Математичка гимназија

МАТУРСКИ РАД

из анализе

Квадратни остаци

Ученик:
Војин Бојић

Ментор:
Миљан Кнежевић

Београд, Мај 2023.

Садржај

1 Увод

Математика је изванредна наука која нам омогућава да разумемо и тумачимо различите аспекте света око нас. Математика је оно по чему је ова школа добила име, оно што нас све повезује у овој установи. Једна од њених најинтригантнијих грана је теорија бројева, која проучава целе бројеве и односе између њих. У оквиру ове дисциплине постоји мали кутак посвећен **квадратним остацима**, који већ хиљадама година привлачи пажњу истраживача, математичких ентузијаста и највећих умова света.

Чак и да никад нисте чули за појам квадратног остатка, вероватно можете претпоставити шта је то - број чији се остатак при дељењу са неким другим бројем може написати као квадрат неког целог броја. Ова тривијална, а на први поглед и бескорисна дефиниција, кроз историју је довела до великих резултата у теорији бројева.

У овом матурском раду истражићемо квадратне остатке и њихове примене. Пре тога ћемо морати да се осврнемо на саме основе теорије бројева као што су дељивост, прости бројеви и појам конгруенције. Тек након тога ћемо дефинисати шта је то квадратни остатак, Лежандров и Јакобијев симбол и упустићемо се у истраживање закона који за њих важе, као што су Ојлеров критеријум, Гаусова „златна теорема" и Гаусов закон реципроцитета.

Заронимо у ову узбудљиву математичку тему која ће нас инспирисати и открити нам нове начине размишљања о бројевима и математици!

2 Дељивост целих бројева

Дефиниција 1. Цео број a **дељив је** целим бројем b, различитим од нуле, ако постоји цео број q такав да је $a = bq$.

Ако је број a дељив бројем b, писаћемо $b \mid a$ ("b дели a"), у супротном пишемо $b \nmid a$ ("b не дели a"). Тада кажемо да је број b делилац броја a. На пример, $5 \mid 20$ и $6 \nmid 22$. На основу дефиниције наводимо неколико особина дељивости целих бројева:

Теорема 1. Нека су a, b и c цели бројеви. Тада важи:

1. $a \mid a$.
2. Ако $a \mid b$ и $b \mid c$, онда $a \mid c$.
3. Ако $a \mid b$, онда $a \mid bc$.
4. Ако $a \mid b$ и $a \mid c$, онда $a \mid bx + cy$ за све $x, y \in \mathbf{Z}$.
5. Ако $a \mid b$, онда $ac \mid bc$.
6. Ако $ab \mid ac$ и $a \neq 0$, онда $b \mid c$.
7. $1 \mid a$.
8. $a \mid 0$.
9. Ако $a \mid b$ и $b \neq 0$, онда је $|a| \leq |b|$.
10. Ако $a \mid b$ и $b \mid a$, онда је $a = b$ или $a = -b$.
11. Ако $a \mid b$, онда $\dfrac{b}{a} \mid b$.

Доказ. 4. Како важи $a \mid b$, то постоји $\alpha_1 \in \mathbf{Z}$ такво да је $b = \alpha_1 a$. Слично, постоји $\alpha_2 \in \mathbf{Z}$ такво да је $c = \alpha_2 a$, па за произвољне целе бројеве x и y важи $bx+cy = \alpha_1 ax+\alpha_2 ay = a(\alpha_1 x+\alpha_2 y)$, тј. $bx + cy = a\alpha_3$, $\alpha_3 \in \mathbf{Z}$, па по дефиницији дељивости важи $a \mid bx + cy$.
Остале тврдње се доказују на сличан начин. ■

Теорема 2. Ако се у једнакости облика

$$\sum_{k=1}^{n} a_k = 0 \tag{1}$$

за све сабирке осим једног зна да су дељиви целим бројем a, онда је и тај сабирак дељив са a.

Доказ. Нека за број a_i не знамо да ли је дељив са a, а за све остале знамо. Важи $a_k = ab_k$, $k \neq i$,$b_k \in \mathbf{Z}$. Тада је једнакост (1) еквивалентна са

$$a_i = -ab_1 - ab_2 - \cdots - ab_n = a(-b_1 - \cdots - b_n) = ab_i, \quad b_i \in \mathbf{Z},$$

што је и требало доказати.■

Теорема 3 (Алгоритам дељења). Ако је $a \in \mathbf{Z}$ и $b \in \mathbf{N}$, тада се a може на јединствен начин представити преко b у облику

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

где $q, r \in \mathbf{Z}$. Број q се назива *количником*, а број r *остатком* при дељењу a са b.

Доказ. Како треба да одредимо целе бројеве q и r за које је $a - bq = r$, има смисла посматрати скуп $S = \{a - kb : k \in \mathbf{Z}\}$. Узмимо у њему најмањи позитиван елемент, који постоји по једној од основних особина скупа природних бројева (сваки подскуп природних бројева има најмањи елемент). Нека је то број $a - bq$ и обележимо га са r. Тада је $a = bq + r$ и притом важи $0 \leq r < b$, јер би у супротном број $a - b(q + 1)$ био позитиван и мањи од $a - bq$, контрадикција. Тиме је доказана егзистенција бројева q и r. Претпоставимо да постоји још један пар (q_1, r_1), такав да је $a = bq_1 + r_1$ и $0 \leq r_1 < b$. Одузимањем ове једнакости од претходне добијамо

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

одакле следи $b \mid r - r_1$. Из $0 \leq r < b$ и $0 \leq r_1 < b$ следи $|r - r_1| < b$, па је на основу теореме 1.9 $r - r_1 = 0$, тј. $r = r_1$, одакле добијамо и $q = q_1$, чиме је доказана јединственост бројева q и r. ■

Пример 1. Наћи све остатке које квадрати целих бројева дају при дељењу са 4.
Решење. По претходној теореми можемо да напишемо сваки природан број n у облику $n = 4k + r$, где је $r \in \{0, 1, 2, 3\}$. Квадрирањем добијамо $n^2 = 16k^2 + 8kr + r^2 = 4K + r^2$ за $K = 4k^2 + 2kr$. Убацивањем редом добијамо - за $r = 0, n^2 = 4K$, за $r = 1, n^2 = 4K + 1$, за $r = 2, n^2 = 4(K + 1)$, за $r = 3, n^2 = 4(K + 2) + 1$, па су могући остаци при дељењу n^2 са 4 бројеви 0 и 1. □

Цео број d је **заједнички делилац** бројева $a_1, a_2, ..., a_n$ ако $d \mid a_1$, $d \mid a_2, ...,$ $d \mid a_n$. Сваки цео број различит од нуле има коначно много делилаца, па је и скуп заједничких делилаца целих бројева $a_1, a_2, ..., a_n$ коначан и у њему постоји највећи елемент. У складу с тим даје се и

Дефиниција 2. Највећи међу заједничким делиоцима бројева $a_1, a_2, .., a_n$ је **највећи заједнички делилац** бројева $a_1, a_2, ..., a_n$ и обележава се са $(a_1, a_2, ..., a_n)$. За целе бројеве $a_1, a_2, .., a_n$ кажемо да су **релативно прости** ако је $(a_1, a_2, ..., a_n) = 1$. За два цела броја a и b кажемо да су **узајамно прости** ако је $(a, b) = 1$. За целе бројеве $a_1, a_2, .., a_n$ кажемо да су **релативно прости у паровима** ако је $(a_i, a_j) = 1$ за $i = 1, 2, ..., n,\ j = 1, 2, ..., n,\ i \neq j$.

Осим уведене ознаке $(a_1, a_2, ..., a_n)$, у литератури се користе и друге ознаке, нпр. НЗД$(a_1, a_2, ..., a_n)$ и $\gcd(a_1, a_2, ..., a_n)$.

Јасно је да важи $(a, 1) = 1,\ c \mid a$ и $c \mid b \Rightarrow c \mid (a, b)$, као и $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$.

Теорема 4. Ако је d највећи заједнички делилац бројева a и b, тада постоје цели бројеви α и β такви да је $d = \alpha a + \beta b$. Прецизније, d је најмања позитивна вредност коју узима израз $\alpha a + \beta b$ када α и β пролазе кроз целе бројеве.
Доказ. Посматрајмо скуп целих бројева

$$S = \{\alpha a + \beta b \mid \alpha, \beta \in \mathbf{Z}\}.$$

Означимо са $d = \alpha a + \beta b$ најмањи позитиван елемент тог скупа. Доказаћемо да је $d = (a, b)$. На основу теореме 1.4 важи $(a, b) \mid d$. Претпоставимо да $d \nmid a$. Тада постоје цели бројеви q и r за које је $a = dq + r, 0 < r < d$. Но, тада је $r = a - dq = a - q(\alpha a + \beta b) = a(1 - q\alpha) - q\beta b \in S$, контрадикција. Дакле, $d \mid a$. Слично доказујемо $d \mid b$. Према томе, $d \mid (a, b)$, што по теореми 1.10 повлачи $d = (a, b)$. ■

Последица 1. Бројеви a и b су узајамно прости ако и само ако постоје цели бројеви α и

β такви да је $\alpha a + \beta b = 1$.
Доказ. Ако је d било који заједнички делилац бројева a и b, тада важи $d \mid \alpha a + \beta b = 1 \Rightarrow (a, b) = 1$. Обратно је посебан случај теореме 4. ■

Последица 2. Линеарна једначина $ax + by = c$ има решења ако и само ако $(a, b) \mid c$. ■

Теорема 5.

1. Ако је $k > 0$, онда је $(ka, kb) = k(a, b)$.
2. Ако је $a = bq$ и $b \geq 0$, онда је $(a, b) = b$.

Доказ.

1. Из теореме 4 знамо да је (a, b) најмањи природан број облика $\alpha a + \beta b,\ \alpha, \beta \in \mathbf{Z}$. Тада је $k(a, b) = k(\alpha a + \beta b) = \alpha ka + \beta kb$, што је најмањи природан број облика $\alpha(ka) + \beta(kb)$, што је управо (ka, kb).
2. На основу претходног је $(a, b) = (bq, b) = b(q, 1) = b$. ■

Приликом решавања задатака често се користи следеће тврђење.

Теорема 6. Ако $q \mid ab$ и при томе су q и b узајамно прости, онда $q \mid a$.

Доказ. Из услова да су q и b узајамно прости и последице 1 знамо да постоје цели бројеви α, β за које је $\alpha q + \beta b = 1$, што након множења са a постаје $\alpha aq + \beta ab = a$. Сада је лева страна по услову задатка дељива са q, што одмах повлачи $q \mid a$. ■

Теорема 7. Ако је $a = bq + r$, тада је $(a, b) = (b, r)$.
Доказ. Нека је $D = \{d \in \mathbf{Z} : d \mid a \text{ и } d \mid b\}$ и $D' = \{d \in \mathbf{Z} : d \mid b \text{ и } d \mid r\}$. Ако $d \in D$, онда важи $d \mid a + (-q)b$, тј. $d \mid r$, па $d \in D'$. Дакле, $D \subseteq D'$. Ако $d \in D'$, онда важи $d \mid b$ и $d \mid r$, па важи $d \mid qb + r = a$, па $d \in D$, што значи $D' \subseteq D$. Следи да је $D = D'$, па су им и највећи елементи једнаки, тј. $(a, b) = (b, r)$. ■

Поставља се питање како наћи највећи заједнички делилац целих бројева a и b. Како он не зависи од знака, можемо сматрати да су a и b природни бројеви. Посматрајмо следећи низ једнакости:

$$\begin{aligned} a &= bq_1 + r_1, & 0 \leq r_1 < b, \\ b &= r_1 q_2 + r_2, & 0 \leq r_2 < r_1, \\ r_1 &= r_2 q_3 + r_3, & 0 \leq r_3 < r_2, \\ &\dots \\ r_{n-1} &= r_n q_{n+1}. \end{aligned}$$

Како бројеви r_n чине строго опадајући низ природних бројева, овај низ ће се након коначног броја корака завршити, тј. доћи ћемо до једнакости облика $r_{n-1} = r_n q_{n+1}$, која говори о дељивости два узастопна остатка.

Теорема 8. Последњи остатак r_n који је различит од нуле у претходном низу представља највећи заједнички делилац бројева a и b.
Доказ. На основу теореме 7 добијамо низ једнакости

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

Како $r_n \mid r_{n-1}$, на основу теореме 5.2 важи $(r_{n-1}, r_n) = r_n$, што је и требало доказати.

Малопре описан поступак за добијање највећег заједничког делиоца два броја зове се **Еуклидов алгоритам**, назван по старогрчком математичару.
Преко Еуклидовог алгоритма не само да можемо да нађемо највећи заједнички делилац два цела броја a и b, већ можемо наћи и целе бројеве α и β из теореме 4 за које важи $\alpha a+\beta b=(a,b)$.

Пример 2. Наћи највећи заједнички делилац бројева $a=792$ и $b=336$ и представити га као линеарну комбинацију $\alpha a+\beta b$.
Решење. Еуклидовим алгоритмом добијамо

$$792=336\cdot 2+120,\ 336=120\cdot 2+96,\ 120=96\cdot 1+24,\ 96=24\cdot 4+0.$$

Па је $(792,336)=24$. Линеарну комбинацију добијамо на следећи начин

$$24=120-96=120-(336-120\cdot 2)=3\cdot 120-336=3\cdot(792-2\cdot 336)-336=3\cdot 792-7\cdot 336.\square$$

Дефиниција 3. Заједничким садржаоцем целих бројева $a_1,a_2,...,a_n$, различитих од нуле, називамо сваки број који је дељив сваким од бројева $a_1,a_2,...,a_n$. Најмањи међу позитивним садржаоцима тих бројева зове се **најмањи заједнички садржалац** и обележава се са $[a_1,a_2,...,a_n]$.
Осим уведене ознаке $[a_1,a_2,...,a_n]$ користе се још и НЗС$(a_1,a_2,...,a_n)$ и $\mathrm{lcm}(a_1,a_2,...,a_n)$.

Највећи заједнички делилац и најмањи заједнички садржалац два цела броја повезани су на следећи начин.

Теорема 9. За целе бројеве a и b важи $(a,b)\cdot[a,b]=|ab|$. Специјално, за узајамно просте бројеве a и b важи $[a,b]=|ab|$.

Доказ. Да нам не би сметале апсолутне заграде, претпоставимо не умањујући општост да су a,b природни бројеви. Нека је $s=[a,b]$. Тада је $s=ak$ и $b\mid s$, па је број $\frac{ak}{b}$ цео. Како је s најмањи заједнички садржалац, број k можемо схватити као најмањи природан број за који је број $\frac{ak}{b}$ цео. Даље, нека је $d=(a,b)$ и $a=\alpha d, b=\beta d, (\alpha,\beta)=1$. Тада је $\frac{ak}{b}=\frac{\alpha k}{\beta}$, па $\beta\mid\alpha k$. Тада по теореми 6 важи $\beta\mid k$. Најмање k које је дељиво са β је управо β. Дакле, $s=a\beta$, па је $sd=a\beta d=ab$, што је и требало доказати. ■

Ова теорема се може једноставније доказати користећи основни став аритметике (видети теорему 4 у наредном поглављу).

3 Прости бројеви

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

Првих неколико простих бројева су: $2,3,5,7,11,13,17,19...$
Број 1 није ни прост ни сложен. Лако се види да ако прост број p не дели цео број a, онда су они узајамно прости.

Теорема 1. Сваки природан број $n\geq 2$ је или прост или производ простих бројева.

Доказ. Тврђење доказујемо индукцијом по n.
База индукције: Број 2 је прост, па је тврђење тачно за $n=2$.

Индуктивна хипотеза: Претпоставимо да за сваки природан број k, $k < n$, важи тврђење. Ако је број n прост, тврђење важи и за n. Ако је n сложен, постоји природан број m, $1 < m < n$, који дели n. Тада су бројеви m и $\frac{n}{m}$ природни бројеви већи од 1 и мањи од n, па за њих важи индуктивна хипотеза, тј. они су прости или производ простих бројева, па закључујемо да је и $n = m \cdot \frac{n}{m}$ производ простих бројева. Дакле, тврђење важи за n, па на основу принципа математичке индукције, важи за сваки природан број n, што је и требало доказати. ■

Да бисмо одредили све просте бројеве мање од датог природног броја N, можемо се послужити такозваним **Ерастотеновим ситом(решетом)**. Исписујемо све природне бројеве до N:

$$\not{1}, 2, 3, \not{4}, 5, \not{6}, 7, \not{8}, \not{9}, \not{10}, 11, \not{12}, 13, \not{14}, \not{15}, \not{16}, 17, \not{18}, 19, \not{20}, \not{21}, \not{22}, 23, ..., N.$$

Прво прецртамо јединицу. Затим, први прост број 2 не прецртамо, али прецртамо све бројеве веће од 2 који су дељиви са 2 (они су сигурно сложени). Следећи непрецртани број је 3 - прецртамо све бројеве веће од 3 који су дељиви са 3. Знамо да је 3 прост, јер да није, био би прецртан. Следећи непрецртани број је 5, па прецртавамо све бројеве дељиве са 5 који су већи од 5. Знамо да је 5 прост, јер да је сложен, био би дељив са 2 или са 3, а сви такви бројеви су прецртани. Понављајући овај поступак добијамо све просте бројеве мање од N.

Теорема 2. Малопре описан поступак можемо завршити кад прецртамо све сложене бројеве који су садржаоци простих бројева не већих од $\sqrt{N}$.
Доказ. Претпоставимо да смо стигли до последњег простог броја не већег од $\sqrt{N}$ и да је остао барем један непрецртан сложен број m. Тада је по претходној теореми m производ простих бројева. Нека су p и q два највећа проста делиоца од m (тада је $m = pqn$, $n \in \mathbf{N}$). Онда важи $p > \sqrt{N}$ и $q > \sqrt{N}$, јер би у супротном m био прецртан. Међутим, тада је $m = pqn \geq pq > \sqrt{N} \cdot \sqrt{N} = N$, контрадикција. Дакле, сви сложени бројеви мањи од N су прецртани, што је и требало доказати.■

Теорема 3. (Еуклид) Постоји бесконачно много простих бројева. Другим речима, од сваког простог броја постоји већи прост број.
Доказ. Претпоставимо да постоји коначно много простих бројева. Нека су то бројеви $p_1, p_2, ..., p_n$. Посматрајмо број

$$N = p_1 p_2 \cdots p_n + 1.$$

Он је већи од сваког од бројева $p_1, p_2, ..., p_n$, па је и различит од њих, што значи да је сложен. Према теореми 1 он мора имати неки прост делилац. Међутим, то је немогуће јер број N при дељењу са сваким од бројева $p_1, p_2, ..., p_n$ даје остатак 1. Тиме је доказ завршен. ■

Иако простих бројева има бесконачно много, они су „ретки“ у скупу природних бројева. О томе говори следећа теорема.

Теорема 4. За сваки природан број n постоји n узастопних сложених природних бројева.
Доказ. Посматрајмо бројеве

$$A_1 = (n+1)! + 2,$$
$$A_2 = (n+1)! + 3,$$
$$\cdots$$
$$A_n = (n+1)! + n + 1.$$

Они представљају низ од n узастопних природних бројева, и притом је сваки од њих сложен - број A_k је већи од $k+1$ и дељив са $k+1$. ■

Означимо са $\pi(x)$ број простих бројева који нису већи од природног броја x. Прости бројеви су веома неправилно распоређени у низу природних бројева, па је проблем испитивања понашања функције $\pi(x)$ веома тежак. На основу претходне теореме знамо да важи $\lim_{x\to\infty}\pi(x)=+\infty$. Један од основних резултата у теорији бројева представља **асимптотски закон расподеле простих бројева** који гласи:

$$\lim_{x\to\infty}\pi(x)\cdot\frac{\ln(x)}{x}=1.$$

Пример 1. Доказати да сваки природан број облика $4k+3$ има барем један прост делилац истог облика.
Решење. Такав број је непаран, па су сви његови прости делиоци облика $4k+1$ и $4k+3$. Ако би сви били облика $4k+1$, тада би и сам број био тог облика. □

Пример 2. Доказати да постоји бесконачно много простих бројева облика $4k+3$.
Решење. Претпоставимо да таквих бројева постоји коначно много, нека су то бројеви $p_1,p_2,...,p_n$. Обележимо њихов производ са N. Посматрајмо број $4N-1$. Он је облика $4k+3$, па по претходном примеру мора имати барем један прост делилац p истог тог облика, односно један од бројева $p_1,p_2,...,p_n$. Међутим, тада $p\mid N$ и $p\mid 4N-1$, па $p\mid 1$, контрадикција. □

Следеће тврђење се лако изводи, али је веома корисно у решавању задатака.

Теорема 5. Ако је p прост број и $p\mid ab$, онда $p\mid a$ или $p\mid b$.
Доказ. Претпоставимо да p не дели a. Тада су a и p узајамно прости, па по теореми 6 из прошлог поглавља важи $p\mid b$. ■

Следећа теорема је једна од најважнијих у теорији бројева, па у складу с тиме носи назив **основни став аритметике**.

Теорема 6. Сваки природан број N већи од 1 се може једнозначно изразити (репрезентовати) у облику производа простих чинилаца, са тачношћу до њиховог поретка.
Доказ. У теореми 1 смо доказали да се сваки природан број већи од 1 може представити као производ простих бројева. Докажимо сада да је та репрезентација јединствена. Претпоставимо да је природан број N најмањи који има две репрезентације:

$$N=p_1p_2...p_k=q_1q_2...q_l,$$

где су p_i и q_j прости бројеви. Како $p_1\mid q_1q_2...q_l$, по теореми 5 имамо да p_1 дели један од ових чинилаца, нека је то q_1. Међутим, како је q_1 прост, његови једини делиоци су 1 и q_1, па имамо $p_1=q_1$. Након скраћивања обе стране једнакости добијамо

$$M=p_2p_3...p_k=q_2q_3...q_l,$$

па број $M<N$ има две различите репрезентације, што је у контрадикцији са минималности броја N. Тиме је доказ завршен. ■

Ако се у репрезентацији броја N неки чиниоци понављају, па се, рецимо, p_1 јавља α_1 пута, p_2 јавља α_2 пута, ... , p_k јавља α_k пута, онда се облик

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

зове канонски облик природног броја N (**канонска факторизација**).

Помоћу канонске факторизације лако се одређује највећи заједнички делилац и најмањи заједнички садржалац два броја. Наиме, ако за целе бројеве a и b важи

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

(допуштамо да неки од бројева α_i, β_i буду нула), тада је:

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

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

Коришћењем ових једнакости се лако доказује теорема 9 из првог поглавља, уз помоћ релације $min\{\alpha,\beta\} + max\{\alpha,\beta\} = \alpha + \beta$.

Теорема 7. Ако је производ два узајамно проста природна броја квадрат целог броја,

$$ab = c^2, \qquad (a,b) = 1,$$

тада су и a и b квадрати целих бројева.
Доказ. Да би број био квадрат потребно је и довољно да су му сви експоненти у факторизацији парни. Како су бројеви a и b узајамно прости, сваки прост делилац броја c^2 се у потпуности јавља или у a или у b, па зато прости фактори бројева a и b морају имати парне експоненте. ■

Пример 3. Нека су $a, b, c \in \mathbf{N}$ такви да је $\dfrac{ab}{a-b} = c$ и $(a,b,c) = 1$. Доказати да је $a - b$ потпун квадрат.
Решење. Претпоставимо да $a - b$ није потпун квадрат. Тада постоје прост број p и природан број k за које важи $p^{2k-1} \mid a - b$ и $p^{2k} \nmid a - b$. Из услова $a - b \mid ab$ имамо да p^k дели барем један од бројева a и b. Међутим, тада из $p^{2k-1} \mid a - b$ следи да p^k дели и други број. Но, тада $p^{2k} \mid ab$, па $p \mid c$, и a, b, c нису узајамно прости, контрадикција. □

Теорема 8. Нека је $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$ канонска факторизација броја a. Тада су сви позитивни делиоци броја a облика

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_n^{\beta_n}, \qquad 0 \le \beta_1 \le \alpha_1, \qquad 0 \le \beta_2 \le \alpha_2, ..., \qquad 0 \le \beta_n \le \alpha_n.$$

Специјално, укупан број позитивних делилаца броја a је

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_n + 1). \quad ■$$

Дефиниција 2. Укупан број позитивних делилаца природног броја a означавамо са $\tau(a)$.

Пример 4. Ако a има само један прост делилац - $a = p^\alpha$, тада је $\tau(a) = \alpha + 1$. Ако је a облика $p_1 p_2 \cdots p_n$, за различите просте бројеве p_i, тада је $\tau(a) = 2^n$. □

Пример 5. Ако природан број n има непаран број позитивних делилаца, тада је он потпун квадрат. Доказати.
Решење. Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонски облик броја n. Тада је број позитивних делилаца $\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$ непаран само ако су сви бројеви $\alpha_1, \alpha_2, ..., \alpha_k$ парни, па је n потпун квадрат. □

4 Конгруенције

У првој глави смо показали да се, за неки фиксиран број m, сваки природан број може записати у облику $n = km + r$, где су k, r цели бројеви и важи $0 \leq r < m$. Број r смо назвали остатком при дељењу броја n бројем m. Тај остатак може имати вредности $0, 1, ..., m-1$. Ови остаци, односно бројеви који дају исти остатак при дељењу са датим m, су предмет нашег тренутног занимања. У складу са тиме даје се следећа дефиниција.

Дефиниција 1. (Гаус) Нека је дат природан број m, већи од 1. За два цела броја a и b кажемо да су **конгруентна по модулу** м ако дају исти остатак при дељењу са m. Пишемо

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

Теорема 1.

1. $a \equiv b \pmod{m}$ ако и само ако је $a = b + km$ за неки цео број k.
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 (тј. она је рефлексивна, симетрична и транзитивна). ■

Многе особине конгруенција су сличне особинама релације једнакости, али постоје и знатне разлике.

Теорема 2.

1. Ако је $a \equiv b \pmod{m}$ и $c \equiv d \pmod{m}$, онда је
$$ax + cy \equiv bx + dy \pmod{m},$$
за све целе бројеве x, y.
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 $d \mid m$, $d > 1$, онда је $a \equiv b \pmod{d}$.
4. Нека је $P(x)$ полином по x са целобројним коефицијентима. Тада из $a \equiv b \pmod{m}$ следи $P(a) \equiv P(b) \pmod{m}$.

Доказ.

1. Из $a \equiv b \pmod{m}$ следи $a - b = km$ за неко целобројно k. Слично из $c \equiv d \pmod{m}$ следи $c - d = lm$ за неко целобројно l. Тада је за произвољне $x, y \in \mathbf{Z}$,
$$(ax + cy) - (bx + dy) = (a - b)x + (c - d)y = kmx + lmy = (kx + ly)m,$$
па је $ax + cy \equiv bx + dy \pmod{m}$
2. Имамо $a = b + km$ и $c = d + lm$, за неке $k, l \in \mathbf{Z}$. Множењем добијамо $ac = bd + (kd + lb + klm)m$, па је $ac \equiv bd \pmod{m}$.
3. Нека $d \mid m$ и $d > 1$. Тада је $m = \alpha d$, $\alpha \in \mathbf{N}$. Из $a \equiv b \pmod{m}$ следи да за неко целобројно k важи $a - b = km = (k\alpha)d$, па је $a \equiv b \pmod{d}$.
4. Тврђење доказујемо директном применом ставки 1 и 2. ■

Теорема 3.

1. Ако је $(a,m)=1$ и $ax \equiv ay \pmod{m}$, онда је $x \equiv y \pmod{m}$.
2. $ax \equiv ay \pmod{m}$ ако и само ако је $x \equiv y \pmod{\frac{m}{(a,m)}}$.
3. $x \equiv y \pmod{a}$ и $x \equiv y \pmod{b}$ ако и само ако је $x \equiv y \pmod{[a,b]}$.

Доказ.

1. Специјалан случај 2.
2. Ако је $ax \equiv ay \pmod{m}$, $d=(a,m)$ и $a=\alpha d, m=\beta d$, онда је $\alpha(x-y)=k\beta$, где су α и β узајамно прости, па $\beta \mid x-y$, тј. $x \equiv y \pmod{\frac{m}{(a,m)}}$. Обратно се слично доказује.
3. Ако је $x \equiv y \pmod{a}$ и $x \equiv y \pmod{b}$ онда је $x-y=\alpha a$ и $x-y=\beta b$, па је $x-y$ заједнички садржалац a и b, што значи да је $x-y=\gamma[a,b]$, односно $x \equiv y \pmod{[a,b]}$. Обратно је став 3 претходне теореме. ■

Истакнимо да тврђење 1 без претпоставке $(a,m)=1$ не важи, што значи да у релацији конгруенције не можемо у општем случају да „скраћујемо“ чланове.

Пример 1. Наћи остатак при дељењу броја 3^{40} са 13.
Решење. Коришћењем особина конгруенција добијамо:

$$3^1 \equiv 3 \pmod{13}, \qquad 3^2 \equiv 9 \pmod{13}, \qquad 3^3 \equiv 27 \equiv 1 \pmod{13},$$

па је $3^{39}=(3^3)^{13} \equiv 1^{13} \equiv 1 \pmod{13}$. Коначно, $3^{40} \equiv 3 \cdot 3^{39} \equiv 3 \pmod{13}$. □

Пример 2. Одреди најмањи природан број n за који је збир

$$1^{2019}+2^{2020}+3^{2021}+4^{2022}+5^{2023}+n$$

дељив са 13.
Решење. Користећи особине конгруенција рачунамо остатке:

$$2^1 \equiv 2 \pmod{13}, \qquad 2^2 \equiv 4 \pmod{13}, \qquad 2^3 \equiv 8 \pmod{13}, \qquad 2^4 \equiv 3 \pmod{13},$$

$$2^5 \equiv 6 \pmod{13}, \qquad 2^6 \equiv 12 \pmod{13}.$$

Приметимо да је $12 \equiv -1 \pmod{13}$, па је $2^{2020} \equiv 2^4 \cdot (2^6)^{336} \equiv 3 \cdot (-1)^{336} \equiv 3 \pmod{13}$. На сличан начин добијамо

$$3^3 \equiv 1 \pmod{13}, \quad 4^3 \equiv -1 \pmod{13}, \quad 5^2 \equiv -1 \pmod{13},$$

одакле је

$$3^{2021} \equiv 9 \pmod{13}, \quad 4^{2022} \equiv 1 \pmod{13}, \quad 5^{2023} \equiv 8 \pmod{13}.$$

Даље је

$$1^{2019}+2^{2020}+3^{2021}+4^{2022}+5^{2023}+n \equiv 22+n \pmod{13},$$

па је тражени број $n=4$. □

Сада наводимо познату теорему о решавању система линеарних конгруенција.

Теорема 4. (Кинеска теорема о остацима) Нека су дати цели бројеви $a_1, a_2, ..., a_k$ и узајамно прости у паровима цели бројеви $m_1, m_2, ...m_k$. Тада систем линеарних конгруенција

$$x \equiv a_1 \pmod{m_1}$$

$$x \equiv a_2 \pmod{m_2}$$

.....

$$x \equiv a_k \pmod{m_k}$$

има једно и само једно решење по модулу $M = m_1 m_2 \cdots m_k$.
Доказ. За свако $i \in \{1, 2, ..., k\}$ бројеви m_i и $\frac{M}{m_i}$ су узајамно прости, па постоје цели бројеви y_i и z_i за које је $y_i m_i + z_i \frac{M}{m_i} = 1$. Означимо $M_i = z_i \frac{M}{m_i}$, тада је $M_i \equiv 1 \pmod{m_i}$ и $M_i \equiv 0 \pmod{m_j}$ за $j \neq i$. Онда важи $M_i a_i \equiv a_i \pmod{m_i}$ и $M_i a_i \equiv 0 \pmod{m_j}$ за $j \neq i$, па је

$$x_0 = M_1 a_1 + M_2 a_2 + ... + M_k a_k \equiv a_i \pmod{m_i}, \qquad i = 1, 2, ..., k,$$

односно број x_0 је једно решење овог система конгруенција. Нека је x' произвољно решење овог система. Тада је $x' \equiv x_0 \pmod{m_1}, x' \equiv x_0 \pmod{m_2}, ..., x' \equiv x_0 \pmod{m_k}$, и како је $(m_i, m_j) = 1$ за $i \neq j$, тј. $[m_1, m_2, ..., m_k] = M$, следи да је $x' \equiv x_0 \pmod{M}$. ■

Релација бити конгруентан по датом модулу је релација еквиваленције, што значи да она „разбијачкуп целих бројева на класе еквиваленције. За дато $m > 1$ постоји управо m класа еквиваленције. То су класе бројева конгруентних са $0, 1, ..., m-1$ по модулу m. Било који скуп од m бројева, у којем је сваки из другачије класе, називамо **потпуним системом остатака** по модулу m. Најчешће се користи малопре наведен скуп $\{0, 1, ..., m-1\}$, али вреди споменути и „систем остатака најмањих по модулу"који за непарно m чине

$$-\frac{m-1}{2}, ..., -1, 0, 1, ..., \frac{m-1}{2},$$

а за парно m

$$-\frac{m}{2}+1, ..., -1, 0, 1, ..., \frac{m}{2} \quad \text{или} \quad -\frac{m}{2}, ..., -1, 0, 1, ..., \frac{m}{2}-1.$$

Потпун систем остатка из којег смо „избацилишве оне чланове који нису узајамно прости са m зове се **сведен систем остатака** по модулу m. Од којег год потпуног система остатака да кренемо, лако се види да ће сведен систем остатака увек имати исти број елемената (број a је узајамно прост са m ако и само ако је број $a + km$ узајамно прост са m). У теорији бројева број елемената тог скупа носи посебно име.

Дефиниција 2. 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 $\varphi(m)$. Фунцкија φ зове се **Ојлерова функција**.

За прост број p сви елементи скупа $\{1, 2, ..., p\}$ осим p су узајамно прости са p, па је $\varphi(p) = p - 1$. За број $n = 2^k$, сви непарни елементи скупа $\{1, 2, ..., p\}$ су узајамно прости са n, па је $\varphi(2^k) = 2^{k-1}$.

Генерално, за прост број p и природан број α, у низу

$$1, 2, ..., p-1, p, p+1, ..., 2p-1, 2p, 2p+1, ..., p^{\alpha-1}p-1, p^{\alpha-1}p$$

постоји тачно $p^{\alpha-1}$ бројева дељивих са p, па је $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$.

О потпуним и сведеним системима остатака важи следеће изузетно корисно тврђење.

Теорема 5. Нека је $(a,m)=1$ и нека је $\{\alpha_1,\alpha_2,...,\alpha_k\}$ произвољан потпун (сведен) систем остатака по модулу m. Тада је $\{a\alpha_1,a\alpha_2,...,a\alpha_k\}$ такође потпун (сведен) систем остатака по модулу m.
Доказ. Како ови скупови имају исти број елемената, треба доказати да важи $a\alpha_i \equiv a\alpha_j \iff i=j$, што очигледно важи на основу теореме 3.1. ■

Теорема 6. Ојлерова функција φ је мултипликативна.
Доказ. Јасно је $\varphi(2)=1\neq 0$. Нека је $(m,n)=1$. Посматрајмо табелу $m\times n$ у којој се налазе сви природни бројеви од 1 до mn.

$$\begin{array}{ccccc} 1 & 2 & ... & n-1 & n \\ n+1 & n+2 & ... & 2n-1 & 2n \\ ... & ... & ... & ... & ... \\ (m-1)n+1 & (m-1)n+2 & ... & mn-1 & mn \end{array}$$

Ако је број a узајамно прост са n, тада је и сваки број конгруентан са a по модулу n такође узајамно прост са n. Другим речима, у свакој колони горње табеле, или су сви бројеви узајамно прости са n, или ниједан није. Таквих колона има $\varphi(n)$. Но, како су m и n узајамно прости, свака колона представља потпун систем остатака по модулу m, па се у свакој колони налази $\varphi(m)$ бројева узајамно простих са m. Дакле, бројева узајамно простих и са m и са n, односно узајамно простих са mn, има $\varphi(m)\varphi(n)$. Тиме смо доказали $\varphi(mn)=\varphi(m)\varphi(n)$. ■

Претходна теорема нам омогућава да лако одредимо вредност функције $\varphi(n)$ за произвољан природан број n. За сваки број n важи следеће:

Теорема 7. Ако је $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$, онда је

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

Доказ. Из претходне теореме добијамо

$$\varphi(n)=\varphi(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k})=\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k})=(p_1^{\alpha_1}-p_1^{\alpha_1-1})(p_2^{\alpha_2}-p_2^{\alpha_2-1})\cdots(p_k^{\alpha_k}-p_k^{\alpha_k-1})$$

$$=p_1^{\alpha_1}(1-\frac{1}{p_1})p_2^{\alpha_2}(1-\frac{1}{p_2})\cdots p_k^{\alpha_k}(1-\frac{1}{p_k})=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right),$$

што је и требало доказати. ■

На пример, $\varphi(792)=\varphi(2^3\cdot 3^2\cdot 11)=2^3\cdot 3^2\cdot 11\cdot\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{10}{11}=240.$

Дошло је време да докажемо две вероватно најпознатије теореме у теорији бројева.

Теорема 8. (Ојлерова теорема) Ако је $(a,m)=1$, тада важи

$$a^{\varphi(m)}\equiv 1 \pmod m.$$

Доказ. Посматрајмо сведени систем остатака по модулу m, нека је то скуп $\{\alpha_1,\alpha_2,...,\alpha_{\varphi(m)}\}$. Како је $(a,m)=1$, по теореми 4 је скуп $\{a\alpha_1,a\alpha_2,...,a\alpha_{\varphi(m)}\}$ такође сведен систем остатака по модулу m, што значи да за сваки број α_i постоји тачно један број $a\alpha_j$ за који је $\alpha_i\equiv a\alpha_j \pmod m$. Множећи све ове конгруенције добијамо

$$\alpha_1\alpha_2...\alpha_{\varphi(m)}\cdot a^{\varphi(m)}\equiv\alpha_1\alpha_2...\alpha_{\varphi(m)} \pmod m.$$

Но, како је у питању сведен систем остатака, сви бројеви α_i су узајамно прости са m, па их можемо скратити:

$$a^{\varphi(m)} \equiv 1 \pmod{m},$$

што је и требало доказати. ■

Теорема 9. („Мала“ Фермаова Теорема) Ако је p прост број и p не дели a, онда је

$$a^{p-1} \equiv 1 \pmod{p}$$

. *Доказ.* Пошто p не дели a, онда је $(a, p) = 1$, и $\varphi(p) = p - 1$, па је ово само специјалан случај Ојлерове теореме. ■

Последица. За сваки прост број p и цео број a важи $a^p \equiv a \pmod{p}$. ■

Пример 3. Доказати да је $n^7 - n$ дељиво са 42 за сваки природан број n.
Решење. Очигледно је $n^7 \equiv n \pmod{2}$. На основу последице важи $n^7 \equiv n \cdot n^6 \equiv n \cdot n^2 \equiv n^3 \equiv n \pmod{3}$ и $n^7 \equiv n \pmod{7}$, па како је $[2, 3, 7] = 42$ добијамо $n^7 \equiv n \pmod{42}$. □

Пример 4. Ако је p прост број већи од 3, доказати да $6p \mid ab^p - a^p b$.
Решење. На основу последице је $ab^p \equiv ab \equiv a^p b \pmod{p}$. Бројеви ab^p и $a^p b$ су исте парности, па $2 \mid ab^p - a^p b$. Ако $3 \mid a$ или $3 \mid b$, онда $3 \mid ab^p - a^p b$, у супротном, како је $p > 3$, то је $p = 2k + 1$ непаран број, но онда имамо $ab^p \equiv 1^k \cdot ab^p \equiv (a^2)^k \cdot a \cdot b^{2k} \cdot b \equiv a^{2k+1} b \equiv a^p b \pmod{3}$, и како је $(p, 6) = 1$, то $6p \mid ab^p - a^p b$. □

До сада разрађивана теорија нам је потребна као предзнање за тему овог рада, у коју смо сада спремни да уронимо. Стекли смо довољно знања из теорије бројева да покренемо причу о **квадратним остацима**.

5 Квадратне конгруенције, квадратни остаци

Дефиниција 1. За дате целе бројеве a и $m > 1$, $(a, m) = 1$ кажемо да је a **квадратни остатак** по модулу m ако конгруенција $x^2 \equiv a \pmod{m}$ има решења у скупу целих бројева. Ако ова конгруенција нема решења, кажемо да је a **квадратни неостатак**.

Ако је x решење једначине $x^2 \equiv a \pmod{m}$, онда је и сваки број облика $x + km$ решење исте једначине. Многа занимљива својства можемо открити ако се фокусирамо само на решења у скупу $\{0, 1, ..., m - 1\}$.

На пример, нека је $m = 10$. Све квадратне остатке ћемо наћи тако што израчунамо вредности b^2 по модулу m за $0 \leq b < m$. Директно добијамо $0^2 \equiv 0, 1^2 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 9, 4^2 \equiv 6, 5^2 \equiv 5, 6^2 \equiv 6, 7^2 \equiv 9, 8^2 \equiv 4, 9^2 \equiv 1 \pmod{10}$. Дакле, квадратни остаци по модулу 10 су 1,4,5,6,9 (нула није квадратни остатак нити неостатак ни по једном модулу, иако конгруенција $x^2 \equiv 0 \pmod{m}$ увек има решења). Закључујемо да се квадрати целих бројева могу завршавати само цифрама 0,1,4,5,6,9. Квадратни неостаци су 2,3,7,8 и то не могу бити последње цифре потпуних квадрата.

За сада ћемо пажњу посветити квадратним остацима по простим модулима.

Теорема 1. За дати непаран прост број p и цео број a, $p \nmid a$, једначина $x^2 \equiv a \pmod{p}$ има или нула или два решења.

Доказ. Претпоставимо да дата конгруенција има решења и нека је x_1 једно њено решење. Тада је и $x_2 = -x_1$ такође решење. Очигледно је $x_2 \not\equiv x_1$, јер је p непаран и $(a, p) = 1$. За било које друго решење x важи $x^2 \equiv a \equiv x_1^2 \pmod{p}$, па $p \mid x_1^2 - x^2 \Rightarrow x \equiv \pm x_1 \pmod{p}$. ■

Теорема 2. За сваки непаран прост број p међу бројевима 1,2,...,$p-1$ има тачно $\dfrac{p-1}{2}$ квадратних остатака, и исто толико неостатака.
Доказ. Претпоставимо да постоји k квадратних остатака по модулу p. За сваки од тих остатака постоје 2 решења у скупу $\{1, 2, ..., p-1\}$, и сва су она међусобно различита, па је $2k \leq p-1$. Међутим, бројеви $1^2, 2^2, ..., \left(\dfrac{p-1}{2}\right)^2$ су различити квадратни остаци и има их $\dfrac{p-1}{2}$, па је k управо једнако $\dfrac{p-1}{2}$. ■

Пример 1. Доказати да конгруенција $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ има решења за сваки прост број p.
Решење. Тврђење очигледно важи за $p = 2$. Ако је p непаран прост број, онда x^2 може имати $\dfrac{p+1}{2}$ вредности (0 и $\dfrac{p-1}{2}$ квадратних остатака). Слично, $-1-y^2$ може имати $\dfrac{p+1}{2}$ вредности, па по Дирихлеовом принципу постоје цели бројеви x, y за које је $x^2 \equiv -1 - y^2 \pmod{p}$, што је и требало доказати. □

Дефиниција 2. За дати прост број p и цео број a, **Лежандров симбол** $\left(\frac{a}{p}\right)$ се дефинише као

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ако } p \nmid a \text{ и } a \text{ је квадратни остатак} \pmod{p} \\ -1, & \text{ако } p \nmid a \text{ и } a \text{ је квадратни неостатак} \pmod{p} \\ 0, & \text{ако } p \mid a. \end{cases}$$

Јасно је да је $\left(\frac{x^2}{p}\right) = 1$ за сваки прост број p и цео број x, $p \nmid x$.
Пошто је $3^2 \equiv -1 \pmod{5}$, а $x^2 \not\equiv 3 \pmod{5}$ за сваки цео број x, то је $\left(\frac{-1}{5}\right) = 1$ и $\left(\frac{3}{5}\right) = -1$.

У теореми 9 прошле главе (*Фермаова теорема*) смо доказали да за прост број p и цео број a узајамно прост са њим важи $a^{p-1} \equiv 1 \pmod{p}$. Број $p-1$ је паран, па уводимо ознаку $p' = \frac{p-1}{2}$. Тада је $(a^{p'})^2 \equiv 1 \pmod{p}$, тј. $p \mid (a^{p'})^2 - 1 = (a^{p'} - 1)(a^{p'} + 1)$. Како је p прост, можемо закључити да $p \mid a^{p'} \pm 1$. Да ли је у питању плус или минус, открива нам следећа теорема.

Теорема 3. (Ојлеров критеријум) $a^{p'} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Доказ. Ако $p \mid a$, тврђење важи. Претпоставимо да је a квадратни неостатак. Треба показати $a^{p'} \equiv -1 \pmod{p}$. Нека је $\mathbf{S} = \{1, 2, ..., p-1\}$ сведен систем остатака по модулу p. Нека је $x \in \mathbf{S}$ произвољно, тада је и $\{xy \mid y \in \mathbf{S}\}$ сведен систем остатака, па постоји тачно једно $y \in \mathbf{S}$ за које је $xy \equiv a \pmod{p}$ (и за то y је x јединствено). Штавише, a је квадратни неостатак по модулу p, па је $x \neq y$. Тиме је скуп $\mathbf{S}$ подељен на p' парова који у производу дају a. Множењем свих ових парова добијамо $(p-1)! \equiv a^{p'} \pmod{p}$. Убацивањем $a = 1$ добијамо познату **Вилсонову теорему**, која каже да је $(p-1)! \equiv -1 \pmod{p}$, па је $a^{p'} \equiv -1 \pmod{p}$. Ако је a квадратни остатак, у скупу $\mathbf{S}$ ће остати неупарени бројеви r и $p-r$ за које важи $r^2 \equiv a \pmod{p}$, и они у производу дају $-a$. Поново помножино све парове и добијамо $(p-1)! \equiv -a^{p'} \pmod{p}$, тј. $a^{p'} \equiv 1 \pmod{p}$. ■

Користећи Ојлеров критеријум се лако доказују нека веома важна својства Лежандровог симбола - наведимо их неколико.

Теорема 4. Лежандров симбол је мултипликативан, тј. за све целе бројеве a,b и непаран прост број p важи $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Доказ. $\left(\frac{ab}{p}\right) \equiv (ab)^{p'} \equiv a^{p'}b^{p'} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, па је очигледно $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. ■

Теорема 5. Важи $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, тј. конгруенција $x^2 \equiv -1 \pmod p$ има решења ако и само ако је $p = 2$ или $p = 4k+1, \quad k \in \mathbf{N}$. ■

Пример 2. Нека су x, y узајамно прости природни бројеви. Тада је сваки прост делилац броја $x^2 + y^2$ или једнак 2, или облика $4k+1, \quad k \in \mathbf{N}$.

Доказ. Нека је p непаран прост делилац броја x^2+y^2. Тада је $x^2 \equiv -y^2 \pmod p$, тј. $1 = \left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{y^2}{p}\right) = (-1)^{p'}$, па је $p \equiv 1 \pmod 4$. □

Дакле, да би се број могао представити као збир квадрата два узајамно проста природна броја, потребно је да му је сваки прост делилац 2 или облика $4k+1$. Овај услов је и довољан, што је први исказао Ферма око 1660. године, а доказао Ојлер 1755. године.

Следеће тврђење се често користи у задацима, а можемо га схватити као проширење примера 2.

Теорема 6. Нека су x, y узајамно прости цели бројеви, и a, b, c произвољни цели бројеви. Ако је p непаран прост делилац броја $ax^2 + bxy + cy^2$ који не дели ниједан од коефицијената a, b, c, тада је $D = b^2 - 4ac$ квадратни остатак по модулу p.

Доказ. Нека је $N = ax^2+bxy+cy^2$. Како је $4aN = (2ax+by)^2-Dy^2$, имамо да је $(2ax+by)^2 \equiv Dy^2 \pmod p$. Даље, p не дели y, јер би у супротном p делило $2ax + by$, па и x, контрадикција. Како је $(y, p) = 1$, постоји y_1 за које је $yy_1 \equiv 1 \pmod p$. Множењем добијене једнакости са y_1^2 добијамо $(2axy_1 + byy_1)^2 \equiv D \pmod p$, што је и требало доказати. ■

За непаран прост број p, најчешће узимамо скуп $\{1, ..., p-1\}$ као сведен систем остатака по модулу p. Посматрајмо сада скуп $S = \{1, 2, ..., \frac{p-1}{2}\}$ и сведен систем остатака $\{\pm s : s \in S\}$. Тада је и $\{\pm as : s \in S\}$ сведен систем остатака за цео број $a, p \nmid a$. За свако $s \in S$ постоји јединствено $s' \in S$ за које је $as \equiv \pm s' \pmod p$. Јасно је да овакав број s' постоји, а лако се доказује и да је он јединствен. Претпоставимо да постоје два различита броја s', s'' за које важи $as \equiv \pm s', as \equiv \pm s'' \pmod p$. Тада би морало да важи $s' \equiv -s'' \pmod p$, али ово је немогуће јер је $0 < s' + s'' < p$, па бројеви s' формирају пермутацију скупа S за $s = 1, 2, ..., \frac{p-1}{2}$. Нека је $as \equiv \varepsilon_s s' \pmod p$, где је $\varepsilon_s = \pm 1$. Множећи ове конгруенције добијамо $a^{\frac{p-1}{2}} \cdot (\frac{p-1}{2})! \equiv (\frac{p-1}{2})! \cdot \varepsilon_1\varepsilon_2...\varepsilon_{p'} \pmod p$. Како из Ојлеровог критеријума важи $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$, добијамо следеће тврђење:

Теорема 7. Важи $\left(\frac{a}{p}\right) = \varepsilon_1\varepsilon_2...\varepsilon_{p'}$.■

Теорема 8. (*Гаусова лема*) Важи $\left(\frac{a}{p}\right) = (-1)^S$, где је $S = \sum_{k=1}^{p'} \left\lfloor \frac{2ka}{p} \right\rfloor$.

Доказ. Приметимо да је $\varepsilon_k = -1$ ако и само ако број ak при дељењу са p даје остатак већи од p', тј. ако и само ако је $ka = pq + r, \frac{p-1}{2} < r < p$, што је еквивалентно са

$$ka = p\lfloor \frac{ka}{p} \rfloor + r, \quad \frac{p+1}{2} \leq r < p.$$

Множењем са 2 и дељењем са p добијамо

$$\frac{2ka}{p} = 2\lfloor\frac{ka}{p}\rfloor + \frac{2r}{p}.$$

Но, како је $1 + \frac{1}{p} \leq \frac{2r}{p} < 2$, претходна једнакост је еквивалентна са

$$\lfloor\frac{2ka}{p}\rfloor = 2\lfloor\frac{ka}{p}\rfloor + 1.$$

Слично добијамо да је $\varepsilon_k = 1$ ако и само ако је $\lfloor\frac{2ka}{p}\rfloor = 2\lfloor\frac{ka}{p}\rfloor$, па важи $\varepsilon_k = (-1)^{\lfloor\frac{2ka}{p}\rfloor}$. Применом теореме 7 добијамо тражену једнакост. ■

Применом Гаусове леме можемо да одредимо када је одређени број квадратни остатак по простом модулу p, тј. да за мало a или мало p одредимо вредност Лежандровог симбола $\left(\frac{a}{p}\right)$. Узмимо да је, на пример, $a = 2$. Тада важи $\left(\frac{2}{p}\right) = (-1)^S$, где је $S = \sum_{k=1}^{p'} \lfloor\frac{4k}{p}\rfloor$. Чланови у суми за које је $k < \frac{p}{4} = \frac{p'}{2} + \frac{1}{4}$, тј. $k \leq \lfloor\frac{p'}{2}\rfloor$ су једнаки нули, док је осталих $p' - \lfloor\frac{p'}{2}\rfloor$ једнако 1. Према томе је $S = p' - \lfloor\frac{p'}{2}\rfloor$. Ако је $p = 8k \pm 1$, онда је $S = 2k$, ако је $p = 8k + 3$, онда је $S = 2k + 1$, ако је $p = 8k - 3$, онда је $S = 2k - 1$. Дакле, важи следеће тврђење

Теорема 9. Број 2 је квадратни остатак по модулу p ако и само ако је $p \equiv \pm 1 \pmod 8$. ■
На сличан начин се могу показати следећа тврђења.

Теорема 10.

1. -2 је квадратни остатак по модулу p акко је $p \equiv 1 \pmod 8$ или $p \equiv 3 \pmod 8$
2. -3 је квадратни остатак по модулу p акко је $p \equiv 1 \pmod 6$
3. 3 је квадратни остатак по модулу p акко је $p \equiv \pm 1 \pmod{12}$
4. 5 је квадратни остатак по модулу p акко је $p \equiv \pm 1 \pmod{10}$. ■

Пример 3. Израчунати $\left\lfloor\frac{1}{2003}\right\rfloor + \left\lfloor\frac{2}{2003}\right\rfloor + \left\lfloor\frac{2^2}{2003}\right\rfloor + ... + \left\lfloor\frac{2^{2001}}{2003}\right\rfloor$.

Решење. На основу Ојлеровог критеријума и теореме 9 имамо $2^{1001} \equiv \left(\frac{2}{2003}\right) \equiv -1 \pmod{2003}$. Дакле, $2003 \mid 2^i(2^{1001} + 1) = 2^{1001+i} + 2^i$, а како 2^i и 2^{1001+i} нису дељиви са 2003, закључујемо да је

$$\left\lfloor\frac{2^i}{2003}\right\rfloor + \left\lfloor\frac{2^{1001+i}}{2003}\right\rfloor = \frac{2^i + 2^{1001+i}}{2003} - 1$$

. Сабирањем ових једнакости за $i = 0, 1, ..., 1000$ добијамо да је тражена сума једнака

$$\frac{1 + 2 + 2^2 + ... + 2^{2001}}{2003} - 1001 = \frac{2^{2002} - 1}{2003} - 1001.$$

Сада следи једна чувена теорема, формулисана од стране Ојлера 1783. и Лежандра 1785. године, а коју је први строго доказао Гаус 1796. године. Ево дакле, Гаусове „златне теореме“ (лат. *Aureum Theorema*).

Теорема 11. (Гаусов закон реципроцитета) Нека су p и q различити прости бројеви. Тада важи

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p'q'},$$

односно

$$\left(\frac{q}{p}\right) = \begin{cases} -\left(\frac{p}{q}\right) & \text{ако је } p \equiv q \equiv 3 \pmod 4, \\ \left(\frac{p}{q}\right) & \text{ако је } p \equiv 1 \text{ или } q \equiv 1 \pmod 4. \end{cases}$$

Другим речима, ако је бар један од простих бројева p, q облика $4k+1$, тада је q квадратни остатак по модулу p ако и само ако је p квадратни остатак по модулу q. У супротном, ако су оба броја облика $4k+3$, тада тачно једна од конгруенција $x^2 \equiv q \pmod{p}$, $x^2 \equiv p \pmod{q}$ има решења.

Доказ. У равни $\mathbf{R}^2$ посматрајмо (отворен) правоугаоник

$$\mathcal{A}_{p,q} = \{(x,y) \mid 0 < x < \frac{p}{2}, 0 < y < \frac{q}{2}\}.$$

Скуп тачака са целобројним координатама које су садржане у $\mathcal{A}_{p,q}$ је управо

$$\mathcal{A}'_{p,q} = \{(x,y) \mid x, y \in \mathbf{N}, 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\},$$

па је $|\mathcal{A}'_{p,q}| = p'q'$. Даље, посматрајмо праву задату једначином $y = \frac{q}{p}x$, која садржи дијагоналу правоугаоника $\mathcal{A}_{p,q}$. Приметимо да се ниједна тачка скупа $\mathcal{A}'_{p,q}$ не налази на овој правој, јер би тада за неке природне бројеве x, y важило $py = qx$, што је немогуће због $0 < x < p$ и $0 < y < q$. Према томе, ова права дели скуп $\mathcal{A}'_{p,q}$ на два дела: на скуп тачака $\mathcal{B}$ које су „испод“ и скуп тачака $\mathcal{C}$ које су „изнад“ посматране праве. Тачка (x,y) припада скупу $\mathcal{B}$ ако и само ако је $1 \leq x \leq p'$ и $1 \leq y \leq \lfloor \frac{q}{p}x \rfloor$, па је $|\mathcal{B}| = \sum_{k=1}^{p'} \lfloor \frac{q}{p}k \rfloor$. Слично добијамо $|\mathcal{C}| = \sum_{k=1}^{q'} \lfloor \frac{p}{q}k \rfloor$. Даље, из Гаусове леме имамо

$$\left(\frac{2}{q}\right)\left(\frac{p}{q}\right) = \left(\frac{2p}{q}\right) = \left(\frac{2(p+q)}{q}\right) = \left(\frac{\frac{p+q}{2}}{q}\right) = (-1)^S,$$

где је

$$S = \sum_{k=1}^{q'} \lfloor \frac{(p+q)k}{q} \rfloor = \sum_{k=1}^{q'} \lfloor \frac{pk}{q} + k \rfloor = \sum_{k=1}^{q'} \lfloor \frac{pk}{q} \rfloor + \sum_{k=1}^{q'} k = |\mathcal{C}| + \frac{q^2-1}{8}.$$

Лако се проверава да је $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$, чиме добијамо $\left(\frac{p}{q}\right) = (-1)^{|\mathcal{C}|}$. Аналогно добијамо $\left(\frac{q}{p}\right) = (-1)^{|\mathcal{B}|}$, па множењем ових једнакости добијамо

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{|\mathcal{B}|+|\mathcal{C}|} = (-1)^{p'q'},$$

што је и требало доказати. ■

Ова теорема нам омогућава да нађемо вредност Лежандровог симбола произвољног целог броја по неком простом модулу, приближно брзином Еуклидовог алгоритма. На пример, желимо да проверимо да ли је 2193 квадратни остатак по модулу 4019. То радимо на следећи начин: $\left(\frac{2193}{4019}\right) = \left(\frac{3}{4019}\right)\left(\frac{17}{4019}\right)\left(\frac{43}{4019}\right)$. Даље, према закону реципроцитета је $\left(\frac{3}{4019}\right) = -\left(\frac{4019}{3}\right) = -\left(\frac{2}{3}\right) = 1$, $\left(\frac{17}{4019}\right) = \left(\frac{4019}{17}\right) = \left(\frac{7}{17}\right) = \left(\frac{17}{7}\right) = \left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{1}{3}\right) = -1$, $\left(\frac{43}{4019}\right) = -\left(\frac{4019}{43}\right) = -\left(\frac{20}{43}\right) = -\left(\frac{5}{43}\right) = -\left(\frac{43}{5}\right) = -\left(\frac{3}{5}\right) = 1$, па је $\left(\frac{2193}{4019}\right) = 1 \cdot (-1) \cdot 1 = -1$.

Пример 4. Доказати да је цео број a квадратни остатак по сваком простом модулу ако и само ако је a потпун квадрат.

Доказ. Претпоставимо да је a најмањи број по апсолутној вредности који није потпун квадрат, а јесте квадратни остатак по сваком простом модулу. Тада је $a = \varepsilon p_1 p_2 \cdots p_k$ за $\varepsilon = \pm 1$ и различите просте бројеве p_i (ако би постојао p_i такав да $p_i^\alpha \mid a, \alpha >= 2$, онда би и број $\frac{a}{p_i^2}$ испуњавао услове задатка, контрадикција са минималношћу броја a). Онда за сваки прост број p важи

$$\left(\frac{a}{p}\right) = \left(\frac{\varepsilon}{p}\right)\prod_{i=1}^{k}\left(\frac{p_i}{p}\right), \qquad \left(\frac{p_i}{p}\right) = (-1)^{p'_i p'}\left(\frac{p}{p_i}\right), \qquad p > 2, p_i > 2.$$

Ако је $a = 2$, одаберимо $p = 5$. У супротном, постоји непаран прост делилац броја a, нека је то p_k. Одаберимо прост број p такав да важи $p \equiv 1 \pmod 4, p \equiv 1 \pmod{p_i}$ за $i = 1, 2, ..., k-1$ и $p \equiv b \pmod{p_k}$, где је $\left(\frac{b}{p_k}\right) = -1$. Овакав прост број p постоји по Дирихлеовој теореми о простим бројевима у аритметичким прогресијама. Тада важи $\left(\frac{-1}{p}\right) = 1$, па свакако и $\left(\frac{\varepsilon}{p}\right) = 1$, као и $\left(\frac{p_i}{p}\right) = 1$ за $i = 1, 2, ..., k-1$. Према томе је $\left(\frac{a}{p}\right) = -1$, контрадикција. □

У многим задацима који се могу наћи на такмичењима је потребно одредити да ли је неки број квадратни остатак по неком сложеном модулу. У складу са тиме, уводимо нови симбол, као уопштење Лежандровог.

Дефиниција 3. Нека су дати цео број a и непаран цео број b, и нека је $b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ канонска факторизација броја b. **Јакобијев симбол** $\left(\frac{a}{b}\right)$ се дефинише као

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Приметимо да Јакобијев и Лежандров симбол имају исту ознаку - заиста, у случају да је b непаран прост број дефиниција се своди на дефиницију 2.

Јасно је да из $\left(\frac{a}{b}\right) = -1$ следи да је a квадратни неостатак по модулу b. Међутим, **обратно не важи**, што илуструје следећи пример.

$$\left(\frac{2}{9}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{3}\right) = (-1) \cdot (-1) = 1,$$

иако је 2 квадратни неостатак по модулу 9.
Да ли је неки број заправо квадратни остатак по сложеном модулу, говори нам следећа теорема.

Теорема 12. Нека је a цео и $b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ природан број. Тада је a квадратни остатак по модулу b ако и само ако је a квадратни остатак по модулу $p_i^{\alpha_i}$ за $i = 1, 2, ..., k$.
Доказ. Ако је a квадратни остатак по модулу b, онда је и квадратни остатак по модулу $p_i^{\alpha_i}, \quad i = 1, 2, ..., k$. Нека је $x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$. Тада по кинеској теореми о остацима постоји цео број x за који је $x_i \equiv x \pmod{p_i^{\alpha_i}}$. Но, тада је $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$, па је $x^2 \equiv a \pmod b$. ■

Теорема 13. За све целе бројеве a, b и непарне бројеве n, m важи

1. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$,
2. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$,
3. $\left(\frac{a+bn}{n}\right) = \left(\frac{a}{n}\right)$,
4. (*Закон реципроцитета*) Ако су m, n узајамно прости, онда је $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{n-1}{2}\frac{m-1}{2}}$,
5. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$,
6. $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Доказ.

1. Нека је $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Тада је $\left(\frac{ab}{n}\right) = \prod_{i=1}^{k} \left(\frac{ab}{p_i}\right)^{\alpha_i} = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{\alpha_i} \left(\frac{b}{p_i}\right)^{\alpha_i} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

2. Слично делу под 1.

3. $x^2 \equiv a \pmod{n} \iff x^2 \equiv a + bn \pmod{n}$.

4. Нека је $n = p_1 p_2 \cdots p_k$ и $m = q_1 q_2 \cdots q_l$, за просте бројеве $p_1, p_2, ..., p_k, q_1, q_2, ..., q_l$. Тада је $\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}(-1)^{p_i' q_j'} = (-1)^{|\mathcal{A}|}$, где је $\mathcal{A} = \{(p,q) : p \mid n, q \mid m \text{ и } p \equiv q \equiv 3 \pmod 4\} = \{p : p \mid n, p \equiv 3 \pmod 4\} \times \{q : q \mid m, q \equiv 3 \pmod 4\}$. Број елемената скупа $\mathcal{A}$ је непаран ако и само ако постоји непаран број p_i-ова и непаран број q_j-ова који дају остатак 3 при дељењу са 4, тј. ако и само ако је $n \equiv 3 \pmod 4$ и $m \equiv 3 \pmod 4$.

5. За непарне бројеве x и y је $(x-1)(y-1) \equiv 0 \pmod 4$, што је еквиваленто са $\frac{x+y-2}{2} \equiv \frac{xy-1}{2} \pmod 2$, тј. $(-1)^{\frac{x+y-2}{2}} = (-1)^{\frac{xy-1}{2}}$. Ако је $n = p_1 p_2 \cdots p_k$ за просте бројеве p_i, доказ вршимо индукцијом по k. За $k = 1$ се исказ своди на теорему 5. Нека тврђење важи за неки природан број $k \geq 2$. Тада је

$$\left(\frac{-1}{n}\right) = \left(\frac{-1}{p_1 p_2 \cdots p_{k-1}}\right)\left(\frac{-1}{p_k}\right) = (-1)^{\frac{p_1 p_2 \cdots p_{k-1}-1}{2}} \cdot (-1)^{\frac{p_k-1}{2}} = (-1)^{\frac{p_1 p_2 \cdots p_{k-1}+p_k-2}{2}} =$$

$$= (-1)^{\frac{p_1 p_2 \cdots p_{k-1} p_k - 1}{2}} = (-1)^{\frac{n-1}{2}}.$$

6. За непарне целе бројеве x, y је $\frac{x^2-1}{8} + \frac{y^2-1}{8} \equiv \frac{x^2 y^2 - 1}{8} \pmod 2$. На основу теореме 8 је $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, па тврђење доказујемо индукцијом, слично као у претходном. ■

Теорема 14. За целе бројеве a, b и непаран прост број $p \nmid a$ важи

$$\sum_{x=0}^{p-1}\left(\frac{ax+b}{p}\right) = 0.$$

Доказ. Бројеви $ax+b$ чине потпун систем остатака по модулу p за $x = 0, 1, ..., p-1$. Међу њима има $\frac{p-1}{2}$ квадратних остатака и исто толико неостатака, као и један члан дељив са p, па је ова сума једнака $\frac{p-1}{2} - \frac{p-1}{2} + 0 = 0$.■

Теорема 15. Нека су a, b дати цели бројеви и нека је p непаран прост број. Тада важи

$$\sum_{x=0}^{p-1}\left(\frac{(x-a)(x-b)}{p}\right) = \begin{cases} -1, & \text{ако је } a \not\equiv b \pmod p \\ p-1, & \text{ако је } a \equiv b \pmod p \end{cases}$$

Доказ. Ако је $a \equiv b$, тада је један члан у овој суми једнак 0 (управо онај за који је $x \equiv a \pmod p$), док су остали једнаки 1. Ако је $a \not\equiv b$, трансформишемо суму на следећи начин:

$$\sum_{x=0}^{p-1}\left(\frac{(x-a)(x-b)}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{(x-a)^2 + (x-a)(a-b)}{p}\right) = \sum_{x=-a}^{p-1-a}\left(\frac{x^2 + x(a-b)}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{x^2 + x(a-b)}{p}\right).$$

Први сабирак у овој суми је очигледно нула. За све остале вредности x постоји јединствено y из скупа $\{1, 2, ..., p-1\}$ за које важи $xy \equiv 1 \pmod p$. Користећи ову чињеницу добијамо

$$\sum_{x=1}^{p-1}\left(\frac{x^2 + x(a-b)}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{1 + y(a-b)}{p}\right) = \sum_{x=1}^{p-1}\left(\frac{1+x}{p}\right) = \sum_{x=0}^{p-1}\left(\frac{x+1}{p}\right) - \left(\frac{1}{p}\right) = -1,$$

јер бројеви $y(a-b)$ формирају сведен систем остатака по модулу p. Последња једнакост важи на основу претходне теореме. ■

Теорема 16. За прост број p постоји $\lceil \frac{p}{4} \rceil$ целих бројева $a \in \{0, 1, ..., p-1\}$ за које су a и $a+1$ квадратни остаци по модулу p.

Доказ. Приметимо да је за $a \neq 0, p-1$ израз $\frac{1}{4}(1+\left(\frac{a}{p}\right))(1+\left(\frac{a+1}{p}\right))$ једнак 1 ако су a и $a+1$ квадратни остаци по модулу p, а 0 у супротном. За $a=0$ су a и $a+1$ очигледно квадратни остаци по сваком модулу, док је за $a=p-1$ вредност израза $\frac{1}{2}(1+\left(\frac{-1}{p}\right))$ једнака 1 ако су a и $a+1$ квадратни остаци, а 0 у супротном. Према томе, израз

$$1+\frac{1}{2}(1+\left(\frac{-1}{p}\right))+\sum_{a=1}^{p-2}\frac{1}{4}(1+\left(\frac{a}{p}\right))(1+\left(\frac{a+1}{p}\right))$$

броји колико има остатака који задовољавају потребан услов. Како је $\frac{1}{4}(1+\left(\frac{a}{p}\right))(1+\left(\frac{a+1}{p}\right))$ једнако $\frac{1}{2}$ за $a=0$ и $\frac{1}{4}(1+\left(\frac{-1}{p}\right))$ за $a=p-1$, претходна сума је једнака изразу

$$\frac{1}{2}+\frac{1}{4}\left(1+\left(\frac{-1}{p}\right)\right)+\sum_{a=0}^{p-1}\frac{1}{4}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right)=\frac{3+(-1)^{\frac{p-1}{2}}}{4}+\frac{1}{4}\sum_{a=0}^{p-1}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right).$$

Одредимо вредност ове суме.

$$\sum_{a=0}^{p-1}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right)=\sum_{a=0}^{p-1}1+\left(\frac{a}{p}\right)+\left(\frac{a+1}{p}\right)+\left(\frac{a^2+a}{p}\right).$$

Збир јединица је p, док је збир чланова $\left(\frac{a}{p}\right)$ и $\left(\frac{a+1}{p}\right)$ једнак 0 по теореми 14. Збир чланова $\sum_{a=0}^{p-1}\left(\frac{a^2+a}{p}\right)$ је једнак -1 по претходној теореми. Дакле, наша циљана сума је

$$\frac{3+(-1)^{\frac{p-1}{2}}}{4}+\frac{1}{4}\sum_{a=0}^{p-1}\left(1+\left(\frac{a}{p}\right)\right)\left(1+\left(\frac{a+1}{p}\right)\right)=\frac{3+(-1)^{\frac{p-1}{2}}}{4}+\frac{1}{4}(p-1)=\frac{p+2+(-1)^{\frac{p-1}{2}}}{4}=\lceil\frac{p}{4}\rceil,$$

што је и требало доказати. ■

За цео број a дефинишимо $K(a)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+a)}{p}\right)$. Претпоставимо да $p \nmid a$. Лако се види да за сваки цео број t важи $K(at^2)=\sum_{x=0}^{p-1}\left(\frac{xt(x^2t^2+at^2}{p}\right)=\left(\frac{t}{p}\right)K(a)$. Према томе, $|K(a)|$ зависи само од тога да ли је a квадратни остатак по модулу p или није. Сада дајемо доказ тврђења да је сваки прост број $p \equiv 1 \pmod 4$ збир два квадрата.

Теорема 17. Нека су a и b редом квадратни остатак и неостатак по модулу простог броја p облика $4k+1$. Тада су $|K(a)|$ и $|K(b)|$ парни природни бројеви који задовољавају

$$(\frac{1}{2}|K(a)|)^2+(\frac{1}{2}|K(b)|)^2=p.$$

Доказ. На основу претходног разматрања је $p'(K(a)^2+K(b)^2)=\sum_{n=1}^{p-1}K(n)^2=\sum_{n=0}^{p-1}K(n)^2$, јер је $K(0)=0$. За свако n је $K(n)^2=\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy(x^2+n)(y^2+n)}{p}\right)$, одакле добијамо

$$\sum_{n=0}^{p-1}K(n)^2=\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right)\sum_{n=0}^{p-1}\left(\frac{(n+x^2)(n+y^2)}{p}\right).$$

На основу теореме 15 је $\sum_{n=0}^{p-1}\left(\frac{(n+x^2)(n+y^2)}{p}\right)$ једнако $p-1$ ако $x \equiv \pm y \pmod p$, а -1 у осталим случајевима. У складу с тиме добијамо

$$\sum_{n=0}^{p-1}K(n)^2=p(2p-2)-\sum_{x=0}^{p-1}\sum_{y=0}^{p-1}\left(\frac{xy}{p}\right)=p(2p-2)=4pp'.$$

Дакле, $K(a)^2 + K(b)^2 = 4p$. Како су 0,1 једини могући остаци потпуних квадрата по модулу 4, следи да су $K(a)$ и $K(b)$ парни, чиме је доказ завршен. ■

6 Примене, задаци са разних такмичења

Велики број задатака из теорије бројева се може решити управо техникама које смо научили у овом раду. Сада ћемо урадити неколико тежих задатака користећи се знањем квадратних остатака.

Задатак 1. (САД изборно такмичење за ММО 2014, задатак 2) Нека је $a_1, a_2, a_3, ...$ низ целих бројева са особином да је аритметичка средина произвољног броја узастопних a_i-ова потпун квадрат. Прецизније, за свака два природна броја n и k, вредност израза

$$\frac{a_n + a_{n+1} + ... + a_{n+k-1}}{k}$$

је квадрат целог броја. Доказати да је низ (a_n) константан.
Решење. Претпоставимо да овај низ није константан. Тада је $a_n \neq 1$ за неко $n \in \mathbf{N}$. Нека је, не умањујући општост, $n = 1$. Како $p \mid a_i + a_{i+1} + ... + a_{i+p-1}$ за свако $i \in \mathbf{N}$, добијамо $p \mid a_j \Rightarrow p \mid a_{j\pm p}$ за свако $j \in \mathbf{N}$. Нека је $k \leq p-1$ најмањи квадратни неостатак по модулу p. Како су оба броја потпуни квадрати, важи

$$\left(\frac{k(a_1 + a_2 + ... + a_k)}{p}\right) = \left(\frac{(k-1)(a_2 + a_3 + ... + a_k)}{p}\right) \Rightarrow \left(\frac{k-1}{p}\right) = \left(\frac{k}{p}\right),$$

контрадикција, осим ако $p \mid a_2 + a_3 + ... + a_k$. Даље важи

$$\left(\frac{a_{k+1}}{p}\right) = 1 = \left(\frac{k(a_2 + a_3 + ... + a_{k+1})}{p}\right) \Rightarrow \left(\frac{k}{p}\right) = 1,$$

опет контрадикција, осим ако $p \mid a_{k+1}$. Сличним резоновањем добијамо $p \mid a_j \Rightarrow p \mid a_{j+k}$ за свако $j \in \mathbf{N}$. Но, како је $(k, p) = 1$, за сваки природан број n постоје цели бројеви α, β за које је $n = \alpha k + \beta p$, тј. можемо добити $p \mid a_n$ за сваки природан број n. Како је сваки члан низа потпун квадрат, важи $p^2 \mid a_n$. Поделимо све чланове низа са p^2, и поновимо поступак на новом низу, чиме добијамо да сви a_i имају исту канонску факторизацију. □

Задатак 2. (*Baltic way* 2017, задатак 20) Нека је S скуп свих уређених парова целих бројева $(a, b), \quad 0 < 2a < 2b < 2017$ за које $2017 \mid a^2 + b^2$. Доказати

$$\sum_{(a,b)\in S} a = \frac{1}{2} \sum_{(a,b)\in S} b.$$

Решење. Нека је $p = 2017$ и $a \in \{1, 2, ..., \frac{p-1}{2}\}$. Тада постоји јединствено $b \in \{1, 2, ..., \frac{p-1}{2}\}$ тако да $2017 \mid a^2 + b^2$. Заиста, 2017 је прост број облика $4k + 1$, па постоји k за које је $k^2 \equiv -1 \pmod{2017}$. Одаберимо $b \in \{1, 2, ..., \frac{p-1}{2}\}, b \equiv \pm ka \pmod{2017}$ и $0 < b < \frac{p-1}{2}$. Тада је $a^2 + b^2 \equiv 0 \pmod{2017}$. Претпоставимо да постоје два таква броја, b_1 и b_2. Тада је $b_1^2 \equiv b_2^2 \pmod{2017}$, па

$2017 \mid (b_1 - b_2)(b_1 + b_2)$. Како је $0 < b_1 + b_2 < 2017$, мора да важи $2017 \mid b_1 - b_2$, што повлачи $b_1 = b_2$. Тиме је доказана и јединственост оваквог b. Даље, нека је

$$S_a = \{a : (\exists b)(a, b) \in S\}.$$

Докажимо да је $a \to b - a$ бијекција скупа S_a у самог себе. Приметимо да је

$$(b - a)^2 + (b + a)^2 = 2(a^2 + b^2) \equiv 0 \pmod{2017}.$$

Ако је $a + b \leq \frac{p-1}{2}$, онда је јасно да $b - a \in S_a$. У супротном је $0 < 2017 - a - b \leq \frac{p-1}{2}$, па из $(a + b)^2 \equiv (2017 - a - b)^2 \pmod{2017}$ следи $b - a \in S_a$. Претпоставимо да постоје цели бројеви a_1, a_2, b_1, b_2 за које $(a_1, b_1), (a_2, b_2) \in S$ и $b_1 - a_1 = b_2 - a_2$. Тада је $b_1^2 - 2a_1b_1 + a_1^2 = b_2^2 - 2a_2b_2 + a_2^2$, што повлачи $a_1b_1 \equiv a_2b_2 \pmod{2017}$. Квадрирањем и коришћењем чињенице $b_1^2 \equiv -a_1^2, b_2^2 \equiv -a_2^2 \pmod{2017}$ добијамо $a_1^4 \equiv a_2^4 \pmod{2017}$, тј. $a_1^2 \equiv \pm a_2^2 \pmod{2017}$. Ако је $a_1^2 \equiv -a_2^2 \pmod{2017}$, онда из јединствености бројева b_1, b_2 добијамо $a_2 = b_1$ и $a_1 = b_2$ и важи $a_1 < b_1 = a_2 < b_2 = a_1$, контрадикција. Зато је $a_1^2 \equiv a_2^2 \pmod{2017}$, онда $2017 \mid a_1^2 - a_2^2$, па је $a_1 = a_2$. Дакле, функција $a \to b - a$ је инјективна. Како она пресликава коначан скуп у самог себе, она је и бијективна. Коначно, добијамо

$$\sum_{(a,b)\in S} a = \sum_{(a,b)\in S} b - a,$$

што је и требало доказати. □

Задатак 3. (ММО шортлиста 2020 $N2$**)** За сваки прост број p постоји царство p-изантија, које се састоји од p острва са ознакама $1, 2, ..., p$. Мост повезује острва m и n ако и само ако $p \mid (n^2 - m + 1)(m^2 - n + 1)$. Доказати да за бесконачно много простих бројева p постоје два острва p-изантије која нису повезана ниједним низом мостова.

Решење. Доказаћемо да за бесконачно много простих бројева у p-изантији постоје два острва која су повезана само једно са другим. Мост повезује m и n ако и само ако је $n \equiv m^2 + 1$ или $m \equiv n^2 + 1 \pmod{p}$. Ако је $m^2 + 1 \equiv n \pmod{p}$, нацртајмо стрелицу од m ка n. Јасно је да од m креће једна стрелица уколико је $m^2 + 1 \not\equiv m \pmod{p}$, и нула стрелица у супротном.

Претпоставимо да је природан број a решење конгруенције $x^2 - x + 1 \equiv 0 \pmod{p}$. Лако се види да је и $b = p + 1 - a$ решење ове конгруенције, као и да је $b \neq a$ за $p > 3$. Даље је $ab \equiv a(1 - a) \equiv a - a^2 \equiv 1 \pmod{p}$. Ако стрелица иде од t према a, онда је t решење конгруенције $t^2 + 1 \equiv a \equiv a^2 + 1 \pmod{p}$ - једино такво $t \neq a$ је $t = p - a$. Слично, једина стрелица која иде према b је $p - b$. Ако једно од острва $p - a$, $p - b$ није на крају ниједне стрелице, рецимо $p - a$, онда је пар $a, p - a$ изолован од осталих острва. Ово је тачно уколико једна од конгруенција $x^2 + 1 \equiv -a, x^2 + 1 \equiv -b$ нема решења, тј. ако је један од бројева $-a - 1$ или $-b - 1$ квадратни неостатак по модулу p.

Приметимо да је $x^2 - x + 1 \equiv x^2 - (a + b)x + ab \equiv (x - a)(x - b) \pmod{p}$. Убацивањем $x = -1$ добијамо $(-1 - a)(-1 - b) \equiv 3 \pmod{p}$. Ако је 3 квадратни неостатак по модулу p, онда је и један од бројева $-1 - a, -1 - b$. Дакле, треба показати да постоји бесконачно простих бројева $p > 3$ за које је 3 квадратни неостатак по модулу p и $x^2 - x + 1 \equiv 0 \pmod{p}$ за неко целобројно x. Ако је $x^2 - x + 1 \equiv 0 \pmod{p} \iff 4x^2 - 4x + 4 \equiv 0 \pmod{p}$, тј. $(2x - 1)^2 \equiv -3 \pmod{p}$, па овакво x постоји ако и само ако је -3 квадратни остатак по модулу p. По теореми 10.2 следи да је $p \equiv 1 \pmod{6}$. По теореми 10.3 је 3 квадратни остатак по модулу p ако и само ако је $p \equiv \pm 1 \pmod{12}$. Према томе, за све просте бројеве облика $12k + 7$, којих има бесконачно по Дирихлеовој теореми о простим бројевима у аритметичким прогресијама, је -3 квадратни остатак, а 3 квадратни неостатак. Тиме је доказ завршен. □

Задатак 4. (СМО 2007.3) Одредити све парове природних бројева (x, n) који су решења једначине $x^3 + 2x + 1 = 2^n$.

Решење. Провером добијамо да за $n \leq 2$ једино решење пар $(1, 2)$. Докажимо да за $n \geq 3$ нема решења.

Нека је (x,n) решење задатка и $n \geq 3$. Број x мора бити непаран, па је $x^2+2 \equiv 3 \pmod 8$. Сада из $x(x^2+2) \equiv -1 \pmod 8$ следи да је $x \equiv 5 \pmod 8$. Шта више, како $3 \mid x(x^2+2)$ (уколико $3 \nmid x$ тада $3 \mid x^2+2$), мора бити $2^n \equiv 1 \pmod 3$, па је n паран број. Важи $2^n+2 = x^3+2x+3 = (x+1)(x^2-x+3)$. Како је n паран број, 2^n је потпун квадрат, па је број -2 квадратни остатак по сваком непарном простом делиоцу p броја $(x+1)(x^2-x+3)$. Зато је

$$1 = \left(\frac{-2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right) = (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{(p-1)(p+5)}{8}},$$

одакле следи да је p облика $8k+1$ или $8k+3$. Производ бројева тог облика је такође облика $8s+1$ или $8s+3$. Међутим, из $x \equiv 5 \pmod 8$ следи да је $x^2-x+3 \equiv 7 \pmod 8$, контрадикција. Дакле, једино решење је $(x,n) = (1,2)$. □

Задатак 5. Доказати да $4kxy-1$ није делилац броја x^m+y^n ни за које природне бројеве x,y,k,m,n.

Решење. Приметимо да су бројеви $4kxy-1, x^m, y^n$ узајамно прости у паровима. Означимо $m' = \lfloor \frac{m}{2} \rfloor$ и $n' = \lfloor \frac{n}{2} \rfloor$. Разматрамо следеће случајеве:

1° $m = 2m'$ и $n = 2n'$. Тада $4kxy-1 \mid (x^{m'})^2 + (y^{n'})^2$, што је немогуце јер је $4kxy-1 \equiv 3 \pmod 4$.

2° $m = 2m'$ и $n = 2n'+1$ (случај $m = 2m'+1$ и $n = 2n'$ је аналоган). Тада $4kxy \mid (x^{m'})^2 + y(y^{n'})^2$, па је по теореми 6 $\left(\frac{-y}{4kxy-1}\right) = 1$. Тврдимо да је то немогуће. Претпоставимо да је y непарно. По закону реципроцитета је $\left(\frac{-y}{4kxy-1}\right) = \left(\frac{-1}{4kxy-1}\right)\left(\frac{y}{4kxy-1}\right) = (-1)\cdot(-1)^{\frac{y-1}{2}}\left(\frac{-1}{y}\right) = -1$, контрадикција. Претпоставимо да је $y = 2^t z$, где су t,z природни бројеви и z је непарно. По теореми 13.6 је $\left(\frac{2}{4kxy-1}\right) = 1$, док је, као у претходном случају, $\left(\frac{-z}{4kxy-1}\right) = \left(\frac{-z}{4(2^t k)xz-1}\right) = -1$. Према томе, $\left(\frac{-y}{4kxy-1}\right) = 1^t \cdot (-1) = -1$.

3° Нека је $m = 2m'+1$ и $n = 2n'+1$. Тада $4kxy-1 \mid x(x^{m'})^2 + y(y^{n'})^2$, па је $\left(\frac{-xy}{4kxy-1}\right) = 1$. Међутим, $\left(\frac{-xy}{4kxy-1}\right) = \left(\frac{-4k^2xy}{4kxy-1}\right) = \left(\frac{-k}{4kxy-1}\right) = -1$, где је последња једнакост доказана у претходном случају. Тиме је доказ завршен. □

Задатак 6. (Румунско изборно такмичење 2004.18) Нека је p непаран прост број и $f(x)$ полином задат са

$$f(x) = a_{p-1}x^{p-2} + a_{p-2}x^{p-3} + \cdots + a_2 x + a1,$$

где је a_i Лежандров симбол $\left(\frac{i}{p}\right)$. Доказати да је

а) $f(x)$ дељив са $x-1$, али не и са $(x-1)^2$ ако и само ако је $p \equiv 3 \pmod 4$,

б) $f(x)$ дељив са $(x-1)^2$, али не и са $(x-1)^3$ ако је $p \equiv 5 \pmod 8$.

Решење.

а) $f(1) = \sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = 0$, па $x-1 \mid f(x)$. Важи $f'(1) = \sum_{k=1}^{p-1}(k-1)\left(\frac{k}{p}\right) = \sum_{k=1}^{p-1} k\left(\frac{k}{p}\right) = \sum_{k=1}^{p-1}(p-k)\left(\frac{p-k}{p}\right) = -(-1)^{\frac{p-1}{2}} f'(1)$. За $p = 4k+1$ је $f'(1) = -f'(1)$, па $(x-1)^2 \mid f(x)$, док за $p = 4k+3$ важи $f'(1) = \sum_{k=1}^{p-1} k\left(\frac{k}{p}\right) \equiv \sum_{k=1}^{p-1} k \equiv 1 \pmod 2$, па је $f'(1) \neq 0$, тј. $(x-1)^2 \nmid f(x)$.

б) Ако је $p \equiv 5 \pmod 8$, тада је $f(1) = f'(1) = 0$, на основу дела под а). Треба показати $\sum_{k=1}^{p-1}(k-1)(k-2)\left(\frac{k}{p}\right) \neq 0$. Ми ћемо показати да је ова сума конгруентна са 4 по модулу 8. Како је $\left(\frac{-1}{p}\right) = 1$, то важи $\left(\frac{k}{p}\right) = \left(\frac{p-k}{p}\right)$. Даље је $(k-2)(k-1)\left(\frac{k}{p}\right) + (p-k-2)(p-k-1)\left(\frac{p-k}{p}\right) \equiv \left(\frac{k}{p}\right)((k-2)(k-1)+(3-k)(4-k)) \equiv \left(\frac{k}{p}\right)(2k^2-10k+14) \equiv \left(\frac{k}{p}\right)(2k^2-2k-2) \pmod 8$. Лако се

види да је $2k^2-2k-2\equiv -2 \pmod 8$ за $j\equiv 0,1 \pmod 4$ и $2k^2-2k-2\equiv 2 \pmod 8$ за $j\equiv 2,3 \pmod 4$. Дакле, $f''(1)\equiv 2(-\left(\frac{1}{p}\right)+\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)-\left(\frac{4}{p}\right)+\cdots+\left(\frac{4k-1}{p}\right)-\left(\frac{4k}{p}\right)-\left(\frac{4k+1}{p}\right)+\left(\frac{4k+2}{p}\right)) \pmod 8$, где је $p=8k+5$. Знамо да је $\sum_{k=1}^{p-1}\left(\frac{k}{p}\right)=0$, а како за прост број $p\equiv 1 \pmod 4$ важи и $\left(\frac{k}{p}\right)=\left(\frac{p-k}{p}\right)$, то је малопре споменута сума једнака $2\sum k=1\frac{p-1}{2}\left(\frac{k}{p}\right)=0$. Сабирањем ове суме и претходног израза за $f''(1)$ добијамо $f''(1)=4(\left(\frac{2}{p}\right)+\left(\frac{3}{p}\right)+\left(\frac{6}{p}\right)+\left(\frac{7}{p}\right)+\cdots+\left(\frac{4k-1}{p}\right)+\left(\frac{4k+2}{p}\right))$. Сабирака у загради има $2k+1$ и сваки је непаран, па је $f''(1)\equiv 4 \pmod 8$, што је и требало доказати. □

Задатак 7. Нека су m и n природни бројеви за које важи $\varphi(5^m-1)=5^n-1$. Тада је $(m,n)>1$. Доказати.
Решење. Претпоставимо да је $(m,n)=1$. Нека је $5^m-1=2^\alpha p_1^{\alpha_1}\cdots p_k^{\alpha_k}$ канонска факторизација броја 5^m-1. Тада је

$$5^n-1=\varphi(5^m-1)=2^{\alpha-1}p_1^{\alpha_1-1}\cdots p_k^{\alpha_k-1}(p_1-1)\cdots(p_k-1).$$

Очигледно $2^\alpha \mid 5^n-1$. С друге стране, $(5^m-1,5^n-1)=5^{(m,n)}-1=4$, што повлачи $\alpha_i=1$ за $i=1,2,...k$ и $\alpha=2$. Лако се види да $2^3 \mid 5^x-1$ за све парне x, закључујемо да је m непарно, тј. $m=2m'+1$ за неки природан број m'. Како $p_i \mid 5(5^{m'})^2-1$ за $i=1,...,k$, то је 5 квадратни остатак по сваком p_i, што по теореми 10 повлачи $p_i\equiv \pm 1 \pmod{10}$. Но, како $p_i-1 \mid 5^n-1$, мора бити $p_i\equiv -1 \pmod{10}$. Једнакост $5^m-1=4p_1p_2\cdots p_k$ по модулу 5 даје $-1\equiv(-1)^{k+1} \pmod 5$, па је k парно. С друге стране, једнакост $5^n-1=2(p_1-1)(p_2-1)\cdots(p_k-1)$ по модулу 5 даје $-1\equiv 2(-2)^k\equiv 2^{k+1}\equiv 4^{\frac{k}{2}}\cdot 2\equiv \pm 2 \pmod 5$, контрадикција. □

Задатак 8. (ММО 2008.3) Доказати да постоји бесконачно много природних бројева n таквих да n^2+1 има прост делилац већи од $2n+\sqrt{2n}$.
Решење. Нека је p прост број облика $8k+1$. Изаберимо $n=\frac{p-1}{2}-a=4k-a, 0\le a<4k$. Тада је $(\frac{p-1}{2}-a)^2+1\equiv 0 \pmod p$ еквивалентно са $16k^2-8ak+a^2+1\equiv 0 \pmod p$, што је даље еквивалентно са $-2k+a+a^2+1\equiv 0 \pmod p$, па је $a(a+1)\equiv 2k-1 \pmod p$. Број $a(a+1)$ је природан и паран, па је $a(a+1)\ge 10k$. Даље је $(a+1)^2>a(a+1)\ge 10k>p$, па је $n=\frac{p+1}{2}-(a+1)<\frac{p+1}{2}-\sqrt{p}<\frac{p+1}{2}-\sqrt{2n}$, па је $2n+\sqrt{2n}-1>p$, што је неједнакост мало јача од тражене. □

7 Закључак

У првом делу рада смо пошли од саме дефиниције дељивости и разрадили најбитнију теорију потребну за рад са квадратним остацима. На том путу смо доказали најпознатије теореме теорије бројева, као што су Еуклидов алгоритам, Ерастотеново сито, основни став аритметике, кинеска теорема о остацима, Ојлерова теорема и Мала Фермаова теорема, пре него што смо уопште дефинисали квадратни остатак.

Квадратни остаци представљају изузетно интересантан концепт у теорији бројева. Пошавши од дефиниције квадратног остатка доказали смо најпознатија тврђења везана за њих - научили смо основна својства Лежандровог и Јакобијевог симбола, како одредити да ли је неки број квадратни остатка по датом модулу преко Гаусове леме, као и разне друге теореме које нам помажу у изради задатака. Показали смо на неколико примера како се најтежи задаци са најтежих такмичења могу лако урадити уз помоћ квадратних остатака. Међутим, много тога је остало неспоменуто у овом раду, као на пример примена квадратних остатака у криптографији, или Лагранжова теорема о збиру четири квадрата, које би читалац који је савладао садржај овог рада могао у потпуности да разуме.

Желео бих пре свега да се захвалим мом ментору, Миљану Кнежевићу, на великој помоћи коју ми је пружио током израде овог матурског рада. Такође бих хтео да се захвалим свим професорима који су ми у било ком тренутку предавали математику и пробудили и одржавали моје интересовање према овој невероватној науци.

8 Литература

1. https://imomath.com/srb/dodatne/TBr_JBMO_vb.pdf
2. https://imomath.com/srb/dodatne/uvodkongr_mr.pdf
3. Анализа са алгебром 2, З. Каделбург, В. Мићић, С. Огњановић, Круг 2017.
4. Увод у теорију бројева, В. Мићић, З. Каделбург, Д. Ђукић, ДМС 2013.
5. https://jgcsr.org/wp-content/uploads/David_M._Burton_Elementary_Number_Theoryz-lib.org_.pdf
6. https://brilliant.org/wiki/quadratic-residues/
7. https://www.mit.edu/ shint/handouts/QuadraticResidues.pdf
8. https://cs.uwaterloo.ca/journals/JIS/VOL21/Pandey/pandey14.pdf
9. https://www.math.cmu.edu/ cargue/arml/archive/19-20/number-theory-at-11-24-19.pdf
10. https://math.gordon.edu/ntic/ntic.pdf
11. https://joshua.smcvt.edu/numbertheory/book.pdf
12. https://sites.millersville.edu/bikenaga/number-theory/quadratic-residues/quadratic-residues.pdf
13. https://artofproblemsolving.com/community/c6t385f6h568274_consecutive _averages_of_sequence_always_integer_squares
14. https://artofproblemsolving.com/community/c6h1543518p11999375
15. https://www.imo-official.org/problems/IMO2020SL.pdf