cdot \underbrace{999\ldots99}_{n} + 4 = \\
&= 4 \cdot \frac{10^{2n}-1}{9} + 16 \cdot \frac{10^n - 1}{9} + 4 = \\
&= \frac{4}{9} \cdot (10^{2n} + 4 \cdot 10^n - 1 - 4 + 9) = \\
&= \left(\frac{2(10^n+2)}{3}\right)^2 = \underbrace{66\ldots6}_{n-1}8^2\,.
\end{aligned}$$

307. Ако су a, b, c цели бројеви такви да је $a+b+c=0$, доказати да је $2a^4+2b^4+2c^4$ потпун квадрат.

Решење. Нека је $P(x)=x^3+px^2+qx+r$ полином чије су нуле a, b, c. Према Виетовим формулама, пошто је $a+b+c=0$, имамо да је $p=0$, па је:

$$a^3+qa+r=0, \quad b^3+qb+r=0, \quad c^3+qc+r=0.$$

Ако последње три једнакости помножимо редом са $2a$, $2b$, $2c$ и саберемо их добијамо:

$$(*) \qquad 2a^4+2b^4+2c^4+2q(a^2+b^2+c^2)+2r(a+b+c)=0.$$

Према услову задатка је $a+b+c=0$, према Виетовим формулама је $ab+bc+ca=q$, па је

$$a^2+b^2+c^2=(a+b+c)^2-2(ab+bc+ca)=-2q,$$

те из једнакости $(*)$ имамо

$$2a^4+2b^4+2c^4=4q^2=(2q)^2,$$

што је и требало доказати.

308. За које природне бројеве n је:
(а) 2^n-1, (б) 2^n+1
потпун квадрат?

Решење. (а) За $n=1$ је $2^n-1=1=1^2$.
За $n>1$ је $2^n-1\equiv -1 \pmod 4$, па не може бити потпун квадрат.
(б) Једначина $2^n+1=k^2$ еквивалентна је следећој једначини: $2^n=(k-1)(k+1)$, одакле је $k-1=2^m$ и $k+1=2^\ell$ $(m<\ell)$, па је

$$2=2^\ell-2^m=2^m\left(2^{\ell-m}-1\right).$$

Сада се лако види да је $m = 1$ и $\ell - m = 1$, тј. $\ell = 2$, одакле је $2^n = 2^2 \cdot 2 = 2^3$, односно $n = 3$.

309. Да ли постоји природан број n такав да је $n^n + 1$ потпун квадрат?

Решење. Нека је $n^n + 1 = m^2$. Број n не може бити паран, јер је у том случају n^n потпун квадрат, па следећи број не може бити потпун квадрат. Посматрајмо случај кад је n непаран број. Тада је $n^n = m^2 - 1 = (m-1)(m+1)$, при чему су $m - 1$ и $m + 1$ непарни бројеви. Бројеви $m - 1$ и $m + 1$ су узајамно прости (као узастопни непарни бројеви). Сваки од та два броја је n–ти степен природног броја. Међутим, разлика n–тих степена два природна броја је већа од 2. Контрадикција. Тражени број не постоји.

310. Наћи најмањи природан број n такав да је

$$\frac{1^2 + 2^2 + \cdots + n^2}{n}$$

потпун квадрат.

Решење. Пошто је

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6},$$

једнакост

$$\frac{1^2 + 2^2 + \cdots + n^2}{n} = m^2$$

еквивалентна је са

$$\frac{(n+1)(2n+1)}{6} = m^2,$$

тј.

$$(n+1)(2n+1) = 6m^2. \tag{$*$}$$

Како је $2n+1$ непаран број, $n+1$ је паран, па је n непаран број, тј. $n = 2k-1$, за неки природан број k. Сада, једнакост $(*)$ можемо записати у облику

$$k(4k-1) = 3m^2,$$

одакле следи да $3 \mid k$ или $3 \mid 4k-1$.

Ако $3 \mid k$, тј. $k = 3s$, за неки s, имамо да је $s(12s-1) = m^2$. Пошто су бројеви s и $12s-1$ узајамно прости следи да је $s = u^2$ и $12s-1 = v^2$, за неке u и v, што је немогуће јер $3 \mid 12u^2$ па v^2 при дељењу са 3 даје остатак 2.

Дакле, $3 \mid k-1$, тј. $k = 3t+1$, за неки t, па је $(3t+1)(4t+1) = m^2$, а пошто је $(3t+1, 4t+1) = 1$, следи да је $3t+1 = x^2$ и $4t+1 = y^2$, за неке природне бројеве x и y веће од 1. Како y мора бити непаран број, додељујући промењивој y редом вредности: 3, 5, 7, 9, 11, 13, 15, …, добијамо редом вредности за t: 2, 6, 12, 20, 30, 42, 56, …, тј. за $3t+1$: 7, 19, 37, 61, 91, 127, <u>169</u>, …

Дакле, $k = 169$ је најмањи потпуни квадрат, па је $n = 2k-1 = 2 \cdot 169 - 1 = 337$.

311. (Савезно такмичење 1998, II разред) Доказати да не постоји природан број n такав да је $8^n + 2^n + 1$ потпун квадрат.

Решење. Нека је $n = 2k$, где је $k \in \mathbb{N}$. Тада важи

$$\left(2^{3k}\right)^2 = 2^{6k} < 2^{6k} + 2^{2k} + 1 < 2^{6k} + 2 \cdot 2^{3k} + 1 = \left(2^{3k}+1\right)^2,$$

одакле следи да број $8^n + 2^n + 1 = 2^{6k} + 2^{2k} + 1$ није потпун квадрат.

Ако је $n = 2k+1$, где је $k \geqslant 0$ цео број, онда важи

$$8^n + 2^n + 1 = 2^{6k+3} + 2^{2k+1} + 1 \equiv 2 + 2 + 1 \equiv 2 \pmod 3.$$

Како квадрати природних бројева при дељењу са 3 дају остатке 0 или 1, то ни у овом случају број $8^n + 2^n + 1$ није потпун квадрат.

312. Наћи све просте бројеве p за које је $p^3 - p + 1$ потпун квадрат.

Решење. Нека је $p^3 - p + 1 = n^2$, тј. $p(p^2-1) = (n-1)(n+1)$. Имамо два случаја:

1. $p \mid n-1$. Тада је $n-1 = kp$ за неко $k \in \mathbb{N}$ па добијамо да је $p(p-k^2) = 2k+1$. Одатле следи $p - k^2 \geqslant 1$ и $p \leqslant 2k+1$, одакле је $k^2+1 \leqslant 2k+1$, односно $k=1$ или $k=2$. За $k=2$ добијамо $p=5$, а $k=1$ не даје решење;

2. $p \mid n+1$. Тада је $n+1 = lp$ за неко $l \in \mathbb{N}$ па добијамо $2l-1 = p(l^2-p)$. Пошто је $p \geqslant 3$ (директно проверавамо) и $l^2 - p \geqslant 1$, следи $l \geqslant 2$ и $p \leqslant 2l-1$ па имамо

   $$2l-1 = p(l^2-p) \geqslant p(l^2-2l+1) \geqslant 3(l-1)^2 \geqslant 3(l-1) \geqslant 2l-1.$$

   Значи, све те неједнакости морају бити једнакости, па је $l=2$ и $p=3$.

313. Наћи све природне бројеве n такве да је број

$$2^4 \cdot 3^{16} + 5^2 \cdot 3^{14} + 3^n$$

потпун квадрат.

Решење. 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 следи 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 $n > 14$. 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 $(v + 13) - (v - 13) = 26$ следи једина могућност $v - 13 = 1$ и $v + 13 = 3^k$. Дакле, $v = 14$ и $27 = 3^k$, тј. $k = 3$ и $n - 14 = 3$. Најзад, добијамо да је $n = 17$.

314. Доказати да број од 1 000 цифара које су све петице осим можда једне не може бити потпун квадрат.

Решење. Нека је n дати број. Ако би све цифре броја биле петице, или би једна била различита од 5, а налазила се на неком од првих 998 места, број не би био потпун квадрат, јер би био дељив са 5, али не и са 25. Нека је та цифра на претпоследњем месту. Ако је она различита од 2 и 7, резонујемо као горе. Ако би она била 2, имали би $n \equiv 2 \pmod 9$, а за седмицу $n \equiv 7 \pmod{16}$, а ни једно ни друго није могуће за квадрат природног броја. Нека је, дакле, цифра различита од 5 на последњем месту. Ако је она 0, 4 или 8, важи $n \equiv 2 \pmod 4$, ако је једнака 1 или 9, имамо $n \equiv 3 \pmod 4$, за тројку и шестицу $n \equiv \pm 3 \pmod 9$, а ништа од тога не може важити за квадрате. Коначно, $55\ldots57 \equiv 5 \pmod{16}$, а $55\ldots52$ је дељиво са 32, а није дељиво са 64, тако да и ови случајеви не долазе у обзир.

315. (Изборно такмичење за ЈБМО 2004) Да ли постоји деветоцифрени природан број чије су све цифре међусобно различите и различите од 0, који је дељив са 5 и потпун је квадрат?

Решење. Претпоставимо да постоји такав број D. Пошто је $D = A^2$ и $A = 10a + 5$ из

$$A^2 = 100a^2 + 100a + 25 = 100a(a + 1) + 25$$

следи да је цифра стотина броја D једнака 2.

На основу следеће табеле

$a \equiv \cdot \pmod{10}$	0	1	2	3	4	5	6	7	8	9
$a(a+1) \equiv \cdot \pmod{10}$	0	2	6	2	0	0	2	6	2	0

закључујемо да је цифра хиљада броја D: $0, 2$ или 6, па према условима задатка то може бити једино цифра 6 (цифре 2 и 5 су већ употребљене, а 0 је искључена). Дакле, $D = 1\,000b + 625$, па $125 \mid D$. Пошто је $D = A^2$, то следи да $5^4 \mid D$, па цифра десетина хиљада броја D мора бити или 0 или 5. Контрадикција.

316. Да ли потпун квадрат може бити број чије су цифре само нуле и шестице?

317. (Зимско математичко такмичење, Бугарска 2000, 8. разред) Наћи све просте бројеве p и q такве да је израз $p^2 + 3pq + q^2$

(а) потпун квадрат;

(б) степен броја 5.

Решење. (а) Нека је $p^2 + 3pq + q^2 = r^2$, где су p, q прости бројеви и $r > 0$ цео број. Ако је $p \neq 3$ и $q \neq 3$ тада је

$$p^2 + 3pq + q^2 \equiv 2 \pmod 3,$$

па је $r^2 \equiv 2 \pmod 3$, што је немогуће. Не умањујући општост претпоставимо да је $p = 3$. Тада је $q^2 + 9q + 9 = r^2$. Последња једначина еквивалентна је са $(2q + 9)^2 - 45 = (2r)^2$, односно са

$$(2q - 2r + 9)(2q + 2r + 9) = 45.$$

Пошто је $r > 0$ то је $2q + 2r + 9 = 15$ или $2q + 2r + 9 = 45$. У првом случају је $q + r = 3$, што је немогуће, а у другом случају решавањем система $q + r = 18$, $2q - 2r + 9 = 1$ добијамо $q = 7$. Због симетрије решења су $p = 3, q = 7$ и $p = 7, q = 3$.

(б) Претпоставимо да је $p^2 + 3pq + q^2 = 5^n$, где је n природан број. Пошто је $p \geqslant 2$ и $q \geqslant 2$ то је $p^2 + 3pq + q^2 \geqslant 20$, па је $n \geqslant 2$. Даље следи да $25 \mid p^2 + 3pq + q^2$ и $5 \mid p^2 + 3pq + q^2 = (p - q)^2 + 5pq$, одакле закључујемо да $5 \mid (p - q)^2$, што имплицира да и $25 \mid (p - q)^2$, а одатле следи да $25 \mid 5pq$, тј. бар један од бројева p и q мора бити једнак 5. Ако је $p = 5$ тада је и $q = 5$ (и обрнуто) и добијамо $p^2 + 3pq + q^2 = 125 = 5^3$. Дакле, једино решење је $p = q = 5$.

318. (Аустралијска математичка олимпијада, 2002) Нека су m и n природни бројеви такви да је $2\,001m^2 + m = 2\,002n^2 + n$. Доказати па је $m - n$ потпун квадрат.

Решење. Дату једнакост можемо записати у облику

$$(m-n)(1 + 2\,001(m+n)) = n^2.$$

Претпоставимо да $m - n$ није потпун квадрат. Тада постоји неки прост број p такав да $p \mid m - n$ и $p \mid 1 + 2\,001(m + n)$. Пошто $p \mid n^2$ следи да $p \mid n$ (p прост број). Даље, $p \mid (m - n) + n$, тј. $p \mid m$, па $p \mid m + n$ и $p \mid 2\,001(m + n)$. Међутим, то је немогуће јер $p \mid 1 + 2\,001(m + n)$. Дакле, бројеви $m - n$ и $1 + 2\,001(m + n)$ су узајамно прости. Пошто је њихов производ потпун квадрат, то и они морају бити потпуни квадрати. Дакле, $m - n$ је потпун квадрат.

319. (Савезно такмичење 1986, II разред) Нека су x и y природни бројеви који задовољавају једначину $2x^2 + x = 3y^2 + y$. Доказати да су бројеви $x - y$, $2x + 2y + 1$ и $3x + 3y + 1$ потпуни квадрати.

Решење. Из $2x^2 + x = 3y^2 + y$ следи:

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

$$y^2 = x - y + 2x^2 - 2y^2 = (x - y)(1 + 2x + 2y).$$

Како су бројеви $3x + 3y + 1 = 3(x + y) + 1$ и $2x + 2y + 1 = 2(x + y) + 1$ узајамно прости, следи да је

$$x - y = (x^2, y^2) = [(x, y)]^2\,.$$

Из наведених израза за x^2 и y^2 сада следи и да су бројеви $3x + 3y + 1$ и $2x + 2y + 1$ такође потпуни квадрати.

320. Доказати да не постоје цели бројеви x и y за које важи

$$(x+y+2)^2 = 3(xy+1).$$

Решење. За сваки природан број m важи тврђење: $3 \mid m^2 \Rightarrow 3 \mid m$, тј. $3 \mid m^2 \Rightarrow 9 \mid m^2$.

Ако би постојали цели бројеви x и y за које важи $(x+y+2)^2 = 3(xy+1)$ имали би да $3 \mid (x+y+2)^2$, па и да $3 \mid (x+y+2)$ и да $3 \mid (xy+1)$.

Из $3 \mid (xy+1)$ следи да ни један од бројева x и y не може бити дељив са 3, нити оба могу давати једнаке остатке при дељењу са 3. (На пример, ако би било $x = 3m+1$ и $y = 3n+1$ за неке m и n, имали би да је $xy+1 = (3m+1)(3n+1)+1 = 3(3mn+m+n)+2$.) Дакле, из $3 \mid (xy+1)$ следи да један од бројева при дељењу са 3 даје остатак 1, а други остатак 2. Нека је $x = 3m+1$ и $y = 3n+2$ за неке m и n. Али тада је $x+y+2 = 3(m+n+1)+2$, што је немогуће јер $3 \mid (x+y+2)$.

Дакле, не постоје цели бројеви x и y такви да је $(x+y+2)^2 = 3(xy+1)$.

321. (Чешко-словачка математичка олимпијада – прва рунда, 2003) Наћи највећи четвороцифрен палиндром, такав да је његов квадрат такође палиндром.

Решење. Сваки четвороцифрен палиндром $p = \overline{abba}$ може се записати у облику

$$p = a \cdot 1001 + b \cdot 110, \quad a \in \{1,2,\dots,9\},\ b \in \{0,1,\dots,9\}.$$

Квадрат броја $\overline{abba}$ је облика

$$\begin{aligned} p^2 &= a^2 \cdot 1\,002\,001 + 2ab \cdot 110\,110 + b^2 \cdot 12\,100 \\ &= a^2 \cdot 10^6 + 2ab \cdot 10^5 + (b^2+2ab) \cdot 10^4 \\ &\quad +(2a^2+2b^2) \cdot 10^3 + (b^2+2ab) \cdot 10^2 + 2ab \cdot 10^1 + a^2. \end{aligned}$$

Последња цифра броја p^2 је иста као и последња цифра броја a^2.

Ако је $a \geqslant 4$, број p^2 има осам цифара. Његова прва цифра је елемент скупа $\{c, c+1, c+2\}$, где је c прва цифра броја a^2. Пошто је и p^2 палиндром, то су његова прва и последња цифра једнаке. Упоређујући прву и последњу цифру бројева $16, 25, 36, 49, 64, 81$ видимо да ниједан од њих није облика $\overline{c(c+2)}$, $\overline{c(c+1)}$ или $\overline{cc}$.

Ако је $a = 3$ и $b \geqslant 2$, број p^2 опет има осам цифара. Тада је његова последња цифра 9, а прва 1, па он није палиндром.

У свим осталим случајевима број p^2 има седам цифара. Тада је број a^2 једноцифрен и сваки од бројева $2ab$, $2ab + b^2$, $2a^2 + 2b^2$ мора бити мањи од 10. Размотрићемо следеће случајеве:

(1) $a = 3$. Тада неједнакост $2 \cdot 3^2 + 2b^2 < 10$ није тачна ни за једно b;

(2) $a = 2$. Тада је неједнакост $2 \cdot 2^2 + 2b^2 < 10$ тачна само за $b = 0$;

(3) $a = 1$. Неједнакост $2 \cdot 1^2 + 2b^2 < 10$ тачна је за $b = 0$ и $b = 1$.

Према томе, решење задатка је број $2\,002$ ($2\,002^2 = 4\,008\,004$).

322. (Предлог за XXX ИМО) Доказати да низ $a_n = \left[n\sqrt{2}\right]$, $n \in \mathbb{N}$, садржи бесконачно много потпуних квадрата.

Решење. Нека је (x_n, y_n), $n \in \mathbb{N}$, бесконачан низ решења једначине $x^2 - 2y^2 = -1$ у скупу природних бројева (видети задатак 238). За произвољно n имамо да је $x_n^2 - 2y_n^2 = -1$, одакле је $x_n^4 + x_n^2 = 2x_n^2 y_n^2$ и

$$\left[\sqrt{2x_n^2 y_n^2}\right] = \left[x_n y_n \sqrt{2}\right] = x_n^2$$

јер је

$$x_n^2 < \sqrt{x_n^4 + x_n^2} = x_n y_n \sqrt{2} < \sqrt{x_n^4 + 2x_n^2 + 1} = x_n^2 + 1.$$

323. (Изборно такмичење за ЈБМО 2004) Ако је разлика кубова два узастопна природна броја једнака n^2, тада је број n једнак збиру квадрата нека два природна броја. Доказати.

Решење. Нека је $(m+1)^3 - m^3 = n^2$, где је m неки природан број. Тада је n^2, а отуда и n, непаран број. Дакле, $(m+1)^3 - m^3 = (2p+1)^2$. То се даље може представити у облику:

$$\begin{aligned} 3m^2 + 3m + 1 &= (2p+1)^2 \\ 4(3m^2 + 3m + 1) - 1 &= 4(2p+1)^2 - 1 \\ 3(4m^2 + 4m + 1) &= (2(2p+1) - 1)(2(2p+1) + 1) \\ 3(2m+1)^2 &= (4p+1)(4p+3). \end{aligned}$$

Како су бројеви $4p+1$ и $4p+3$ узајамно прости, а њихов производ једнак $3(2m+1)^2$, један од њих је потпун квадрат. То не може да буде $4p+3$, јер квадрат сваког непарног броја даје остатак 1 при дељењу са 4. Отуда је $4p+1 = (2t+1)^2$, односно

$$\begin{aligned} 4p + 1 &= 4t^2 + 4t + 1 \\ 2p + \frac{1}{2} &= 2t^2 + 2t + \frac{1}{2} \\ 2p + 1 &= t^2 + t^2 + 2t + 1 \\ 2p + 1 &= t^2 + (t+1)^2. \end{aligned}$$

324. (Национална математичка олимпијада–финална рунда, Румунија 2003, 8. разред) Нека су m и n природни бројеви. Доказати да се број $5^n + 5^m$ може представити као збир два потпуна квадрата ако и само ако је број $m - n$ паран.

Решење. Ако су m и n оба парни тада је $m = 2k$, $n = 2l$ и $5^{2k} + 5^{2l} = \left(5^k\right)^2 + \left(5^l\right)^2$.

Ако су и m и n непарни тада је $m = 2k+1$, $n = 2l+1$ и

$$5^{2k+1} + 5^{2l+1} = \left(5^k + 2\cdot 5^l\right)^2 + \left(5^l - 2\cdot 5^k\right)^2.$$

Нека су m и n различите парности. Тада је

$$5^m + 5^n = 5^{2k+1} + 5^{2l} \equiv 6 \pmod{8}.$$

Како квадрати природних бројева при дељењу са 8 дају остатке 0, 1 или 4, то збир два квадрата не може бити конгруентан са 6 по модулу 8, па се број $5^m + 5^n$ не може представити као збир два квадрата.

325. За које природне бројеве n је број

$$n(n+1)(n+2)\cdots(n+7) + 1\cdot 2\cdot 3\cdot \ldots \cdot 7$$

могуће представити као збир квадрата два природна броја?

Решење. Ни за једно n. Заиста, нека је за $n, m, k \in \mathbb{N}$

$$n(n+1)(n+2)\cdots(n+7) + 1\cdot 2\cdot 3\cdot \ldots \cdot 7 = m^2 + k^2.$$

Број $n(n+1)(n+2)\cdots(n+7)$ дељив је са 2^7, јер су четири фактора дељива са 2, од тога два са 4, а један и са 8. Број $1\cdot 2\cdot 3\cdot \ldots \cdot 7$ дељив је са 2^4, али не и са 2^5. Значи, лева страна горње једнакости дељива је са 16, па мора бити и десна. Како су остаци при дељењу квадрата природног броја са 16 само 0, 1, 4 и 9, следи да су и m^2 и k^2 дељиви са 16, тј. $m = 4m_1, k = 4k_1$. Делећи горњу једнакост са 16 на левој страни добијамо број конгруентан са 3 по модулу 4, а са десне $m_1^2 + k_1^2$, што не може бити конгруентно са 3 по модулу 4. Контрадикција.

326. (Савезно такмичење 1986, I разред) Доказати да постоји бесконачно много тројки узастопних природних бројева од којих је сваки збир два потпуна квадрата. (Пример: $72 = 6^2+6^2$, $73 = 8^2+3^2$, $74 = 7^2 + 5^2$.)

Решење. За произвољан природан број n важи:

$$n^2 + n^2 = 2n^2, \qquad (n-1)^2 + (n+1)^2 = 2n^2 + 2.$$

Зато је довољно доказати да постоји бесконачно много природних бројева n таквих да за неке целе бројеве a и b важи

$$(n-a)^2 + (n-b)^2 = 2n^2 + 1,$$

односно

$$n^2 - 2an + a^2 + n^2 - 2bn + b^2 = 2n^2 + 1,$$

тј.

$$2n(a+b) = a^2 + b^2 - 1.$$

Ако за произвољан природан број b узмемо $a = 1 - b$ и $n = b(b-1)$ тада ће важити

$$2n(a+b) = 2b(b-1)(1-b+b) = 2b^2 - 2b$$

и

$$a^2 + b^2 - 1 = (1-b)^2 + b^2 - 1 = 1 - 2b + b^2 + b^2 - 1 = 2b^2 - 2b.$$

327. Показати да постоји бесконачно много природних бројева који се не могу представити као сума квадрата три природна броја.

Решење. Квадрат природног броја може при дељењу са 8 давати остатке 0, 1 и 4. Ниједна комбинација три од ових бројева не може у збиру дати 7, па збир квадрата три природна броја не може бити облика $8k+7$, а природних бројева тог облика има бесконачно много.

328. (Зимско математичко такмичење, Бугарска 1999, 8. разред) Нека је $n \neq 2$ природан број. Наћи све целе бројеве m такве да је $k = m \cdot 2^{n-2}$ цео број и $A = 1\,999^k + 6$ сума n потпуних квадрата (не обавезно различитих и различитих од нуле).

Решење. Пошто је A цео број то треба разматрати само ненегативне целе бројеве m.

(1) Ако је $n = 1$ онда је $k = \dfrac{m}{2}$ цео број ако и само ако је $m = 4p$ или $m = 4p + 2$. Ако је $m = 4p$ индукцијом се може показати да је $A \equiv 3 \pmod 4$, па A није потпун квадрат. Ако је $m = 4p + 2$ тада је $A \equiv 5 \pmod{25}$, па није потпун квадрат ($5 \mid A$, али $25 \nmid A$).

(2) Ако је $n = 3$, тада је $k = 2m$ и $A = (8 \cdot 250 - 1)^{2m} + 6$, па је $A \equiv 7 \pmod 8$, што је немогуће за збир три потпуна квадрата.

(3) Ако је $n \geqslant 4$, тада је

$$A = \left(1\,999^{m\cdot 2^{n-3}}\right)^2 + 2^2 + 1^2 + 1^2 + 0^2 + \cdots + 0^2$$

збир n потпуних квадрата.

Према томе, за $n = 1$ или $n = 3$ нема решења, а за $n \geqslant 4$ свако $m \geqslant 0$ је решење.

329. (ИМО 1992) За сваки природан број n са $S(n)$ означимо највећи природан број, такав да за свако цело k, $1 \leqslant k \leqslant S(n)$, број n^2 може бити представљен у облику збира k квадрата природних бројева.

(а) Доказати да је $S(n) \leqslant n^2 - 14$ за свако $n \geqslant 4$.

(б) Наћи природан број n, такав да је $S(n) = n^2 - 14$.

(в) Доказати да постоји бесконачно много природних бројева n, таквих да је $S(n) = n^2 - 14$.

Решење. (а) Претпоставимо да се број n^2 може представити као збир $k = n^2 - 13$ квадрата природних бројева: $n^2 = x_1^2 + x_2^2 + \cdots + x_k^2$; онда се 13 може представити као збир бројева облика $x^2 - 1$, $x \in \mathbb{N}$:

$$13 = n^2 - k = (x_1^2 - 1) + (x_2^2 - 1) + \cdots + (x_k^2 - 1).$$

Лако је видети да је то немогуће, тј. да се 13 не може преставити као збир бројева 0, 3, 8, 15, ... Зато је $S(n) \leqslant n^2 - 14$.

(б) Докажимо да је $S(13) = 13^2 - 14 = 155$. Ако је неки број представљен у облику збира k квадрата, од којих је један паран, онда можемо да га представимо у облику збира $k+3$ квадрата тако што сабирак који је квадрат парног броја разбијемо на четири квадрата: $(2x)^2 = x^2 + x^2 + x^2 + x^2$. Полазећи од једнакости

$$13^2 = 8^2 + 8^2 + 4^2 + 4^2 + 3^2,$$

број 13^2 можемо представити као збир k квадрата природних бројева за $k = 5, 8, 11, \ldots, 155$. Слично, из

$$13^2 = 8^2 + 8^2 + 4^2 + 4^2 + 2^2 + 2^2 + 1^2$$

добијамо репрезентацију броја 13^2 у облику збира $k = 7, 10, 13, \ldots,$ 154 квадрата природних бројева, а из

$$13^2 = 8^2 + 8^2 + 4^2 + 3^2 + 3^2 + 2^2 + 1^2 + 1^2 + 1^2$$

добијамо репрезентацију броја 13^2 у облику збира $k = 9, 12, 15, \ldots,$ 153 квадрата природних бројева. Преостало је још да покажемо да се 13^2 може представити као збир $k = 2, 3, 4, 6$ квадрата природних бројева:

$$\begin{aligned} 13^2 &= 12^2 + 5^2 \\ &= 12^2 + 4^2 + 3^2 \\ &= 11^2 + 4^2 + 4^2 + 4^2 \\ &= 12^2 + 3^2 + 2^2 + 2^2 + 2^2 + 2^2. \end{aligned}$$

(в) Нека је $S(n) = n^2 - 14$ за неко $n \geqslant 13$. Доказаћемо да је $S(2n) = (2n)^2 - 14$. Ако n^2 може да се представи као збир k квадрата природних бројева, полазећи од

$$(2n)^2 = (2x_1)^2 + (2x_2)^2 + \cdots + (2x_k)^2,$$

разбијањем парних квадрата добијамо репрезентацију броја n^2 у облику збира $k, k+3, \ldots, 4k$ квадрата. Значи да се број $(2n)^2$ може представити као збир k квадрата природних бројева, за $1 \leqslant k \leqslant 4n^2 - 62$.

Ако је $4n^2 - 63 \leqslant k \leqslant 4n^2 - 14$, онда је $14 \leqslant 4n^2 - k \leqslant 63 \leqslant 4 \cdot 13^2 - 63 \leqslant k$. Лако је доказати да се сваки број $m \geqslant 14$ може представити као збир $k \geqslant m$ бројева облика $x^2 - 1$, $x \in \mathbb{N}$. Ако ову чињеницу применимо на $4n^2 - k$, добијамо

$$4n^2 - k = (x_1^2 - 1) + (x_2^2 - 1) + \cdots + (x_k^2 - 1),$$

а одавде $4n^2 = x_1^2 + x_2^2 + \cdots + x_k^2$. Из предходног разматрања следи да је $S(n) = n^2 - 14$ за $n = 2^s \cdot 13$, $s \in \mathbb{N}$.

330. Доказати да ниједан број облика $10\ldots02$ (произвољан број нула) није збир кубова неколико узастопних природних бројева.

Решење. Ако између 1 и 2 нема нула имамо број 12 за који се лако проверава да није збир кубова неколико узастопних природних бројева. Стога се ограничимо на бројеве облика $10\ldots02$.

Претпоставимо да је

$$10\ldots02 = (k+1)^3 + (k+2)^3 + \cdots + n^3$$

за неке природне бројеве k и n. Како је

$$\begin{aligned}
&(k+1)^3 + (k+2)^3 + \cdots + n^3 \\
&= \big(1^3 + 2^3 + \cdots + n^3\big) - \big(1^3 + 2^3 + \cdots + k^3\big) \\
&= \left(\frac{n(n+1)}{2}\right)^2 - \left(\frac{k(k+1)}{2}\right)^2,
\end{aligned}$$

то је

$$10\ldots02 = \left(\frac{n(n+1)}{2}\right)^2 - \left(\frac{k(k+1)}{2}\right)^2.$$

На левој страни је паран број који није дељив са 4 (завршава се са 02), а на десној разлика квадрата два природна броја. Међутим, лако се показује да је разлика квадрата два природна броја или непаран број или паран број дељив са 4. Контрадикција.

331. Два 2 002–цифрена броја m и n су потпуни седми степени. Да ли 4 004–цифрен број који се добија исписивањем броја n иза броја m може бити потпун седми степен?

Решење. Нека је $m = x^7$ и $n = y^7$. Тада је број који се из њих добија надовезивањем

$$10^{2002}x^7 + y^7 = \left(10^{286}x\right)^7 + y^7.$$

Међутим, овај број не може бити потпун седми степен, на основу Велике Фермаове теореме.

332. (Предлог за XXIX ИМО) Нека је

$$a_n = \left[\sqrt{(n+1)^2 + n^2}\right], \quad n \in \{0, 1, 2, \dots\}$$

Доказати да:

(1) постоји бесконачно много природних бројева m таквих да је $a_{m+1} - a_m = 1$;

(2) постоји бесконачно много природних бројева m таквих да је $a_{m+1} - a_m > 1$.

Решење. Потражимо, у скупу природних бројева, решења једначине $(n+1)^2 + n^2 = y^2$, тј. $2n^2 + 2n + 1 = y^2$. Према задатку 238, једначина $x^2 - 2y^2 = -1$ има бесконачно много решења у скупу природних бројева (при чему је прва координата решења непаран број). Стављајући у последњу једначину да је $x = 2n + 1$, добијамо $2n^2 + 2n + 1 = y^2$, одакле следи да и ова једначина има бесконачно много решења у скупу природних бројева. Дакле, за бесконачно много природних бројева n важи:

$$a_n = \left[\sqrt{(n+1)^2 + n^2}\right] = \left[\sqrt{2n^2 + 2n + 1}\right] = \left[\sqrt{y^2}\right] = y.$$

Показаћемо да је

$$y+1<\sqrt{(n+2)^2+(n+1)^2}<y+2,$$

одакле је

$$a_{n+1}=\left[\sqrt{(n+2)^2+(n+1)^2}\right]=y+1,$$

па следи тврђење (1). Наиме, имамо да важи:

$$\begin{aligned}
&y+1<\sqrt{2n^2+6n+5}<y+2\\
\Leftrightarrow\ &y^2+2y+1<2n^2+6n+5<y^2+4y+4\\
\Leftrightarrow\ &2y+1<4n+4<4y+4\\
\Leftrightarrow\ &n<y<2n+\frac{3}{2}\\
\Leftrightarrow\ &n^2<y^2<4n^2+6n+\frac{9}{4}\\
\Leftrightarrow\ &n^2<2n^2+2n+1<4n^2+6n+\frac{9}{4},
\end{aligned}$$

при чему су последње неједнакости очигледно тачне.

Пошто је за $y\geqslant 2$, $y^2-3\geqslant (y-1)^2$, имамо да је

$$\left[\sqrt{2n^2+2n+1}\right]=\left[\sqrt{y^2-3}\right]=y-1,$$

јер је $\sqrt{y^2-3}<y$. Значи, да бисмо доказали тврђење (2), довољно је доказати да једначина $2n^2+2n+1=y^2-3$ има бесконачно много решења. Међутим, последња једначина је еквивалентна са $x^2-2y^2=-7$, где је $x=2n+1$, па тврђење следи према задатку 238. Покажимо зато да је

$$\sqrt{(n+2)^2+(n+1)^2}>y+1,$$

одакле ће следити да је $\left[\sqrt{(n+2)^2+(n+1)^2}\right] \geqslant y+1$, па и тврђење (2).

$$\begin{aligned}\sqrt{2n^2+6n+5} \geqslant y+1 &\Leftrightarrow 2n^2+6n+5 \geqslant y^2+2y+1\\ &\Leftrightarrow 2n^2+6n+5-(2n^2+2n+4) \geqslant 2y+1\\ &\Leftrightarrow 4n+1 \geqslant 2y+1 \Leftrightarrow 2n \geqslant y \Leftrightarrow 4n^2 \geqslant y^2\\ &\Leftrightarrow 4n^2 \geqslant 2n^2+2n+4 \Leftrightarrow n^2 \geqslant n+2\\ &\Leftrightarrow n(n-1) \geqslant 2,\end{aligned}$$

што је тачно за $n \geqslant 2$.

333. (Савезно такмичење 1988, III и IV разред) Дат је строго растући низ $a_1, a_2, \dots$ природних бројева, тако да је $a_1 = 1, a_2 = 2$ и за свака два узајамно проста броја m и n важи $a_m \cdot a_n = a_{mn}$. Доказати да за сваки природан број n важи $a_n = n$.

Решење. Из услова задатка следи

$$a_3a_5 = a_{15} < a_{18} = a_2a_9 = 2a_9 < 2a_{10} = 2a_2a_5 = 4a_5$$

$$\Rightarrow a_3 < 4 \Rightarrow a_3 = 3.$$

Докажимо индукцијом да за сваки природан број $n > 3$ важи $a_n = n$.

Претпоставимо да то важи за све природне бројеве мање или једнаке n. Како су $n-1$ и n узајамно прости, то је

$$a_{(n-1)\cdot n} = a_{n-1} \cdot a_n = (n-1) \cdot n.$$

Како је низ (a_n) строго растући, то је $a_k = k$ за све k за које је $n < k \leqslant (n-1) \cdot n$, па специјално и за $k = n+1$, чиме је тврђење задатка доказано.

334. Низ a_n, $n \in \mathbb{N}$, природних бројева задат је на следећи начин: $a_1 = 200$, $a_2 = 1$ и

$$a_{n+2} = \text{остатак при дељењу збира } a_n + a_{n+1} \text{ са } 102,\ n \in \mathbb{N}.$$

Одредити остатак при дељењу броја $a_1^3 + a_2^3 + \cdots + a_{2005}^3$ са 9.

Решење. Није тешко показати да важе следеће импликације:

$$a \equiv b \pmod{102} \Rightarrow a \equiv b \pmod{3};$$

$$a \equiv b \pmod{3} \Rightarrow a^3 \equiv b^3 \pmod{9}.$$

Како је, према услову задатка, за сваки природан број n,

$$a_{n+2} \equiv a_n + a_{n+1} \ (\mathrm{mod}\ 102),$$

то је и

$$a_{n+2} \equiv a_n + a_{n+1} \ (\mathrm{mod}\ 3),$$

па је:

$$\begin{array}{lll} a_1 \equiv -1 \ (\mathrm{mod}\ 3), & a_2 \equiv 1 \ (\mathrm{mod}\ 3), & a_3 \equiv 0 \ (\mathrm{mod}\ 3), \\ a_4 \equiv 1 \ (\mathrm{mod}\ 3), & a_5 \equiv 1 \ (\mathrm{mod}\ 3), & a_6 \equiv -1 \ (\mathrm{mod}\ 3), \\ a_7 \equiv 0 \ (\mathrm{mod}\ 3), & a_8 \equiv -1 \ (\mathrm{mod}\ 3). & \end{array}$$

Како је

$$\begin{aligned} a_{n+4} &\equiv a_{n+3} + a_{n+2} \equiv (a_{n+2} + a_{n+1}) + a_{n+2} \\ &\equiv 2a_{n+2} + a_{n+1} \equiv 2\left(a_{n+1} + a_n\right) + a_{n+1} \\ &\equiv 3a_{n+1} + 2a_n \equiv -a_n \ (\mathrm{mod}\ 3), \end{aligned}$$

то је $a_{n+8} \equiv -a_{n+4} \equiv a_n (\mathrm{mod}\ 3)$, па је

$$a_{8m+k} \equiv a_k (\mathrm{mod}\ 3), \quad (k = 1, 2, \ldots, 8)\,.$$

Сада имамо да је

$$\begin{aligned} &a_{8m+1}^3 + a_{8m+2}^3 + \cdots + a_{8m+8}^3 \\ \equiv\ &a_1^3 + a_2^3 + \cdots + a_8^3 \\ \equiv\ &(-1)^3 + 1^3 + 0^3 + 1^3 + 1^3 + (-1)^3 + 0^3 + (-1)^3 \\ \equiv\ &0 \ (\mathrm{mod}\ 9). \end{aligned}$$

Како је $2\,005 = 250 \cdot 8 + 5$, то ће бити

$$\begin{aligned}
&a_1^3 + a_2^3 + \cdots + a_{2005}^3\\
&\equiv (a_1^3 + \cdots + a_8^3) + (a_9^3 + \cdots + a_{16}^3) + \cdots +\\
&+ (a_{1993}^3 + \cdots + a_{2000}^3) + a_{2001}^3 + a_{2002}^3 + a_{2003}^3 + a_{2004}^3 + a_{2005}^3\\
&\equiv 0 + \cdots + 0 + a_1^3 + a_2^3 + a_3^3 + a_4^3 + a_5^3\\
&\equiv 2 \pmod 9.
\end{aligned}$$

Дакле, остатак при дељењу броја $a_1^3 + a_2^3 + \cdots + a_{2005}^3$ са 9 је 2.

335. (БМО 1990) Низ a_n, $n \in \mathbb{N}$ је дат на следећи начин $a_1 = 1$, $a_2 = 3$ и

$$a_{n+2} = (n+3)a_{n+1} - (n+2)a_n$$

за све природне бројеве n. Наћи све чланове овог низа који су дељиви са 11.

Решење. Нека је r_n остатак који се добија дељењем a_n са 11. Ако се има у виду да је

(1) $$r_{n+2} \equiv (n+3)r_{n+1} - (n+2)r_n \pmod{11},$$

није тешко израчунати првих 11 чланова низа r_n, $n \in \mathbb{N}$:

n	1	2	3	4	5	6	7	8	9	10	11
r_n	1	3	9	0	10	4	6	0	1	0	0

Математичком индукцијом није тешко показати да је $r_n = 0$ за $n \geqslant 10$. При том се користи рекурентна веза (1) и чињеница да је $r_{10} = r_{11} = 0$. Према томе, дељиви са 11 су чланови са индексима $n = 4$, $n = 8$ и $n \geqslant 10$.

336. (Зимско математичко такмичење, Бугарска 1998, 10. разред) Нека је n природан број. Наћи број низова $a_1, a_2, \ldots, a_{2n}$ таквих да је $a_i \in \{-1,1\}$ и

$$\left|\sum_{i=2k-1}^{2l} a_i\right| \leqslant 2 \quad \text{за све } 1 \leqslant k \leqslant l \leqslant n.$$

Решење. Јасно је да било који низ код кога је $a_{2k-1}+a_{2k}=0$ за $1 \leqslant k \leqslant n$ задовољава услове задатка. Постоји 2^n таквих низова.

Анализирајмо сада низове код којих постоји k за које је $a_{2k-1}+a_{2k} \neq 0$. За дати такав низ, нека су $k_1, k_2, \ldots, k_s$ сви индекси који имају поменуто својство. Ако је $a_{2k_i-1}+a_{2k_i}=2(-2)$ тада је $a_{2k_{i+1}-1}+a_{2k_{i+1}}=-2(2)$. Према томе, сви збирови $a_{2k_i-1}+a_{2k_i}$ (па отуда и сви парови (a_{2k_i-1}, a_{2k_i})) су јединствено одређени са $a_{2k_1-1}+a_{2k_1}$ (постоје две могућности за (a_{2k_1-1}, a_{2k_1})). Постоје две могућности за сваки од преосталих $n-s$ парова за које је $a_{2t-1}+a_{2t}=0$. Дакле, постоји

$$2^n + 2 \cdot 2^{n-1}\binom{n}{1} + \cdots + 2 \cdot 2^{n-k}\binom{n}{k} + \cdots + 2 \cdot 2\binom{n}{n-1} + 2 \cdot \binom{n}{n}$$

низова са траженом особином. Додајући и одузимајући 2^n у горњем изразу добијамо да је тај број једнак

$$2 \cdot \left[2^n\binom{n}{0} + 2^{n-1}\binom{n}{1} + \cdots + 2\binom{n}{n-1} + \binom{n}{n}\right] - 2^n = 2 \cdot 3^n - 2^n.$$

337. (Зимско математичко такмичење, Бугарска 1998, 11. разред) Нека је $(a_m)_{m=1}^{\infty}$ низ природних бројева који имају само парне цифре у свом децималном запису: $a_1=2, a_2=4, a_3=6, a_4=8, a_5=20, \ldots$. Наћи све природне бројеве m такве да је $a_m=12m$.

Решење. Нека је m природан број и $m=b_0+b_1 \cdot 5+\cdots+b_n \cdot 5^n$, $0 \leqslant b_i \leqslant 4$, $b_n \neq 0$. Означимо

$$f(m)=2b_0+2b_1 \cdot 10+\cdots+2b_n \cdot 10^n.$$

Јасно је да је $\{f(m) \mid m \in \mathbb{N}\}$ скуп свих позитивних целих бројева који имају само парне цифре у децималном запису. Како је

$$f(m_1) < f(m_2) \Leftrightarrow m_1 < m_2,$$

следи да је $a_m = f(m)$ за све m. Дакле, треба наћи све m такве да важи

$$12(b_0 + b_1 \cdot 5 + \cdots + b_n \cdot 5^n) = 2b_0 + 2b_1 \cdot 10 + \cdots + 2b_n \cdot 10^n,$$

тј.

$$(*) \qquad 6(b_0 + b_1 \cdot 5 + \cdots + b_n \cdot 5^n) = b_0 + b_1 \cdot 10 + \cdots + b_n \cdot 10^n.$$

Како је

$$b_0 + b_1 \cdot 5 + \cdots + b_n \cdot 5^n \leqslant 5^{n+1} - 1$$

и

$$b_0 + b_1 \cdot 10 + \cdots + b_n \cdot 10^n \geqslant 10^n,$$

из $(*)$ следи да је $6(5^{n+1} - 1) \geqslant 10^n$, одакле је $6 \cdot 5^{n+1} > 10^n$. Даље се добија $2^n < 30$, тј. $n \leqslant 4$.

За $n = 4$ из $(*)$ добијамо да је $b_0 + 4b_1 + 10b_2 = 50b_3 + 1\,250b_4 \geqslant 1\,250$, што је немогуће. Слично се показује да мора бити $n \geqslant 3$, тј. $n = 3$. У том случају је $b_0 + 4b_1 + 10b_2 = 50b_3$. Очигледно је $b_3 = 1$ и $b_0 = b_1$ јер је $b_0 - b_1$ дељиво са 5. Даље је $b_0 + 2b_2 = 10$ одакле је $b_0 = 2, b_2 = 4$ или $b_0 = 4, b_2 = 3$. Према томе, тражени бројеви m су $m = 2 + 2 \cdot 5 + 4 \cdot 5^2 + 5^3 = 237$ и $m = 4 + 4 \cdot 5 + 3 \cdot 5^2 + 5^3 = 224$.

338. (Национална математичка олимпијада–финална рунда, Бугарска 1998) Дат је природан број n. Наћи најмањи природан број k за који постоји k низова нула и јединица дужине $2n + 2$ са следећом особином: било који низ нула и јединица дужине $2n + 2$ поклапа се у најмање $n + 2$ позиције са неким од ових k низова.

Решење. Показаћемо да је $k = 4$. Претпоставимо да је $k \leqslant 3$ и нека су одговарајући низови $a_1^i, a_2^i, \ldots, a_{2n+2}^i$, $i = 1, \ldots, k$. Пошто је $k \leqslant 3$ то постоји низ $b_1, b_2, \ldots, b_{2n+2}$ такав да је

$$(b_{2l+1}, b_{2l+2}) \neq (a_{2l+1}^i, a_{2l+2}^i) \quad \text{за} \quad l = 0, 1, \ldots, n \quad \text{и} \quad i = 1, \ldots, k,$$

што је контрадикција. За $k = 4$ лако се проверава да низови $000\ldots0$, $011\ldots1$, $100\ldots0$ и $111\ldots1$ имају тражену особину.

339. (Национална математичка олимпијада–регионална рунда, Бугарска 2000) Дат је низ $(a_n)_{n=1}^{\infty}$, дефинисан са $a_1 = 43$, $a_2 = 142$ и $a_{n+1} = 3a_n + a_{n-1}$ за $n \geqslant 2$. Доказати:

(а) a_n и a_{n+1} су узајамно прости за све n;

(б) за сваки природан број m постоји бесконачно много природних бројева n, таквих да су и $a_n - 1$ и $a_{n+1} - 1$ дељиви са m.

Решење. (а) Претпоставимо супротно, тј. да постоје природни бројеви n и $m > 1$ такви да m дели и a_n и a_{n+1}. Тада из $a_{n-1} = a_{n+1} - 3a_n$ следи да m дели и a_{n-1}. Настављајући даље овакву анализу закључујемо да m дели и a_1 и a_2. Међутим, то је немогуће јер су a_1 и a_2 узајамно прости.

(б) Посматрајмо низ $(a_n)_{n=-\infty}^{\infty}$, дефинисан са $a_{n-1} = a_{n+1} - 3a_n$ за негативне индексе. Тада је $a_0 = a_2 - 3a_1 = 13$, $a_{-1} = a_1 - 3a_0 = 4$, $a_{-2} = a_0 - 3a_{-1} = 1$, $a_{-3} = a_{-1} - 3a_{-2} = 1$ итд. Према томе, дефинисали смо низ $(a_n)_{-\infty}^{\infty}$ целих бројева, такав да је $a_{n+1} = 3a_n + a_{n-1}$ за све $n \in \mathbb{Z}$. Пошто парова $(p \pmod m), q \pmod m)$ има коначно много, следи да постоје цели бројеви r и s, $s > r$, такви да је $a_r \equiv a_s \pmod m$ и $a_{r+1} \equiv a_{s+1} \pmod m$. Из рекурентне релације тада следи

$$a_{r+2} = 3a_{r+1} + a_r \equiv 3a_{s+1} + a_s \ (\mathrm{mod}\ m),$$

тј. $a_{r+2} \equiv a_{s+2} \pmod m$ одакле индукцијом можемо показати да је $a_{r+i} \equiv a_{s+i} \pmod m$ за све i. Дакле, низ $(a_n \pmod m))_{-\infty}^{\infty}$ је периодичан. Пошто је $a_{-3} \equiv a_{-2} \equiv 1 \pmod m$, то постоји бесконачно много природних бројева таквих да су и $a_n - 1$ и $a_{n+1} - 1$ дељиви са m.

340. (IV селекционо такмичење за ИМО, Румунија 2003) Нека је $\mathcal{P}$ скуп свих простих бројева и M подскуп од $\mathcal{P}$, који има бар три елемента, такав да за било који прави подскуп A од M важи да сви прости делиоци броја

$$-1 + \prod_{p \in A} p$$

припадају скупу M. Доказати да је $M = \mathcal{P}$.

Решење. Ако $2 \notin M$, узмимо $A = \{p\}$, $p \in M$. Тада је $p - 1$ паран број, па према услову задатка следи да $2 \in M$. Контрадикција. Дакле, $2 \in M$.

Претпоставимо сада да је скуп M коначан, $M = \{2, p_2, \dots, p_k\}$, $k \geqslant 3$. Нека је $A = \{2, p_3, \dots, p_k\}$ и означимо са P производ свих елемената скупа M. Тада добијамо

$$(*) \qquad 2p_3 \cdots p_k - 1 = \frac{P}{p_2} - 1 = p_2^{\alpha} \Rightarrow P = p_2^{\alpha+1} + p_2.$$

Нека је сада $A = \{p_3, \dots, p_k\}$. Тада имамо

$$(**) \qquad p_3 \cdots p_k - 1 = \frac{P}{2p_2} - 1 = 2^{\beta} p_2^{\gamma} \Rightarrow P = 2p_2(2^{\beta} p_2^{\gamma} + 1).$$

Из $(*)$ и $(**)$ следи

$$p_2^{\alpha+1} + p_2 = 2p_2(2^{\beta} p_2^{\gamma} + 1) \Rightarrow p_2^{\alpha} + 1 = 2^{\beta+1} p_2^{\gamma} + 2 \Rightarrow 1 \equiv 2 \pmod{p_2},$$

што је контрадикција. Дакле, скуп M није коначан.

Претпоставимо сада да постоји прост број q, такав да $q \notin M$, $M = \{2, p_2, p_3, \dots, p_k, \dots\}$. Тада међу бројевима

$$2 - 1,\ 2p_2 - 1,\ \dots,\ 2p_2 p_3 \cdots p_{q+1} - 1$$

најмање два имају исти остатак при дељењу са q. Нека је

$$2 \cdots p_i - 1 \equiv 2 \cdots p_j - 1 \pmod{q}, \quad 1 \leqslant i < j \leqslant q+1.$$

Тада је

$$2 \cdots p_i(p_{i+1} \cdots p_j - 1) \equiv 0 \pmod{q} \Rightarrow p_{i+1} \cdots p_j - 1 \equiv 0 \pmod{q},$$

одакле следи да $q \in M$, што је контрадикција. Према томе $M = \mathcal{P}$.

341. (III селекционо такмичење за ЈБМО, Румунија 2003) Нека је a природан број такав да a^n има непаран број цифара у декадном запису за све $n > 0$. Доказати да је тада број a паран степен броја 10.

Решење. Како број a има непаран број цифара, тада за неко целобројно $k \geqslant 0$ важи $10^{2k} \leqslant a < 10^{2k+1}$. Треба показати да је $a = 10^{2k}$.

Приметимо најпре да је $10^{4k} \leqslant a^2 < 10^{4k+2}$. Пошто и број a^2 има непаран број цифара, то је $10^{2k} \leqslant a < 10^{2k+\frac{1}{2}}$.

Даље, из $10^{8k} \leqslant a^4 < 10^{8k+2}$, с обзиром на то да a^4 има непаран број цифара, следи $10^{2k} \leqslant a < 10^{2k+\frac{1}{4}}$.

Индукцијом по n добијамо да је $10^{2k} \leqslant a < 10^{2k+\frac{1}{2^n}}$, за све $n > 0$.

Претпоставимо супротно, тј. да је $a \geqslant 10^{2k} + 1$. Тада је

$$\begin{aligned} 10^{2k+\frac{1}{2^n}} > 10^{2k} + 1 &\Leftrightarrow 10^{2k}\left(10^{\frac{1}{2^n}} - 1\right) > 1 \\ &\Leftrightarrow 10^{\frac{1}{2^n}} > 1 + \frac{1}{10^{2k}} \\ &\Leftrightarrow 10 > \left(1 + \frac{1}{10^{2k}}\right)^{2^n}, \quad \text{за све} \quad n > 0. \end{aligned}$$

С друге стране, коришћењем Бернулијеве неједнакости, имамо

$$\left(1 + \frac{1}{10^{2k}}\right)^{2^n} \geqslant 1 + \frac{2^n}{10^{2k}}, \quad \text{за све} \quad n > 0,$$

па ће за довољно велико n бити $1 + \dfrac{2^n}{10^{2k}} > 10$. Контрадикција.

342. (Аустралијска математичка олимпијада, 2002) Нека су n и q природни бројеви, $n \geqslant 5$, $2 \leqslant q \leqslant n$. Доказати да $q-1$ дели $\left[\dfrac{(n-1)!}{q}\right]$.

Решење. Размотрићемо неколико случајева:

(1) $q < n$. Тада производ $(n-1)! = 1 \cdot 2 \cdot \ldots \cdot (n-1)$ садржи као факторе и q и $q-1$, па $q(q-1) \mid (n-1)!$, односно

$$q-1 \mid \frac{(n-1)!}{q} = \left[\frac{(n-1)!}{q}\right].$$

(2) $q = n$, при чему је q прост број. Тада је према Вилсоновој теореми $(n-1)! \equiv -1 \equiv n-1 \pmod n$, одакле добијамо, због $(n, n-1) = 1$, да је $(n-2)! \equiv 1 \pmod n$. Дакле, $(n-2)! = yn+1$ за неки цео број y. Тада је

$$\left[\frac{(n-1)!}{n}\right] = \left[\frac{(n-1)(yn+1)}{n}\right] = \left[ny - y + 1 - \frac{1}{n}\right] = (n-1)y,$$

што је дељиво са $n-1 = q-1$.

(3) $q = n$, при чему је q сложен број. Довољно је показати да $n(n-1) \mid (n-1)!$.

Нека је p највећи прост делилац броја n и $n = px$. Тада је $1 < x < n$. Како $x \mid n$ то не може бити $x = n-1$. Дакле, $1 < x \leqslant n-2$.

(3а) Ако је $p \neq x$ тада се и p и x појављују на различитим местима у развоју производа $(n-2)! = 1 \cdot 2 \cdot \ldots \cdot (n-1)$, па $n = px \mid (n-2)!$, одакле следи да $n(n-1) \mid (n-1)!$.

(3б) Ако је $p = x$ тада је $n = p^2$. Пошто је $n > 4$, то је $p > 2$, па је $p^2 > 2p$. Како је у овом случају $(2p, n) = p$, то не може бити $2p = n - 1$, па је $2p \leqslant n - 2$. Тада се бројеви p и $2p$ појављују на различитим местима у развоју производа $(n-2)! = 1 \cdot 2 \cdot \ldots \cdot (n-1)$, па $2p^2 \mid (n-2)!$, одакле следи да $n(n-1) \mid (n-1)!$.

343. (Азијско-пацифичка математичка олимпијада, 2002) Нека је $a_1, a_2, \ldots, a_n$ низ ненегативних целих бројева, $n \in \mathbb{N}$. Доказати да је

$$a_1!a_2! \cdots a_n! \geqslant ([A_n]!)^n,$$

где је

$$A_n = \frac{a_1 + a_2 + \cdots + a_n}{n}.$$

Решење. Нека је збир бројева a_i фиксиран и једнак k. Како постоји само коначно много n-торки ненегативних целих бројева a_i чији је збир једнак k, онда постоји једна која минимизира вредност производа $M = a_1! \cdot a_2! \cdot \ldots \cdot a_n!$. Без смањења општости можемо претпоставити да је $a_1 \geqslant a_2 \geqslant \cdots \geqslant a_n$.

Докажимо најпре да се минимална вредност производа M достиже када је $a_1 = a_n + 1$ или $a_1 = a_n$.

Претпоставимо супротно. Тада је $a_1 \geqslant a_n + 2 \geqslant 2$, па је $a_1 - 1 \geqslant 1$. Тада је:

$$\begin{gathered} a_n + 1 < a_1 \\ \frac{(a_n+1)!}{a_n!} < \frac{a_1!}{(a_1-1)!} \\ (a_1-1)! \cdot a_2! \cdot \ldots \cdot a_{n-1}! \cdot (a_n+1)! < a_1! \cdot a_2! \cdot \ldots \cdot a_{n-1}! \cdot a_n! \leqslant M, \end{gathered}$$

што је контрадикција са минималношћу вредности производа M.

(1) $a_1 = a_n$. Тада су сви бројеви a_i међусобом једнаки и нека је та вредност a. Тада је $[A_n] = a$, па су лева и десна страна тражене неједнакости једнаке $(a!)^n$.

(2) $a_1 = a_n + 1$. Тада је

$$na_n < k \leqslant a_n + (n-1)a_1 = a_n + (n-1)(a_n+1) = na_n + n - 1,$$

па је

$$a_n < A_n \leqslant a_n + \frac{n-1}{n}, \quad \text{тј.} \quad [A_n] = a_n.$$

Сада је

$$\begin{aligned} a_1! \cdot a_2! \cdot \ldots \cdot a_n! &\geqslant a_1!(a_n!)^{n-1} \\ &= (a_n!)^n(a_n+1) \\ &= ([A_n]!)^n(a_n+1) \\ &\geqslant ([A_n]!)^n. \end{aligned}$$

344. (ИМО 2002) Одредити све парове целих бројева m, n не мањих од 3, за које је

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

цео број, за бесконачно много природних бројева a.

Решење. Дефинишимо полиноме

$$f(x) = x^m + x - 1 \quad \text{и} \quad g(x) = x^n + x^2 - 1.$$

Нека је $q(x)$ количник, а $r(x)$ остатак при дељењу f са g. Како су коефицијенти полинома f и g цели, а водећи коефицијент полинома g једнак 1, коефицијенти полинома q и r су цели бројеви. Како је

$$\frac{f(a)}{g(a)} = q(a) + \frac{r(a)}{g(a)},$$

то је $\dfrac{r(a)}{g(a)}$ цео број за бесконачно много природних бројева a. Како овај количник тежи нули кад a тежи ∞, то је $\dfrac{r(a)}{g(a)} = 0$, односно, $r(a) = 0$, за бесконачно много природних бројева a. Следи $r(x) = 0$, тј. полином $f(x)$ је дељив са полиномом $g(x)$. Докажимо да је $m = 5$ и $n = 3$.

Ставимо $m = n + k$, $k \geqslant 0$. Како је

$$f(x) = x^k g(x) + (1 - x)(x^{k+1} + x^k - 1),$$

полином g дели $(1 - x)(x^{k+1} + x^k - 1)$, дакле и $h(x) = x^{k+1} + x^k - 1$. Зато је $k + 1 \geqslant n \geqslant 3$. Како је $g(0) < 0$ и $g(1) > 0$, полином g има у интервалу $(0, 1)$ реалан корен α, који је и корен полинома h. Из неједнакости $\alpha^n \geqslant \alpha^{k+1}$ и $\alpha^2 \geqslant \alpha^k$, следи $\alpha^n + \alpha^2 \geqslant \alpha^{k+1} + \alpha^k$, што је, због $\alpha^n + \alpha^2 = 1$ и $\alpha^{k+1} + \alpha^k = 1$, могуће једино када у обе неједнакости важи једнакост. Отуда је $n = k+1$ и $2 = k$, дакле, $n = 3$ и $m = 5$.

345. (Савезно такмичење 1983, III и IV разред) Низ природних бројева (x_n) је дефинисан на следећи начин:

$$x_1 = 2, \qquad x_{n+1} = \left[\frac{3}{2}x_n\right] \quad (n = 1, 2, 3 \ldots).$$

Доказати да у низу (x_n) има бесконачно много непарних и бесконачно много парних природних бројева.

Решење. Претпоставимо да у низу (x_n) има коначно много непарних бројева. Тада постоји природан број m, такав да је x_n паран број за сваки n такав да је $n \geqslant m$. Нека је $x_m = 2k_0$, $k_0 \in \mathbb{N}$. Тада је

$$x_{m+1} = \left[\frac{3}{2}x_m\right] = \left[\frac{3}{2} \cdot 2k_0\right] = 3k_0.$$

Како је x_{m+1} паран број, то је $k_0 = 2k_1,\ k_1 \in \mathbb{N}$. Даље је

$$x_{m+2} = \left[\frac{3}{2}x_{m+1}\right] = \left[\frac{3}{2}\cdot 3k_0\right] = \left[\frac{3}{2}\cdot 3\cdot 2\cdot k_1\right] = 3^2k_1.$$

Како је x_{m+2} такође паран број, то је $k_1 = 2k_2,\ k_2 \in \mathbb{N}$, и $k_0 = 2^2k_2$.

Настављајући поступак добијамо да за сваки природан број s постоји, такође природан, број k_s тако да је $k_0 = 2^sk_s$, тј. за сваки природан број s, $2^s \mid k_0$, што је немогуће.

Претпоставимо сада да у низу (x_n) има коначно много парних бројева. Тада постоји природан број m такав да је x_n непаран број за сваки n такав да је $n \geqslant m$. Нека је $x_m = 2k_0 + 1,\ k_0 \in \mathbb{N}$. Тада је

$$x_{m+1} = \left[\frac{3}{2}(2k_0+1)\right] = 3k_0 + 1.$$

Како је x_{m+1} непаран број, то је $k_0 = 2k_1,\ k_1 \in \mathbb{N}$. Даље, аналогно као у првом случају доказујемо да нас оваква претпоставка доводи до контрадикције.

346. (ИМО 1968) За сваки природан број n израчунати збир

$$\left[\frac{n+1}{2}\right] + \left[\frac{n+2}{4}\right] + \cdots + \left[\frac{n+2^k}{2^{k+1}}\right] + \cdots .$$

Решење. За сваки реалан број x важи (видети теорему 1.1. (9)):

$$(*) \qquad \left[x + \frac{1}{2}\right] = [2x] - [x].$$

Ако саберемо једнакости добијене из $(*)$ стављањем да је $x = \dfrac{n}{2^{k+1}}$, $k = 0, 1, \ldots, m$, добијамо да је

$$\sum_{k=0}^{m}\left[\frac{n+2^k}{2^{k+1}}\right] = [n] - \left[\frac{n}{2^m}\right].$$

Пошто за свако n постоји природан број m такав да је $2^m > n$, имамо да је $\lim\limits_{m\to+\infty}\left[\dfrac{n}{2^m}\right] = 0$, па је

$$\sum_{k=0}^{+\infty}\left[\frac{n+2^k}{2^{k+1}}\right] = n.$$

347. (ИМО 1976) Низ (u_n) дефинисан је на следећи начин

$$\begin{aligned} &u_0 = 2, \quad u_1 = \frac{5}{2} \\ &u_{n+1} = u_n\left(u_{n-1}^2 - 2\right) - u_1 \qquad (n = 1, 2, 3, \dots) \end{aligned}$$

Доказати да је

$$[u_n] = 2^{\frac{2^n-(-1)^n}{3}}, \quad n = 1, 2, \dots .$$

Решење. Доказаћемо да је

$$(*) \qquad u_n = 2^{\frac{2^n-(-1)^n}{3}} + 2^{-\frac{2^n-(-1)^n}{3}}, \ n = 0, 1, 2, \dots$$

Заиста, једнакост $(*)$ је тачна за $n = 0$ и $n = 1$. Претпоставимо да је тачна за неке узастопне природне бројеве $n-1$ и n. Тада имамо да је

$$\begin{aligned} u_{n+1} &= \left(2^{\frac{2^n-(-1)^n}{3}} + 2^{-\frac{2^n-(-1)^n}{3}}\right)\left(2^{2\frac{2^{n-1}-(-1)^{n-1}}{3}} + 2^{-2\frac{2^{n-1}-(-1)^{n-1}}{3}}\right) - \frac{5}{2} \\ &= 2^{\frac{2^n-(-1)^n+2^n-2(-1)^{n-1}}{3}} + 2^{\frac{2^n-(-1)^n-2^n+2(-1)^{n-1}}{3}} + \\ &\quad +2^{\frac{-2^n+(-1)^n+2^n-2(-1)^{n-1}}{3}} + 2^{\frac{-2^n+(-1)^n-2^n+2(-1)^{n-1}}{3}} - \frac{5}{2} \\ &= 2^{\frac{2^{n+1}-(-1)^{n+1}}{3}} + 2^{(-1)^{n+1}} + 2^{-(-1)^{n+1}} + 2^{\frac{-2^{n+1}+(-1)^{n+1}}{3}} - \frac{5}{2} \\ &= 2^{\frac{2^{n+1}-(-1)^{n+1}}{3}} + 2^{-\frac{2^{n+1}-(-1)^{n+1}}{3}} \end{aligned}$$

јер је $2^{(-1)^{n+1}} + 2^{-(-1)^{n+1}} = \frac{5}{2}$ (један од сабирака је увек 2, а други $\frac{1}{2}$).

Ако је $n > 0$, други сабирак у једнакости $(*)$ је мањи од 1 (јер је одговарајући експонент негативан), а први је цео број (јер из идентитета $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$ следи да је одговарајући експонент цео број) и биће

$$[u_n] = 2^{\frac{2^n - (-1)^n}{3}}, \quad n = 1, 2, \ldots .$$

348. Одредити највећи степен броја 2 који дели $\left[\left(1+\sqrt{3}\right)^n\right]$.

Решење. Број $\left(1+\sqrt{3}\right)^n + \left(1-\sqrt{3}\right)^n$ је цео и важи:

$$\left[\left(1+\sqrt{3}\right)^n\right] = \begin{cases} \left(1+\sqrt{3}\right)^n + \left(1-\sqrt{3}\right)^n - 1, & n \text{ паран број} \\ \left(1+\sqrt{3}\right)^n + \left(1-\sqrt{3}\right)^n, & n \text{ непаран број} \end{cases}$$

јер је $0 < \left(1-\sqrt{3}\right)^n < 1$, ако је n паран број, и $-1 < \left(1-\sqrt{3}\right)^n < 0$, ако је n непаран број.

Ако је n паран број, тј. $n = 2m$, за неки природан број m, онда је

$$\begin{aligned} \left[\left(1+\sqrt{3}\right)^{2m}\right] &= \left(1+\sqrt{3}\right)^{2m} + \left(1-\sqrt{3}\right)^{2m} - 1 \\ &= \left(\left(1+\sqrt{3}\right)^2\right)^m + \left(\left(1-\sqrt{3}\right)^2\right)^m - 1 \\ &= \left(4+2\sqrt{3}\right)^m + \left(4-2\sqrt{3}\right)^m - 1 \\ &= 2^m\left(\left(2+\sqrt{3}\right)^m + \left(2-\sqrt{3}\right)^m\right) - 1. \end{aligned}$$

Пошто је $\left(2+\sqrt{3}\right)^m + \left(2-\sqrt{3}\right)^m$ цео број, то је, у овом случају, $\left[\left(1+\sqrt{3}\right)^n\right]$ непаран број.

Ако је n непаран број, тј. $n=2m+1$, тада је

$$\begin{aligned}\left[\left(1+\sqrt{3}\right)^{2m+1}\right] &= \left(1+\sqrt{3}\right)^{2m+1}+\left(1-\sqrt{3}\right)^{2m+1}\\ &= \left(4+2\sqrt{3}\right)^{m}\left(1+\sqrt{3}\right)+\left(4-2\sqrt{3}\right)^{m}\left(1-\sqrt{3}\right)\\ &= 2^m\left(\left(2+\sqrt{3}\right)^{m}\left(1+\sqrt{3}\right)+\left(2-\sqrt{3}\right)^{m}\left(1-\sqrt{3}\right)\right).\end{aligned}$$

Ако је $\left(2+\sqrt{3}\right)^m=a_m+b_m\sqrt{3}$, онда је и $\left(2-\sqrt{3}\right)^m=a_m-b_m\sqrt{3}$ и важи:

$$a_m^2-3b_m^2=\left(2+\sqrt{3}\right)^m\left(2-\sqrt{3}\right)^m=1.$$

Из претходних једнакости следи да је

$$\begin{aligned}&2^m\left(\left(2+\sqrt{3}\right)^{m}\left(1+\sqrt{3}\right)+\left(2-\sqrt{3}\right)^{m}\left(1-\sqrt{3}\right)\right)\\ &=2^m(2a_m+6b_m)=2^{m+1}(a_m+3b_m).\end{aligned}$$

Како је

$$(a_m+3b_m)(a_m-3b_m)=a_m^2-9b_m^2=a_m^2-3b_m^2-6b_m^2=1-6b_m^2,$$

број a_m+3b_m је непаран, па је највећи степен броја 2 који дели број $\left[\left(1+\sqrt{3}\right)^n\right]$ једнак $\dfrac{n+1}{2}=m+1$.

349. Познато је да постоје тачно два проста броја чије реципрочне вредности записане у облику децималног броја имају периоде 7. Један од тих бројева је $4\,649$. Који је други?

Решење. Нека је p тражени број. Тада је

$$\frac{1}{p}=0,a_1a_2\dots a_n(b_1b_2\dots b_7).$$

Из тога следи да је

$$\begin{aligned} q &= 10^{n+7} \cdot \frac{1}{p} - 10^{n} \cdot \frac{1}{p} \\ &= \overline{a_1a_2\ldots a_nb_1b_2\ldots b_7},(b_1b_2\ldots b_7) - \overline{a_1a_2\ldots a_n},(b_1b_2\ldots b_7) \\ &= \overline{a_1a_2\ldots a_nb_1b_2\ldots b_7} - \overline{a_1a_2\ldots a_n} \end{aligned}$$

цео број. Дакле,

$$10^n \cdot (10^7 - 1) \cdot \frac{1}{p} = 10^n \cdot 9\,999\,999 \cdot \frac{1}{p} = q,$$

одакле је

$$p = \frac{10^n \cdot 9\,999\,999}{q} = \frac{2^n \cdot 5^n \cdot 3^2 \cdot 239 \cdot 4\,649}{q}\,.$$

Како је p прост број, q је производ неких од наведених фактора. Другим речима, $p \in \{2, 3, 5, 239, 4\,649\}$. Могућност $p = 4\,649$ отпада због услова задатка. Такође отпадају $p = 2, 3, 5$, јер њихове реципрочне вредности немају периоде 7; $\frac{1}{2} = 0,5$, $\frac{1}{3} = 0,(3)$, $\frac{1}{5} = 0,2$. Тако остаје $p = 239$, што и јесте решење с обзиром на то да је $\frac{1}{239} = 0,(0041841)$.

350. Нека је n природан број који у систему са основом $2\,005$ има 20 цифара. Ако те цифре, узете неким редом, образују аритметичку прогресију, доказати да је n сложен број.

Решење. Користићемо следеће тврђење које се лако доказује: *Ако је збир цифара неког броја написаног у систему са основом b, $(b > 1)$, дељив са m и $b - 1$ дељиво са m, тада је и сам број дељив са m.* На пример, из наведене теореме следе критеријуми дељивости са 3 и 9 у декадном систему.

Нека је n двадесетоцифрен број у систему са основом $2\,005$. Како цифре, узете неким редом, образују аритметичку прогресију, збир цифара броја n је

$$a + (a + d) + \cdots + (a + 19d) = 20a + 190d = 2(10a + 95d).$$

Дакле, дељив је са 2. Међутим, са 2 је дељиво и $2\,005 - 1 = 2\,004$. На основу наведеног тврђења и број n је дељив са 2.

351. Решити у скупу целих бројева једначину

$$x^3 + 24 = 2^x.$$

Решење. Једино решење је $x = 10$. Заиста, за $x < 0$ десна страна једначине није цео број, а лева јесте. За $x = 0, 1, \ldots, 9$ провером добијамо да нису решења, а за $x > 10$ докажимо индукцијом да је $x^3 + 24 < 2^x$. (Читаоци који су упознати са основама диференцијалног рачуна могу показати да је $f'(x) > 0$ за $x \geqslant 10$, где је $f(x) = 2^x - x^3 - 24$.) За $x = 11$ тврђење важи. Нека је тачно и за произвољно $x \geqslant 11$. Тада је

$$\begin{aligned}(x+1)^3 + 24 &= x^3 + 3x^2 + 3x + 1 + 24 \\ &= (x^3 + 24) + (3x^2 + 3x + 1) < 2^x + 2^x = 2^{x+1}.\end{aligned}$$

Ово следи из $3x^2 + 3x + 1 < 2^x$, што опет доказујемо индукцијом: за $x = 11$ је испуњено, а ако важи за ма које $x \geqslant 11$, онда је

$$3(x+1)^2 + 3(x+1) + 1 = (3x^2 + 3x + 1) + (6x + 6) < 2^x + 2^x < 2^{x+1}.$$

(За доказ неједнакости $6x + 6 < 2^x$ поново користимо индукцију; то остављамо читаоцу за вежбу.)

352. Са речима над азбуком $\{0, 1\}$ дозвољено је вршити следеће операције:

(1) убацити на произвољно место између два суседна слова, на почетку или на крају речи, реч облика ppp;

(2) избрисати било коју подреч облика ppp.

Тако се, на пример, из речи 0001 могу добити речи 0111001 и 1. Да ли се наведеним операцијама из речи 01 може добити реч 10?

Решење. Речи над датом азбуком посматрајмо као бинарне записе бројева. Посматрајмо реч $a = \overline{a_n a_{n-1} \cdots a_1 a_0}$, и реч добијену убацивањем ppp: $b = \overline{a_n a_{n-1} \cdots a_k ppp a_{k-1} a_{k-2} \cdots a_0}$. (Брисање се разматра аналогно.)

$$\begin{aligned} b - a &= \overline{a_n a_{n-1} \cdots a_k} \cdot 2^{k+3} + \overline{ppp} \cdot 2^k + \overline{a_{k-1} a_{k-2} \cdots a_0} - \overline{a_n a_{n-1} \cdots a_0} \\ &= 2^k \left(7\overline{a_n a_{n-1} \cdots a_k} + \overline{ppp} \right). \end{aligned}$$

Како $\overline{ppp}$ може бити или 0 или 7, ова разлика је увек дељива са 7, па ако је број c добијен од броја d наведеним операцијама, важи $c \equiv d \pmod 7$, а то није случај са бројевима $\overline{01} = 1$ и $\overline{10} = 2$.

353. Нека је $a_1, a_2, a_3, \ldots$ низ различитих природних бројева такав да је $a_n < 100n$, за сваки природан број n. Доказати да у том низу постоји број у чијем се декадном запису појављује 2 000 узастопних јединица.

Решење. Доказаћемо најпре следеће тврђење: у датом низу постоји члан у чијем се декадном запису појављује бар једна јединица. Претпоставимо супротно. Тада се међу првих 10^c природних бројева може налазити највише 9^c чланова низа. Међутим, ако ставимо $n = 10^c$, из услова $a_{10^c} < 100 \cdot 10^c = 10^{c+2}$ видимо да се 10^c чланова низа налази међу првих 10^{c+2} природних бројева. Али међу првих 10^{c+2} природних бројева може бити највише 9^{c+2} чланова низа. Сада из чињенице да за довољно велико c важи $10^c > 9^{c+2}$ (доказати!) долазимо до контрадикције.

Имитирајући тај доказ можемо показати општије тврђење: ако низ природних бројева задовољава услов $a_n < kn$, за неко $k \in \mathbb{N}$, онда за свако $m \in \mathbb{N}$ и свако $l < m$ постоји члан тог низа у чијем се запису са бројном основом m јавља цифра l. Заиста, претпоставимо супротно, тј. да постоји цифра која се у запису са основом m не јавља ни у једном члану низа. Међу свим природним бројевима са највише c цифара (у том запису), којих има m^c, може бити највише $(m-1)^c$ чланова низа. Нека је $d \in \mathbb{N}$ такво да је $m^d > k$. Тада из услова $a_n < kn$ закључујемо $a_n < m^d n$, тј. за $n = m^c$, да важи $a_{m^c} < m^{c+d}$. Дакле, првих m^c чланова низа налази се међу првих m^{c+d} природних бројева, а ту их може бити највише $(m-1)^{c+d}$. Сада још остаје да приметимо да за довољно велико c важи $m^c > (m-1)^{c+d}$. Контрадикција.

Сада посматрајмо запис чланова низа у систему са основом $m = 10^{2000}$. По горњем тврђењу бар један члан низа има у свом запису цифру која одговара броју $\underbrace{11\ldots1}_{2000}$ у декадном запису. Тај члан садржи и 2 000 узастопних јединица.

354. Нека је $(a_n)_{n\geqslant 2}$ низ природних бројева дефинисан са:

$$a_n = n^6 + 5n^4 - 12n^2 - 36.$$

Доказати:

(а) сваки прост број дели бар један члан тог низа;

(б) постоји природан број који не дели ниједан члан тог низа.

Решење.

(а) Лако се види да је

$$a_n = (n^2+6)(n^2+2)(n^2-3).$$

Претпоставимо да постоји прост број p такав да $p \nmid a_n$, тј.

$$\left(\frac{-2}{p}\right) = \left(\frac{3}{p}\right) = \left(\frac{-6}{p}\right) = -1,$$

где је $\left(\frac{\cdot}{\cdot}\right)$ Лежандров симбол. Лежандрова функција је мултипликативна, што значи да за узајамно просте a и b важи $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$. Али то значи да је

$$\left(\frac{-2}{p}\right)\left(\frac{3}{p}\right) = \left(\frac{-6}{p}\right).$$

Контрадикција.

(б) То је нпр. $n = 8$. Квадратни остаци по модулу 8 су 0, 1 и 4, а a_n је конгруентно са 4 или 6 по модулу 8, па не може бити дељиво са 8.

355. (Савезно такмичење 1994, II разред) Одредити све основе бројних система које су мање од 100, тако да је у тим бројним системима број 2 101 потпун квадрат.

Решење. Означимо са k основу бројног система и нека је број 2 101 у систему са основом k потпун квадрат, рецимо, једнак m^2. Тада је

$$(*)\qquad \begin{aligned} 2\,101 &= 2k^3 + k^2 + 1 = (2k^2 - k + 1)(k+1) \\ &= [2k(k+1) - 3(k+1) + 4](k+1) = m^2. \end{aligned}$$

Највећи заједнички делилац бројева $2k^2 - k + 1$ и $k + 1$ је делилац броја 4 (због $2k^2 - k + 1 - (k+1) = 2k(k-1)$), па из једнакости $(*)$ добијамо да је број $k + 1$ потпун квадрат или је једнак двоструком потпуном квадрату. Ако је $k + 1 = n^2$, онда провером за вредности

n из скупа $\{2, 3, \ldots, 10\}$ добијамо да $n = 2$ и $n = 3$ (тј. $k = 3$ и $k = 8$) дају решења:

$$\begin{array}{ll}\text{за } k = 3: & 2\,101 = 2k^3 + k^2 + 1 = 64 = 8^2;\\ \text{за } k = 8: & 2\,101 = 2k^3 + k^2 + 1 = 1\,089 = 33^2.\end{array}$$

За $n \in \{4, 5, \ldots, 10\}$ провером добијамо да нема нових решења. Ако је $k + 1 = 2n^2$, онда n може узети вредности из скупа $\{2, 3, 4, 5, 6, 7\}$. Провером добијамо да ниједна од датих вредности за n не даје решење.

Према томе, све вредности за k за које је број $2\,101$ потпун квадрат су $k = 3$ и $k = 8$.

356. (Савезно такмичење 1994, III и IV разред) Нека је q прост број већи од 5 и $1 \leqslant p < q$. Претпоставимо да је број $\dfrac{p}{q}$ у децималном запису чисто периодичан, са периодом од $2n$ цифара. Доказати да је збир броја кога формирају првих n цифара периода и броја кога формирају последњих n цифара периода једнак $10^n - 1$.

Решење. Нека је

$$\frac{p}{q} = 0,\underbrace{c_1c_2\ldots c_{2n}}\underbrace{c_1c_2\ldots c_{2n}}\ldots$$

децимални запис броја $\dfrac{p}{q}$, где је $\overline{c_1c_2\ldots c_{2n}}$ основни период. Означимо

$$A = \overline{c_1c_2\ldots c_n} \quad \text{и} \quad B = \overline{c_{n+1}c_{n+2}\ldots c_{2n}}.$$

Тада важи једнакост

$$10^{2n} \cdot \frac{p}{q} = 10^n A + B + \frac{p}{q}\,. \tag{1}$$

Користећи чињеницу да је $\overline{c_1c_2\ldots c_{2n}}$ основни период добијамо да је број $10^{2n} - 1$ дељив са q, а број $10^n - 1$ није дељив са q. Зато је број

10^n+1 дељив са q. Према томе, број $(10^n+1)\dfrac{p}{q}$ је природан, тј.

$$(10^n+1)\frac{p}{q}=A+1. \tag{2}$$

Из једнакости (1) и (2) добијамо да је

$$\begin{aligned}10^nA+B&=(10^{2n}-1)\frac{p}{q}=(10^n-1)(10^n+1)\frac{p}{q}\\&=(10^n-1)(A+1)=10^nA-A+(10^n-1),\end{aligned}$$

одакле следи да је $A+B=10^n-1$, што је и требало доказати.

357. (Савезно такмичење 1997, I разред) Доказати да међу бројевима облика $\left[2^{k+\frac{1}{2}}\right]$, где је k природан број, има бесконачно много парних.

Решење. Претпоставимо супротно и нека је k_0 највећи природан број за који је број $\left[2^{k_0+\frac{1}{2}}\right]$ паран. Нека је $2^{k_0+\frac{1}{2}}=2l+\alpha$, где је α разломљени део броја $2^{k_0+\frac{1}{2}}$. Докажимо да је $\dfrac{1}{2}\leqslant\alpha<1$. Заиста, ако је $0<\alpha<\dfrac{1}{2}$, онда важи

$$\left[2^{k_0+1+\frac{1}{2}}\right]=[2(2l+\alpha)]=4l\in\mathbb{N},$$

а то је у контрадикцији са дефиницијом броја k_0.

Разломљени део броја $2^{k_0+1+\frac{1}{2}}$ је $2\alpha-1$ и за њега аналогно доказујемо $2\alpha-1\in\left[\dfrac{1}{2},1\right)$. Даље, аналогно добијамо да је

$$2(2\alpha-1)-1=4\alpha-3\in\left[\frac{1}{2},1\right)$$

и, уопште, да за сваки природан број n важи:

$$(*) \qquad \frac{1}{2} \leqslant 2^n\alpha - (2^n - 1) < 1.$$

Из неједнакости $(*)$ добијамо да за сваки природан број n важи

$$1 - \alpha \leqslant 1 - \frac{2^n - \frac{1}{2}}{2^n} = \frac{1}{2^{n+1}}\,,$$

што очигледно није тачно. Добијена контрадикција доказује тврђење задатка.

358. (Савезно такмичење 2000, III и IV разред) Нека је S скуп свих простих бројева p таквих да је

$$\frac{1}{p} = 0, c_1c_2\ldots c_{3r_p}c_1c_2\ldots c_{3r_p}\ldots,$$

где је $3r_p$ дужина основног периода у децималном запису. За $k \in \{1, 2, \ldots, r_p\}$ дефинишемо $f(k,p) = c_k + c_{k+r_p} + c_{k+2r_p}$. Одредити

$$\max\{f(k,p) : p \in S, k = 1, 2, \ldots, r_p\}.$$

Решење. Нека је $3r = 3r_p$ број цифара основног периода у децималном запису броја $1/p$, где је $p \in S$. Тада важи

$$p \mid 10^{3r} - 1, \quad p \nmid 10^r - 1, \quad p \mid 10^{2r} + 10^r + 1.$$

Нека је $1/p = 0, c_1c_2c_3\ldots$ и

$$\begin{aligned} x_j &= \frac{10^{j-1}}{p} = c_1c_2\ldots c_{j-1}, c_jc_{j+1}c_{j+2}\ldots, \\ y_j &= \{x_j\} = 0, c_jc_{j+1}c_{j+2}\ldots . \end{aligned}$$

Очигледно важи $c_j < c_j, c_{j+1}c_{j+2}\cdots = 10y_j$, одакле следи

$$f(k,p) = c_k + c_{k+r} + c_{k+2r} < 10(y_k + y_{k+r} + y_{k+2r}).$$

Даље, приметимо да је

$$x_k + x_{k+r} + x_{k+2r} = \frac{10^{k-1}}{p}\left(10^{2r} + 10^r + 1\right)$$

природан број, па је зато и $y_k + y_{k+r} + y_{k+2r}$ цео број. Како је $y_k + y_{k+r} + y_{k+2r} < 3$, то је $y_k + y_{k+r} + y_{k+2r} \leqslant 2$. Према томе, $f(k,p) < 10 \cdot 2 = 20$, тј. $f(k,p) \leqslant 19$. За $p = 7$ добијамо да је $1/p = 0{,}142857142857\ldots$ и $f(2,7) = 4 + 8 + 7 = 19$. Коначно добијамо:

$$\max\{f(k,p) : p \in S, k \geqslant 1\} = 19.$$

359. (Савезно такмичење 2001, III и IV разред) Наћи сва решења једначине $x^y + y = y^x + x$ у скупу природних бројева.

Решење. Лако се уочавају решења $(1,n)$, $(n,1)$, (n,n), где је n произвољан природан број. Нека је $x < y$, тј. $y = x + t$, где је t природан број. Тада једначина постаје:

$$x^{x+t} + x + t = (x+t)^x + x,$$

па је

$$x^t + \frac{t}{x^x} = \left(1 + \frac{t}{x}\right)^x < 3^t,$$

одакле је $x < 3$. Следи да је $x = 2$, па добијамо:

$$2^t = \left(1 + \frac{t}{2}\right)^2 - \frac{t}{4}.$$

Последња једначина у скупу природних бројева има решење $t = 1$, док се за $t \geqslant 2$ лако показује да је

$$2^t > 1 + \frac{3t}{4} + \frac{t^2}{4}.$$

За $t = 1$ налазимо $x = 2, y = 3$.

360. (Савезно такмичење 2001, III и IV разред) Нека је k природан број и N_k број низова дужине 2 001 чији су сви чланови елементи скупа $\{0, 1, 2, \dots, 2k+1\}$, а непаран број чланова сваког низа једнак је 0. Одредити највећи степен двојке који дели N_k.

Решење. Нека је x_n број низова дужине n чији су сви чланови елементи скупа $\{1, 2, \dots, 2k+1\}$, а непаран број њих је једнак нули. Тада је $x_1 = 1$ и

$$x_n = (2k+1)x_{n-1} + (2k+2)^{n-1} - x_{n-1} = 2kx_{n-1} + (2k+2)^{n-1} \quad \text{за } n \geqslant 2.$$

Користећи рекурентну везу добијамо

$$\begin{aligned} x_n &= 2kx_{n-1} + (2k+2)^{n-1} \\ &= (2k)^2 x_{n-2} + 2k(2k+2)^{n-2} + (2k+2)^{n-1} \\ &\vdots \\ &= (2k)^{n-1}x_1 + (2k)^{n-2}(2k+2) + \cdots + \\ &\qquad + 2k(2k+2)^{n-2} + (2k+2)^{n-1}. \end{aligned}$$

Како је $x_1 = 1$, то следи

$$\begin{aligned} x_n &= \frac{(2k+2)^n - (2k)^n}{(2k+2) - 2k} = \frac{1}{2}\left[(2k+2)^n - (2k)^n\right] \\ &= 2^{n-1}\left[(k+1)^n - k^n\right] . \end{aligned}$$

Број $(k+1)^n - k^n$ је непаран, па следи да је 2^{n-1} највећи степен двојке који дели x_n. За $n = 2\,001$, тражени највећи степен двојке је 2^{2000}.

361. (ИМО 1989) Доказати да за сваки природан број n постоји n узастопних природних бројева од којих ниједан није цео степен простог броја.

Решење. За дато $n \in \mathbb{N}$ изаберимо $k = (n+1)!^2 + 1$. Докажимо да ниједан од бројева $k+1, k+2, \ldots, k+n$ није степен простог броја.

За свако j за које је $1 \leqslant j \leqslant n$ број $1+j$ је прави делилац броја $k+j$. Претпоставимо да је за неко такво j испуњено $k+j = p^{\alpha}$, где је p прост, а α природан број. Онда је за неко β, $1 \leqslant \beta < \alpha$, испуњено $1+j = p^{\beta}$. Али тада $p^{\beta+1} \mid (n+1)!^2$ и $p^{\beta+1} \mid p^{\alpha}$, тј. $p^{\beta+1} \mid k-1$ и $p^{\beta+1} \mid k+j$, па $p^{\beta+1} \mid 1+j$, што је контрадикција.

362. (ИМО 2001) Нека је n непаран природан број већи од 1 и нека су k_1, k_2,..., k_n дати цели бројеви. За сваку од $n!$ пермутација $a = (a_1, a_2, \ldots, a_n)$ скупа $\{1, 2, \ldots, n\}$ нека је

$$S(a) = \sum_{i=1}^{n} k_i a_i.$$

Доказати да постоје две пермутације b и c, $b \neq c$, такве да је $n!$ делилац броја $S(b) - S(c)$.

Решење. Означимо са Σ збир свих $n!$ бројева $S(a)$. Претпоставимо да број $S(b) - S(c)$ није дељив са $n!$ за сваке две различите пермутације b и c. Тада сви бројеви $S(a)$ морају имати различите остатке при дељењу са $n!$. Пошто је број свих пермутација једнак $n!$, то се појављују сви остаци $0, 1, 2, \ldots, n! - 1$. Дакле,

$$(1) \qquad \Sigma \equiv \frac{(n!-1)\, n!}{2} \pmod{n!}.$$

Приметимо такође да се сваки од бројева k_i множи, у збиру Σ, сваким од бројева $1, 2, \ldots, n$, укупно $(n-1)!$ пута. Зато је коефицијент уз k_i

у збиру Σ једнак $(n-1)!(1+2+\cdots+n)=\dfrac{1}{2}(n+1)!$, па је

$$\Sigma=\frac{(n+1)!}{2}k_i. \tag{2}$$

За непарне природне бројеве n број $\dfrac{(n+1)!}{2}$ је дељив са $n!$, а број $\dfrac{(n!-1)n!}{2}$ није дељив са $n!$, ако је $n>1$. Зато једнакости (1) и (2) дају контрадикцију.

363. Да ли важи обрат тврђења задатка 177?

Решење. Нека је $q=2^{m+1}+1$ прост број. Тада је $\varphi(q)=q-1=2^{m+1}$. Како је $q\geqslant 5$, то је $(3,q)=1$. Према Малој Фермаовој теореми је $3^{\varphi(q)}\equiv 3^{2^{m+1}}\equiv 1 \pmod q$, па је

$$3^{\varphi(q)/2}\equiv 3^{2^m}\equiv \pm 1 \pmod q. \tag{$*$}$$

Пошто је $q\equiv 1 \pmod 4$ и $q\equiv 2 \pmod 3$, то је

$$\left(\frac{3}{q}\right)=(-1)^{(3-1)(q-1)/4}\left(\frac{q}{3}\right)=\left(\frac{2}{3}\right)=-1,$$

где је $\left(\frac{\cdot}{\cdot}\right)$ Лежандров симбол. С друге стране, пошто је

$$-1=\left(\frac{3}{q}\right)\equiv 3^{(q-1)/2} \pmod q,$$

вредност у $(*)$ је -1, па отуда $q \mid \left(3^{2^m}+1\right)$, што доказује обрат тврђења задатка 177.

364. Нека су m и n природни бројеви такви да

$$m\mid n^2,\quad n^2\mid m^3,\quad m^3\mid n^4,\quad n^4\mid m^5,\quad \ldots$$

Доказати да је $m = n$.

Решење. Нека је:

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_\ell^{\alpha_\ell}, \quad n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_\ell^{\beta_\ell}$$

(неки од бројева α_i, β_i могу бити и једнаки нули). Из услова задатка добијамо да за свако $i \in \{1, 2, \ldots, \ell\}$ важи:

$$\alpha_i \leqslant 2\beta_i \leqslant 3\alpha_i \leqslant 4\beta_i \leqslant 5\alpha_i \leqslant 6\beta_i \leqslant \cdots$$

одакле следи да је:

$$\alpha_i \leqslant 2\beta_i,\ \beta_i \leqslant \frac{3}{2}\alpha_i,\ \alpha_i \leqslant \frac{4}{3}\beta_i,\ \beta_i \leqslant \frac{5}{4}\alpha_i,\ \alpha_i \leqslant \frac{6}{5}\beta_i,\ \beta_i \leqslant \frac{7}{6}\alpha_i,\ \ldots,$$

тј.

$$\alpha_i \leqslant \frac{2k}{2k-1}\beta_i \to \beta_i\ (k \to +\infty) \quad \text{и} \quad \beta_i \leqslant \frac{2k+1}{2k}\alpha_i \to \alpha_i\ (k \to +\infty)$$

па се добија $\alpha_i \leqslant \beta_i$ и $\beta_i \leqslant \alpha_i$, тј. $\alpha_i = \beta_i$.

365. Наћи $\lim\limits_{n\to\infty} \dfrac{\nu(n)}{n}$, где је $\nu(n)$ број простих делилаца броја n.

Решење. Пошто највећи прост делилац броја n није већи од $\sqrt{n}$, имамо да је $\nu(n) < \sqrt{n}$ па је и

$$0 < \frac{\nu(n)}{n} \leqslant \frac{\sqrt{n}}{n} = \frac{1}{\sqrt{n}}.$$

Пошто $\lim\limits_{n\to\infty} \dfrac{1}{\sqrt{n}} = 0$, следи да је и $\lim\limits_{n\to\infty} \dfrac{\nu(n)}{n} = 0$.

366. Доказати да за сваки природан број n важе неједнакости:

$$\frac{n^2}{2} < \varphi(n)\sigma(n) < n^2,$$

где је φ Ојлерова функција, а $\sigma(n)$ збир природних делилаца броја n.

Решење. Пошто је

$$\varphi(n) = n\prod_{i=1}^{k}\left(1-\frac{1}{p_i}\right)$$

и

$$\sigma(n) = \prod_{i=1}^{k}(1+p_i+\cdots+p_i^{\alpha_i}) = n\prod_{i=1}^{k}\left(1+\frac{1}{p_i}+\cdots+\frac{1}{p_i^{\alpha_i}}\right),$$

за n чија је канонска факторизација $p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, имамо да је

$$\varphi(n)\sigma(n) = n^2\prod_{i=1}^{k}\left(1-\frac{1}{p_i^{\alpha_i+1}}\right) < n^2$$

и

$$\varphi(n)\sigma(n) \geqslant n^2\prod_{i=1}^{k}\left(1-\frac{1}{q_i^2}\right),$$

где је q_i $i-$ти прост број. Такође, имамо да је

$$\prod_{i=1}^{k}\left(1-\frac{1}{q_i^2}\right) > \left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\sum_{i=3}^{\infty}\frac{1}{(i+2)^2}\right)$$
$$> \frac{3}{4}\cdot\frac{8}{9}\left(1-\int_4^{\infty}\frac{dx}{x^2}\right) = \frac{1}{2},$$

одакле следи тражена неједнакост.

367. (БМО 1984) Доказати да за сваки природан број m постоји n, $n > m$, тако да се декадни приказ броја 5^n добија из декадног приказа броја 5^m додавањем извесног броја цифара с леве стране.

Решење. Нека је $5^m = \overline{a_k \dots a_0}$. Треба доказати да је за неко n и за неке цифре $a_{k+1}, \dots, a_\ell$ испуњено $5^n = \overline{a_\ell \dots a_k \dots a_0}$, што је еквивалентно са

$$(1) \qquad 5^n - 5^m \equiv 0 \pmod{10^{k+1}}.$$

При том је јасно да је $k + 1 \leqslant m$. Према томе, $5^n - 5^m$ је дељиво са 5^{k+1} за све $n > m$. Дакле, да бисмо доказали конгруенцију (1) треба само показати да постоји $n > m$ тако да је $5^n - 5^m$ дељиво са 2^{k+1}, тј. да је

$$5^{n-m} - 1 \equiv 0 \pmod{2^{k+1}}.$$

Како су 5 и 2^{k+1} узајамно прости бројеви, на основу Ојлерове теореме је

$$5^{\varphi(2^{k+1})} - 1 \equiv 0 \pmod{2^{k+1}},$$

па је довољно узети $n = m + \varphi(2^{k+1})$.

368. Нека је $c_1, c_2, c_3, \dots, c_k$ низ од k цифара, $k \geqslant 2$, $c_1 \neq 0$. Доказати да ако природан број a, $a > 10$, није степен броја 10, тада постоји природан број n такав да децимални запис броја a^n почиње са $c_1 c_2 \dots c_k$.

Решење. Докажимо најпре две леме.

Лема 1. *Ако је θ ирационалан број и N дати позитиван број, тада за сваки реалан број r и свако $\varepsilon > 0$, постоје цели бројеви m и n, при чему је $n > N$, такви да је*

$$r - \frac{\varepsilon}{2} < n\theta + m < r + \frac{\varepsilon}{2},$$

односно за сваки интервал (α, β), постоје цели бројеви m и n, при чему је $n > N$, такви да је $n\theta + m \in (\alpha, \beta)$.

Скица доказа. Наредна тврђења није тешко доказати, а из њих лема директно следи.

1) Затворен интервал $I = [0,1]$ можемо поделити на коначно много подинтервала I_1, I_2,..., I_k чије су дужине мање од ε.

2) За сваки природан број $n > N$, постоји цео број m такав да је $n\theta + m \in I$.

3) Постоји бесконачно много бројева:

$$a_1 = n_1\theta + m_1,\ a_2 = n_2\theta + m_2, \ldots$$

у интервалу I таквих да су n_i и m_i цели бројеви и важе неједнакости $n_i > N$ и $n_{i+1} - n_i > N$.

4) Из 3) следи да бар један од подинтервала, на које је подељен интервал I, садржи два од бројева $a_1, a_2, \ldots$; на пример a_i и a_j.

5) Ако је $j > i$, тада је разлика $a' = a_j - a_i$ број облика $n'\theta + m'$, $m', n' \in \mathbb{Z}$, $n' > N$, и различит је од нуле. Такође је и $|a'| < \varepsilon$.

6) Посматрајмо бројеве $0, a', 2a', 3a', \ldots$. Ако је $a' > 0$, тада ове тачке деле ненегативан део реалне осе на интервале чије су дужине мање од ε. Ако је $a' < 0$, тада ове тачке деле непозитиван део реалне осе на довољно мале интервале. У првом случају додавањем негативних целих бројева бројевима $0, a', 2a', 3a', \ldots$ интервале ограничене овим тачкама транслирамо на негативан део реалне осе. У другом случају додавањем природних бројева бројевима $0, a', 2a', 3a', \ldots$ интервале транслирамо на позитиван део реалне осе. На тај начин читава реална оса покривена је интервалима дужине $a' < \varepsilon$. ■

ЛЕМА 2. *Ако природан број a, већи од 1, није степен броја 10, тада је број $\log a$ ирационалан.*

ДОКАЗ. Нека је $x = \log a$ и претпоставимо да постоје узајамно прости цели бројеви p и q такви да је $x = \dfrac{p}{q}$. Тада, из $a = 10^x$, следи да је $a^q = 2^p \cdot 5^p$. Даље, ако је $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ канонска факторизација броја a, имамо да је

$$p_1^{q\alpha_1} \cdots p_k^{q\alpha_k} = 2^p \cdot 5^p.$$

Тада према Основном ставу аритметике следи да је $k = 2$, $p_1 = 2$, $p_2 = 5$, $q\alpha_1 = p$ и $q\alpha_2 = p$, тј. $\alpha_1 = \alpha_2$. Дакле, $a = 2^{\alpha_1} \cdot 5^{\alpha_1} = 10^{\alpha_1}$, супротно претпоставци да a није степен броја 10. ■

Докажимо сада тврђење задатка. Треба да покажемо да за неко n имамо да је

$$a^n = \overline{c_1c_2 \dots c_kd_1d_2 \dots d_m},$$

где је $d_1d_2 \dots d_m$ неки низ од m цифара.

Нека је $z = \overline{c_1c_2 \dots c_k} = c_110^{k-1} + \dots + c_{k-1}10 + c_k$. Потражимо n тако да за неко m важи

$$z \cdot 10^m \leqslant a^n < (z+1) \cdot 10^m,$$

или еквивалентно

$$\log z + m \leqslant n \log a < \log(z+1) + m.$$

Како је, према леми 2, $\log a$ ирационалан број, користећи лему 1, није тешко доказати да постоје природни бројеви n и m такви да број $n \log a - m$ припада интервалу $(\log z, \log(z+1))$, при чему је $m > 0$ јер је $n \log a > 0$ и $\log z \geqslant 0$.

369. Нека је $c_1, c_2, c_3, \dots, c_k$ низ од k цифара, $k \geqslant 2$, $c_1 \neq 0$. Доказати да постоји потпун квадрат чији децимални запис почиње са $c_1c_2 \dots c_k$.

Решење. Треба да покажемо да за неко n имамо да је

$$n^2 = \overline{c_1c_2 \dots c_kd_1d_2 \dots d_m},$$

где је $d_1d_2 \dots d_m$ неки низ од m цифара.

Нека је $z = \overline{c_1c_2 \dots c_k} = c_110^{k-1} + \dots + c_{k-1}10 + c_k$. Потражимо n тако да за неко m важи

$$z \cdot 10^m \leqslant n^2 < (z+1) \cdot 10^m,$$

или еквивалентно

$$(*) \qquad \log z + m \leqslant 2\log n < \log(z+1) + m.$$

Потражимо бројеве n и m у облику $n = 2^p$ и $m = 2\ell$. Неједнакости $(*)$ постају

$$\frac{1}{2}\log z \leqslant p\log 2 - \ell < \frac{1}{2}\log(z+1).$$

Према леми 1, претходног задатка, постоје природни бројеви p и ℓ који задовољавају последње неједнакости, одакле следи да за ове p и ℓ важи и:

$$z \cdot 10^{2\ell} \leqslant (2^m)^2 < (z+1) \cdot 10^{2\ell}.$$

Дакле, број $(2^m)^2$ почиње цифрама $c_1c_2\ldots c_k$.

370. (ММО 2001) Доказати да постоји природан број n такав да број $2\,000^n$ у декадном запису почиње низом цифара 200 120 012 001.

7. Додатак

Принцип математичке индукције

Нека је $P(n)$ тврђење, које се односи на промењљиву n, $n \in \mathbb{N}$. Да би тврђење било тачно за све природне бројеве довољно је да је:

1. $P(1)$ тачно;

2. за све природне бројеве n тачна импликација $P(n) \Rightarrow P(n+1)$.

Краће принцип математичке индукције можемо записати:

$$P(1) \wedge (\forall n \in \mathbb{N})(P(n) \Rightarrow P(n+1)) \Rightarrow (\forall n \in \mathbb{N})P(n).$$

Важе и следеће модификације овог принципа:

- Индукција са једном претпоставком:

$$\begin{aligned} P(n_0) \ \wedge \ & (\forall n \in \mathbb{N})(n > n_0 \Rightarrow (P(n) \Rightarrow P(n+1))) \Rightarrow \\ & \Rightarrow (\forall n \in \mathbb{N})(n > n_0 \Rightarrow P(n)), \quad \text{где је } n_0 \in \mathbb{N}. \end{aligned}$$

- Индукција са k претпоставки ($k \in \mathbb{N}$):

$$\begin{aligned} & P(1) \wedge P(2) \wedge \cdots \wedge P(k) \wedge (\forall n \in \mathbb{N})(n > k \Rightarrow \\ & (P(n-k+1) \wedge P(n-k+2) \wedge \cdots \wedge P(n) \Rightarrow P(n+1))) \Rightarrow \\ & \Rightarrow (\forall n \in \mathbb{N})P(n). \end{aligned}$$

- Потпуна индукција :

$$(\forall n \in \mathbb{N})((\forall k < n)(P(k) \Rightarrow P(n))) \Rightarrow (\forall n \in \mathbb{N})P(n).$$

Основни идентитети

- Разлика квадрата: $a^2 - b^2 = (a-b)(a+b)$.
- Збир и разлика кубова: $a^3 \pm b^3 = (a \pm b)(a^2 \mp ab + b^2)$.
- Разлика $n-$тих степена за произвољан природан број n:

$$a^n - b^n = (a-b)\left(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \cdots + ab^{n-2} + b^{n-1}\right).$$

- Збир $n-$тих степена за непаран природан број n:

$$a^n + b^n = (a+b)(a^{n-1} - a^{n-2}b + a^{n-3}b^2 - \cdots - ab^{n-2} + b^{n-1}).$$

- Квадрат бинома: $(a \pm b)^2 = a^2 \pm 2ab + b^2$.
- Куб бинома: $(a \pm b)^3 = a^3 \pm 3a^2b + 3ab^2 \pm b^3$.
- Биномна формула:

$$\begin{aligned}(a+b)^n &= \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i \\ &= a^n + \binom{n}{1} a^{n-1} b + \cdots + \binom{n}{k} a^{n-k} b^k + \cdots + \\ &\qquad + \binom{n}{n-1} a b^{n-1} + b^n.\end{aligned}$$

- Особине биномних коефицијената:

$$\binom{n}{k} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!} = \frac{n!}{k!(n-k)!}$$

$$\left(n! = 1\cdot 2\cdot\ldots\cdot(n-1)\cdot n,\quad 0! \overset{\text{деф}}{=} 1\right)$$

$$\binom{n}{k} = \binom{n}{n-k},\quad \binom{n}{0} = \binom{n}{n} = 1$$

$$\sum_{k=0}^{n}\binom{n}{k} = (1+1)^n = 2^n$$

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

- Квадрат тринома: $(a+b+c)^2 = a^2+b^2+c^2+2ab+2bc+2ca.$

- Идентитет Софи Жермен:

$$\begin{aligned} a^4+4b^4 &= a^4+4a^2b^2+4b^4-4a^2b^2 = (a^2+2b^2)^2-(2ab)^2 \\ &= (a^2+2b^2+2ab)(a^2+2b^2-2ab). \end{aligned}$$

- Збирови који се често користе:

$$\begin{aligned} &1+2+3+\cdots+n = \frac{n(n+1)}{2} \\ &1^2+2^2+3^2+\cdots+n^2 = \frac{n(n+1)(2n+1)}{6} \\ &1^3+2^3+3^3+\cdots+n^3 = \left[\frac{n(n+1)}{2}\right]^2 \\ &1^4+2^4+3^4+\cdots+n^4 = \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} \\ &1+3+5+\cdots+(2n-1) = n^2. \end{aligned}$$

Неједнакости

- Бернулијева неједнакост:

$$(1+x)^n \geqslant 1+nx, \quad \text{за } x>-1,\ n\in\mathbb{N}.$$

- Неједнакости између бројних средина (за $a_1, a_2, \ldots, a_n \in \mathbb{R}^+$ и $n \in \mathbb{N}$):

$$\begin{aligned}\min\{a_1,a_2,\ldots,a_n\} &\leqslant \frac{n}{\frac{1}{a_1}+\frac{1}{a_2}+\cdots+\frac{1}{a_n}} \leqslant \sqrt[n]{a_1a_2\cdots a_n}\\ &\leqslant \frac{a_1+a_2+\cdots+a_n}{n} \leqslant \sqrt{\frac{a_1^2+a_2^2+\cdots+a_n^2}{n}}\\ &\leqslant \max\{a_1,a_2,\ldots,a_n\}.\end{aligned}$$

Литература

[1] М. Ашић, М. Божић, Љ. Чукић, В. Јанковић, З. Каделбург, В. Мићић, Л. Милин, Ј. Вукмировић, Ђ. Вукомановић, *Мађународне математичке олимпијаде*, Друштво математичара Србије, Београд, 1986.

[2] Н. Божовић, Ж. Мијајловић, *Увод у теорију група*, Научна књига, Београд, 1990.

[3] А. А. Бухштаб, *Теория чисел*, Москва, 1966.

[4] S. Grozdev, E. Kolev, O. Mushkarov, N. Nikolov, *Bulgarian Mathematical Competitions 1997–2002*, Sofia, 2002.

[5] В. Драговић, Ђ. Дугошија, П. Младеновић, *Републичка и савезна такмичења из математике 1990–2001*, Друштво математичара Србије, Материјали за младе математичаре, Свеска 39, Београд, 2002.

[6] A. Engel, *Problem–Solving Strategies*, Springer–Verlag, New York, Berlin, Heidelberg, 1998.

[7] А. Золић, З. Каделбург, С. Огњановић, *Анализа са алгебром 1*, Круг, Београд, 2003.

[8] В. Јанковић, З. Каделбург, П. Младеновић, *Међународне и балканске математичке олимпијаде 1984–1995. године*, Друштво математичара Србије, Материјали за младе математичаре, Свеска 32, Београд, 1996.

[9] З. Каделбург, П. Младеновић, *Савезна такмичења из математике*, Друштво математичара Србије, Материјали за младе математичаре, Свеска 23, Београд, 1990.

[10] М. Н. Марчевский, *Теория чисел*, Издательство Харьковского Университета, Харьков, 1958.

[11] В. Мићић, З. Каделбург, *Увод у теорију бројева*, Друштво математичара Србије, Материјали за младе математичаре, Свеска 15, Београд, 2001.

[12] Ш. Х. Михелович, *Теория чисел*, Государственное издательство Высшая школа, Москва, 1962.

[13] I. Tonov, K. Bankov, T. Vitanov, D. Rakovska, *Bulgarian Mathematics Competitions, Selected Problems*, Regalia, Sofia, 2001.

[14] Д. Ђ. Тошић, Н. Д. Станковић, *Тестови из математике за пријемне испите*, Грифон, Београд, 1996.

[15] Р. Тошић, В. Вукославчевић, *Елементи теорије бројева*, Алеф, Нови Сад, 1995.

[16] Э.Трост, *Простые числа*, Государственное издательство физико-математической литературы, Москва, 1959.

[17] Д. К Фаддеев, И. С. Соминский, *Сборник задач по высшей алгебре*, Издательство Наука, Москва, 1977.

[18] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford, At the Clarendon press, 1960.

[19] J. Cofman, *Numbers and Shapes Revisited: More Problems for Young Mathematicians*, Clarendon press – Oxford, 1995.

[20] Часопис *„Тангента“*, Друштво математичара Србије

[21] Часопис *„Triangle“*, Удружење математичара Босне и Херцеговине