Универзитет у Београду

Математички факултет

МАСТЕР РАД

- из Методике наставе математике-

Квадратне конгруенције и проблемски задаци

Професор:
др Зоран Каделбург

Студент:
Милица Мисојчић

Београд, септембар 2019.

Садржај

1 Увод **1**

2 Примитивни корен **3**

3 Квадратни остаци и квадратни реципроцитет **7**

4 Задаци **13**

5 Литература **22**

1 Увод

Теорија бројева, коју је Гаус звао "Краљицом математике", је посебно подложна историјском схватању. Оснивачи теорије бројева били су Ферма, Ојлер, Лагранж, Лежандр и Гаус. Од отприлике 1630. године, када је Ферма почео да се бави теоријом бројева, све до Гаусове публикације *Disquisitiones Arithmeticae* 1801., сваки од ових математичара надграђивао је рад својих претходника и на тај начин значајно допринео развоју теорије бројева. Они су развили основе теорије бројева, формулисали и доказали многе од основних теорема и поставили многа питања на која и данас немамо одговор.

Адријен-Мари Лежандр (1752.-1833.) провео је свој живот у Француској као један од водећих математичара у Европи, али није био признат као Ојлер, Лагранж, Лаплас или Гаус, чији су се животи преклапали са његовим. Омиљене Лежандрове области биле су небеска механика, елиптични интеграли и теорија бројева. Његово име у вези је са многим појмовима укључујући Лежандрове полиноме, методу најмањег квадрата као и Лежандров симбол.

Многе Лежандрове резултате је независно од њега пронашао Гаус, што је довело до неколико озбиљних несугласница. Жан Итард у својој биографији о Лежандру каже:

"Гаус је сматрао да је теорема његова ако је он дао њен први строг доказ. Лежандр, који је био 25 година старији од Гауса, имао је много шире и слободније мишљење о строгости доказа. За Лежандра, закаснелог следбеника Ојлера, доказ је често био једва уверљив. Као последица, било каква дискусија између њих двојице представљала је дијалог глувих."

1798. Лежандр је објавио своју *Теорију бројева*, прву систематску књигу посвећену искључиво теорији бројева. Ова књига је имала јак утицај на математичаре тог времена и била је ревизирана неколико пута. Међутим, чак и у последњем издању (1830.), Лежандр није усвојио супериорне методе које је развио Гаус. У овом раду, дискутоваћемо само о неким његовим важим закључцима из теорије бројева.

Мала Фермаова теорема произилази из питања који прости бројеви деле бројеве облика $a^n - 1$. Ојлер је био изузетно заинтересован за слично питање који прости бројеви деле бројеве облика $a^n + 1$. Ово је довело до студије о квадратним остацима, што је довело до закона о квадратном реципроцитету.

Историја закона реципроцитета је заправо историја теорије бројева. Ојлеров начин проучавања овог закона је био следећи: квадратни карактер од a по модулу p зависи једино од класе остатака p по модулу $4a$. За Лежандра, који је и увео термин реципроцитет, закон реципроцитета је био исказан на следећи начин: непарни прост број p је квадратни остатак по модулу q, где је q неки други непаран прост број ако и само ако је q квадратни остатак по модулу p, осим када је $p \equiv q \equiv 3 \pmod 4$.

У домену изучавања квадратних конгруенција намеће се следеће питање: ако је a цео број, за које просте бројеве p конгруенција $x^2 \equiv a \pmod p$ има решења? Одговор нам даје квадратни закон реципроцитета. Овај закон је формулисан од стране Ојлера и Лежандра али Гаус је био први који је изнео комплетан доказ. Гаус је био веома поносан на свој резултат и назвао је теорему која говори о квадратном закону реципроцитета златном теоремом.

У овом раду изложене су основне формулације ове теорије за коју је најзаслужнији био Лежандр. Међу њима су у сваком појединачном доказу присутне леме и ставови који се морају имати у виду да би се доказ могао спровести смислено. Акценат рада је на теорији о примитивном корену, квадратним остацима и Гаусовом закону реципроцитета. Последње поглавље посвећено је њиховој примени у решавању проблемских задатака.

На крају уводног текста желим да се захвалим свом ментору др Зорану Каделбургу, редовном професору Математичког факултета у Београду, на неизмерној помоћи и начину на који ме је упућивао пре и за време писања овог рада.

2 Примитивни корен

Циљ овог рада је разумевање детаљне структуре решења квадратне конгруенције. Да бисмо дошли до одговора кренућемо од следећег задатка: потребно је пронаћи бројеве $t \in \mathbb{N}$ за које је $a^t \equiv 1 \pmod{m}$, и посебно најмањи такав број t.

Дефиниција 2.1. Најмањи од природних бројева t за које важи

$$a^t \equiv 1 \pmod{m}$$

назива се **поретком** броја a по модулу m и означава са $r_m(a)$.

На питање који бројеви имају поредак одговара:

Теорема 2.1. Поредак броја a по модулу m постоји ако и само ако су бројеви a и m узајамно прости.

Доказ. Ако је $a^t \equiv 1 \pmod{m}$ за неко t, онда је $a^t - mu = 1$, односно $a \cdot a^{t-1} - mu = 1$, па из теореме о Еуклидском дељењу целих бројева следи $(a, m) = 1$. Обратно, ако су a и m узајамно прости, онда из Ојлерове теореме следи да је $a^{\varphi(m)} = 1 \pmod{m}$, тј. постоји бар један природан број t за који је $a^t \equiv 1 \pmod{m}$. Најмањи од таквих бројева је тражени поредак.

Јасно је да сви бројеви који су међусобно конгруентни по модулу m (припадају истој класи еквиваленције) имају исти поредак по модулу m (ако га уопште имају). Међутим, могуће је да бројеви из разних класа имају једнаке поретке. Следеће једноставно својство олакшава налажење поретка.

Теорема 2.2. Ако је t поредак броја a по модулу m, тада је $a^s \equiv 1 \pmod{m}$, ако и само ако $t \mid s$. Специјално, $r_m(a) \mid \varphi(m)$.

Доказ. Нека је $a^s \equiv 1 \pmod{m}$. Ако би било $s = tq + r,\ 0 < r < t$, из $a^s = (a^t)^q a^r$ би следило $a^r \equiv 1 \pmod{m}$, што противречи минималности поретка t. Обратно, ако је $s = tq$, онда је $a^s = (a^t)^q \equiv 1 \pmod{m}$.

Пример. Лако се проверава да је $\varphi(22) = 10$. Зато поретци по модулу 22 бројева $3, 5, 7, 9, 13, 15, 17, 19, 21$ (који су узајамно прости са 22) могу бити само $1, 2, 5$ или 10. Тако на пример, поредак броја 3 једнак је 5, јер је $3^1, 3^2 \not\equiv 1 \pmod{22}$, $3^5 \equiv 1 \pmod{22}$, а поредак броја 7 је 10, јер је $7^1, 7^2, 7^5 \not\equiv 1 \pmod{22}$, а $7^{10} \equiv 1 \pmod{22}$.

Дефиниција 2.2. Ако је поредак броја g по модулу m једнак $\varphi(m)$, број g се назива **примитивним кореном** по модулу m.

Пример. Посматрајмо остатке $1, 2, 3, -3, -2, -1$ по модулу 7 ($\varphi(7) = 6$). Лако се проверава да су њихови поретци по модулу 7 једнаки, редом, $1, 3, 6, 3, 6, 2$. Бројеви 3 и -2 су примитивни корени по модулу 7.
По модулу 8, бројеви који имају поредак су $1, 3, 5$ и 7. Ниједан од њих, међутим, није примитивни корен, јер је поредак сваког од њих једнак 2, а $\varphi(8) = 4$.

Пример. 2 је примитивни корен по модулу 5, јер је $2, 2^2, 2^3, 2^4 \equiv 2, 4, 3, 1 \pmod 5$. 3 је примитивни корен по модулу 5, јер је $3, 3^2, 3^3, 3^4 \equiv 3, 4, 2, 1 \pmod 5$.

Ојлер је увео термин "примитивни корен"али доказ његовог постојања није био задовољавајући. Лежандр је дао први коректан доказ. Већина доказа ове теореме, која је заправо специјалан случај теореме да је било која коначна подгрупа мултипликативне групе у пољу циклична, користе Ојлерову φ функцију. Доказ изложен у овом раду је захваљујући Лежандру, директан и елегантан.

Ако је $a \in \mathbb{Z}$, нека $o(a)$ представља ред подгрупе генерисане класом остатка $\overline{a}$ у групи $(\mathbb{Z}/p\mathbb{Z})^\times$, односно $r_m(a)$ је најмањи позитиван цео број k такав да је $a^k \equiv 1 \pmod p$.

Теорема 2.3. Група $(\mathbb{Z}/p\mathbb{Z})^\times$ остатака класе еквиваленције по модулу p у односу на операцију множења је циклична. На језику конгруенција ово значи да за сваки прост број p постоји примитивни корен по модулу p, $g \in \mathbb{Z}$, такав да је сваки цео број $n \not\equiv 0 \pmod p$ конгруентан по модулу p тачно једном од целих бројева $g, g^2, g^3, \ldots, g^{p-1}$. Дакле, редослед бројева $g, g^2, g^3, \ldots, g^{p-1}$ може се преуредити тако да по модулу p буде конгруентан секвенци бројева $1, 2, \ldots, p-1$.

Доказ теореме следи из три тврђења:

i) Ако је $r_m(x) = ab$, онда је $r_m(x^a) = b$.

Доказ. Означимо $r_m(x^a) = \gamma$. Тада је $(x^a)^\gamma \equiv 1 \pmod m$, тј. $x^{a\gamma} \equiv 1 \pmod m$, па $r_m(x) = ab \mid a\gamma$, одакле следи $b \mid \gamma$. Обратно, из $x^{ab} \equiv 1 \pmod m$ следи $(x^a)^b \equiv 1 \pmod m$, одакле $r_m(x^a) = \gamma \mid b$. Значи, $\gamma = b$.

ii) Ако је $r_m(x) = a$, $r_m(y) = b$ и $(a, b) = 1$, тада је $r_m(xy) = ab$.

Доказ. Означимо $r_m(xy) = \gamma$. Тада је $(xy)^\gamma \equiv 1 \pmod{m}$, па и $x^{b\gamma}y^{b\gamma} \equiv 1 \pmod{m}$. Због $r_m(y) = b$ одавде следи да је $x^{b\gamma} \equiv 1 \pmod{m}$, а како је $r_m(x) = a$, и $a \mid b\gamma$. Из $(a, b) = 1$ следи и да $a \mid \gamma$. Слично се доказује и да $b \mid \gamma$, дакле $ab \mid \gamma$. С друге стране, из $x^a \equiv 1 \pmod{m}$ и $y^b \equiv 1 \pmod{m}$ следи $(xy)^{ab} \equiv 1 \pmod{m}$, па $\gamma = r_m(xy) \mid ab$. Значи, $\gamma = ab$.

iii) Нека је p прост број, $n \in \mathbb{N}$ и

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

полином са целобројним коефицијентима. Ако конгруенција

$$f(x) \equiv 0 \pmod{p} \tag{1}$$

има више од n решења (различитих по модулу p), онда $p \mid a_k$ за свако $k = 0, 1, \ldots, n$.

Доказ. Нека су $x_1, x_2, \ldots, x_{n+1}$ остаци по модулу p различитих решења конгруенције (1). Полином $f(x)$ се може представити у облику

$$\begin{aligned} f(x) = {} & b_n(x - x_1)(x - x_2)\cdots(x - x_{n-1})(x - x_n) \\ & + b_{n-1}(x - x_1)(x - x_2)\cdots(x - x_{n-1}) \\ & + \ldots \\ & + b_1(x - x_1) \\ & + b_0. \end{aligned}$$

Заиста, изаберимо најпре $b_n = a_n$. Затим бирамо коефицијент b_{n-1} тако да збир коефицијената уз x_{n-1} полинома на десној страни (уствари, полинома који се добија када се измноже заграде у прва два његова сабирка) буде једнак a_{n-1}. Настављајући овај поступак одређују се остали коефицијенти $b_{n-2}, \ldots, b_1, b_0$.
Замењујући у горњој релацији, редом, $x = x_1, x = x_2, \ldots, x = x_{n+1}$, закључујемо да $p \mid b_0, p \mid b_1, \ldots, p \mid b_n$, одакле непосредно следи да су и сви коефицијенти $a_n, a_{n-1}, \ldots, a_0$ полазног полинома дељиви са p, као суме бројева дељивих са p.

Докажимо сада теорему 2.3:

Доказ. За $p = 2$ тврђење је тривијално. Петпоставимо да је p непаран. Нека је

$$\{r_p(1), r_p(2), \ldots, r_p(p-1)\} = \{\gamma_1, \gamma_2, \ldots, \gamma_r\},$$

тј. нека су $\gamma_1, \gamma_2, \ldots, \gamma_r$ сви могући различити поретци бројева $1, 2, \ldots, p-1$ по модулу p. Означимо са $S = [\gamma_1, \gamma_2, \ldots, \gamma_r]$ најмањи заједнички садржалац тих бројева и нека је $S = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ његова канонска факторизација. Сваки фактор $q_i^{\alpha_i}$ тог разлагања је делилац бар једног од бројева γ_j, тј. важи $\gamma_j = \beta q_i^{\alpha_i}$. Нека је сада c_j било који од бројева $1, 2, \ldots, p-1$ за који је $r_p(c_j) = \gamma_j$. На основу тврђења i, за $d_j = c_j^{\beta}$ је $r_p(d_j) = q_i^{\alpha_i}$, па из тврђења ii следи да за број $g = d_1 d_2 \cdots d_k$ важи $r_p(g) = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k} = S$. Но, то значи да $S \mid p - 1 = \varphi(p)$.

Сада, међутим, имамо да сви бројеви $\gamma_1, \gamma_2, \ldots, \gamma_r$ деле S, што значи да је за свако $x \in \{1, 2, \ldots, p-1\}$ задовољена конгруенција $x^S \equiv 1 \pmod{p}$. Но, према тврђењу iii онда мора бити $p-1 \leq S$, па из доказаног $S \mid p - 1$ следи да је $S = p - 1$ и g је примитивни корен по модулу p.

3 Квадратни остаци и квадратни реципроцитет

Дефиниција 3.1. Нека је a цео број узајамно прост са датим модулом m, $m \in \mathbb{N}, m > 1$. Кажемо да је a **квадратни остатак** по модулу m ако постоји цео број x такав да m дели $x^2 - a$. У супротном, кажемо да је a **квадратни неостатак** по модулу m.

Дакле, a је квадратни остатак по модулу m ако конгруенција $x^2 \equiv a \pmod{m}$ има целобројних решења. Уколико је модул m прост број, квадратни остаци дају јак неопходан услов за тај прост број да буде облика $x^2 - ay^2$.

Теорема 3.1. Нека је p прост и a цео број који није дељив са p. Ако је

$$p = x^2 - ay^2$$

за неке целе бројеве x, y, тада је a квадратни остатак по модулу p.

Доказ. С обзиром да је p прост, следи да је $(p, y) = 1$. Дакле, постоје цели бројеви k и m, такви да је $kp + my = 1$. Замењујући $my = 1 - kp$ у

$$pm^2 = x^2m^2 - ay^2m^2 = (xm)^2 - a(ym)^2,$$

добијамо

$$pm^2 = (xm)^2 - a(1 - kp)^2,$$

одакле је

$$(xm)^2 - a = p(m^2 - 2ka + k^2pa).$$

Дакле, p дели $(xm)^2 - a$, па је a квадратни остатак по модулу p.

Лежандр је сматрао да је веома корисно увести симбол $\left(\frac{a}{p}\right)$, који сада зовемо Лежандров симбол, на следећи начин: ако је p непаран прост број који не дели цео број a, тада је $\left(\frac{a}{p}\right) = 1$ ако је a квадратни остатак по модулу p, а $\left(\frac{a}{p}\right) = -1$ иначе.

Дефиниција 3.2. За дати прост број p и цео број a, **Лежандров симбол** $\left(\frac{a}{p}\right)$ се дефинише као

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

Пример. Јасно је да је $\left(\frac{x^2}{p}\right) = 1$ за сваки прост број p и цео број x, за који $p \nmid x$.

Пример. Пошто је 2 квадратни остатак по модулу 7 ($3^2 \equiv 2$), а 3 то није, имамо $\left(\frac{2}{7}\right) = 1$ и $\left(\frac{3}{7}\right) = -1$.

Јасно је да је приликом решавања једначине $x^2 \equiv a \pmod{m}$ довољно наћи њена решења у скупу $\{0, 1, \ldots, m-1\}$, јер ако је x било које решење, тада је и сваки број из његове класе конгруенције по модулу m такође решење једначине. Зато ћемо се у даљем тексту увек ограничавати на таква решења.

Теорема 3.2. За дати непаран прост број p и цео број a, $p \nmid a$, једначина $x^2 \equiv a \pmod{p}$ или нема решења, или има тачно два решења.

Доказ. Претпоставимо да дата конгруенција има решења и да је x_1 једно од њих. Тада је очигледно и $x_2 = -x_1$ решење. Других решења по модулу p нема, јер $x^2 \equiv a \equiv x_1^2 \pmod{p}$ повлачи $x \equiv \pm x_1 \pmod{p}$. При том би $x_1 \equiv -x_1 \pmod{p}$ имало за последицу $2x_1 \equiv 0 \pmod{p}$, што је немогуће због $(2, p) = (x_1, p) = 1$.

Из овог једноставног тврђења следи:

Теорема 3.3. За сваки непаран прост број p међу бројевима $1, 2, \ldots, p-1$ има тачно $\frac{p-1}{2}$ квадратних остатака и исто толико квадратних неостатака.

У даљем тексту, осим ако другачије нагласимо, сматраћемо да је p непаран прост број и a цео број, и писаћемо $p' = \frac{p-1}{2}$.

Јасно је да је a квадратни остатак по модулу p ако и само ако је то и $a + kp$ за неки цео број k. Зато можемо сматрати да је Лежандров симбол функција из скупа класа остатака по модулу p у скуп $\{-1, 0, 1\}$.

На основу Фермаове теореме важи $a^{p-1} \equiv 1 \pmod{p}$, одакле следи и $a^{p'} \equiv \pm 1 \pmod{p}$. Прецизније, важи следеће тврђење:

Теорема 3.4. (Ојлеров критеријум) Нека је p непаран прост броји који не дели цео број a. Тада

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

Доказ. Нека је g примитивни корен по модулу p (он постоји на основу теореме 2.3). Тада је сваки остатак по модулу p задат са g^i, $i = 0, 1, \ldots, p-2$. Приметимо да је $(g^i)^{p'} = g^{ip'} \equiv 1$ ако и само ако $p-1|ip'$, тј. ако и само ако $2|i$.
С друге стране, g^i је квадратни остатак по модулу p ако и само ако постоји $j \in \{0, 1, \ldots, p-2\}$ такав да је $(g^j)^2 \equiv g^i \pmod{p}$, што је еквивалентно са $2j \equiv i \pmod{p-1}$. Последња конгруенција има решења ако и само ако $2|i$, дакле управо онда када је $(g^i)^{p'} \equiv \pmod{p}$.

Ојлер није знао нотацију Лежандровог симбола и отуда су његова тврђења била мање компактна.

Последица. За сваки прост број $p > 2$ важи $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Другим речима, конгруенција $x^2 \equiv -1$ по простом модулу p има решења ако и само ако је $p = 2$ или $p \equiv 1 \pmod{4}$. Такође,

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

Следећа важна својства Лежандровог симбола следе директно из Ојлеровог критеријума.

Теорема 3.5. Лежандров симбол је мултипликативан, тј. за све целе бројеве a и b и прост број $p > 2$ важи

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$

Такође, из $\left(\frac{-a^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a^2}{p}\right) = \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$ следи да је $\left(\frac{-a^2}{p}\right) = 1 \Leftrightarrow p \equiv 1 \pmod{4}$.

За цео број a, $p \nmid a$ и $k = 1, 2, \ldots, p'$ постоји јединствено

$$r_k \in \{-p', \ldots, -2, -1, 1, 2, \ldots, p'\}$$

за које је $ka \equiv r_k \pmod{p}$. Штавише, никоја два од r_k-ова не могу бити једнаки по апсолутној вредности, па је $|r_1|, |r_2|, \ldots, |r_{p'}|$ заправо пермутација скупа $\{1, 2, \ldots, p'\}$. Тада је $a^{p'} = \frac{a \cdot 2a \cdot \ldots \cdot p'a}{1 \cdot 2 \cdot \ldots \cdot p'} \equiv a^{p'} = \frac{r_1 \cdot r_2 \cdot \ldots \cdot r_{p'}}{1 \cdot 2 \cdot \ldots \cdot p'}$. Ако сада пишемо $r_k = \varepsilon_k |r_k|$ за $k = 1, \ldots, p'$, при чему је $\varepsilon_k = \pm 1$, из Ојлеровог критеријума добијамо да важи:

Теорема 3.6. $\left(\frac{a}{p}\right) = \varepsilon_1\varepsilon_2\ldots\varepsilon_{p'}$.

Приметимо да је $r_k = -1$ ако и само ако је остатак броја ka при дељењу са p већи од p', тј. ако и само ако је $\left[\frac{2ka}{p}\right] = 2\left[\frac{ka}{p}\right] + 1$. Према томе, $r_k = (-1)^{\left[\frac{2ka}{p}\right]}$. Сада из претходне теореме добијамо следеће:

Теорема 3.7. (Гаусова лема) Важи $\left(\frac{a}{p}\right) = (-1)^S$, где је $S = \sum_{k=1}^{p'}\left[\frac{2ka}{p}\right]$.

Гаусова лема нам омогућава да за мало a или мало p лако израчунамо вредност Лежандровог симбола $\left(\frac{a}{p}\right)$. На пример, за $a = 2$ имамо $\left(\frac{2}{p}\right) = (-1)^S$, где је $S = \sum_{k=1}^{p'}\left[\frac{4k}{p}\right]$. У овој суми је тачно $\left[\frac{1}{2}p'\right]$ сабирака једнако 0, док је преосталих $p' - \left[\frac{1}{2}p'\right]$ једнако 1. Према томе, $S = p' - \left[\frac{1}{2}p'\right] = \left[\frac{p+1}{4}\right]$, што је парно за $p \equiv \pm 1$, а непарно за $p \equiv \pm 3 \pmod 8$. Овако смо добили да важи:

Теорема 3.8. $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$. Другим речима, 2 је квадратни остатак по простом модулу $p > 2$ ако и само ако је $p \equiv \pm 1 \pmod 8$.

На сличан начин се могу доказати следећа тврђења:

Теорема 3.9. 1° -2 је квадратни остатак по модулу p ако и само ако је $p \equiv 1$ или $p \equiv 3 \pmod 8$;
2° -3 је квадратни остатак по модулу p ако и само ако је $p \equiv 1 \pmod 6$;
3° 3 је квадратни остатак по модулу p ако и само ако је $p \equiv \pm 1 \pmod{12}$;
4° 5 је квадратни остатак по модулу p ако и само ако је $p \equiv \pm 1 \pmod{10}$.

У току истраживања репрезентације броја p преко $x^2 \pm qy^2$, где су p и q различити прости бројеви, Лежандр је схватио да мора да посматра и $\left(\frac{q}{p}\right)$ као и $\left(\frac{p}{q}\right)$. Ова истраживања довела су га до формулације његовог познатог закона о квадратном реципроцитету.

Теорема 3.10. (Гаусов закон реципроцитета) Нека су p и q различити непарни прости бројеви. Тада важи

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

при чему је $p' = \dfrac{p-1}{2}$ и $q' = \dfrac{q-1}{2}$.

Доказ 1. Означимо $S(p,q) = \sum_{k=1}^{q'} \left[\dfrac{kp}{q}\right]$. Прво ћемо доказати следеће помоћно тврђење.

Лема. $S(p,q) + S(q,p) = p'q'$.

Доказ. Приметимо да је $\left[\dfrac{kp}{q}\right]$ број тачака у координатној равни са координатама (k,l), таквим да је $0 < l < kp/q$, тј таквим да је $0 < ql < kp$. Одавде закључујемо да је сума $S(p,q)$ број свих тачака (k,l) таквих да је $0 < k < p'$ и $0 < ql < kp$. Другим речима, $S(p,q)$ је број тачака са координатама у $\mathbb{N}$ унутар правоугаоника $ABCD$ (укључујући и границу) које се налазе испод праве AE, где је $A(0,0), B(p',0), C(p',q'), D(0,q'), E(p,q)$.

Аналогно добијамо да је $S(q,p)$ број тачака са координатама у $\mathbb{N}$ унутар правоугаоника $ABCD$ која се налазе изнад праве AE. Како је укупан број тачака са целобројним координатама унутар овог правоугаоника једнак $p'q'$, а на правој AE нема таквих тачака, следи да је $S(p,q) + S(q,p) = p'q'$.

Вратимо се сада на доказ теореме. Имамо

$$S(p+q,q) - S(p,q) = 1 + 2 + \cdots + p' = \frac{p^2-1}{8},$$

а лако се проверава да је $\left(\dfrac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. Гаусова лема нам даје

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

дакле, $\left(\dfrac{p}{q}\right) = (-1)^{S(p,q)}$. Аналогно је $\left(\dfrac{q}{p}\right) = (-1)^{S(q,p)}$. Множењем ове две једнакости и коришћењем леме добијамо тражену једнакост.

Доказ 2. За сваки цео брј x, ако је $0 < x < q/2$, постоје цели бројеви y и r такви да је $px = qy + r$. Према Гаусовој леми, $\left(\dfrac{p}{q}\right) = (-1)^k$, где је k број остатака $r = px - qy$ таквих да је $r < 0$. То значи да је k број тачака (x,y) које задовољавају услове: $0 < x < \frac{1}{2}q$ и $-\frac{1}{2}q < px - py < 0$. Отуда следи да је $y < px/q + 1/2 < (p+1)/2$, па како је y цео број, то значи да је $0 < y < p/2$.

Дакле, све тачке (x, y) припадају правоугаонику $P = \{(x, y) : 0 < x < q/2, 0 < y < p/2\}$, а k је број елемената скупа $P_1 \subset P$, који се састоји од тачака (x, y) таквих да важи услов $-q/2 < px - qy < 0$. Слично, $\left(\frac{q}{p}\right) = (-1)^m$, где је m број елемената скупа $P_2 \subset P$, који се састоји од тачака (x, y) таквих да важи услов $-p/2 < qy - px < 0$.

Треба још доказати да је број $s = (p-1)(q-1)/2 - (k+m)$ паран. Међутим, s је број тачака правоугаоника P које нису у P_1 или нису у P_2, односно које припадају $P_1^c \cup P_2^c$. Како скупу P_1^c припадају тачке које задовољавају услов $px - qy \leq -q/2$, а скупу P_2^c тачке за које важи услов $qy - px \leq -p/2$, скупови P_1^c и P_2^c су дисјунктни. Међутим, како је трансформација $x = (q+1)/2 - x'$, $y = (p+1)/2 - y'$ обострано једнозначна и преводи скупове P_1^c и P_2^c један у други, број s мора бити паран.

Урадимо сада пример наведен пре теореме.

Пример. $\left(\frac{814}{2003}\right) = \left(\frac{2}{2003}\right)\left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right) = -\left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right)$. Даље, према закону реципроцитета је $\left(\frac{11}{2003}\right) = -\left(\frac{2003}{11}\right) = \left(\frac{1}{11}\right) = 1$ и $\left(\frac{37}{2003}\right) = \left(\frac{2003}{37}\right) = \left(\frac{5}{37}\right) = \left(\frac{37}{5}\right) = -1$. Добијамо $\left(\frac{814}{2003}\right) = 1$, тј. 814 је квадратни остатак по модулу 2003.

Једну од могућих корисних формулација закона реципроцитета даје и следећа:

Последица. Нека су p и q различити прости бројеви. Ако су p и q оба облика $4k + 3$, онда је једна од једначина

$$x^2 \equiv p \pmod{q}, \quad y^2 \equiv q \pmod{p} \tag{1}$$

решива, а друга није. Ако p и q нису оба облика $4k + 3$, тада су или обе једначине (1) решиве или није ниједна.

Пример. 1° $p = 5, q = 11$. Обе једначине $x^2 \equiv 5 \pmod{11}$, $y^2 \equiv 11 \pmod{5}$ су решиве (нпр. $x = 4, y = 1$).
2° $p = 7, q = 11$. Једначина $x^2 \equiv 11 \pmod{7}$ је решива (нпр. $x = 2$), а $y^2 \equiv 7 \pmod{11}$ није.

4 Задаци

1. Наћи $\left(\frac{30}{211}\right)$.

Решење. Имамо $\left(\frac{30}{211}\right) = \left(\frac{2}{211}\right)\left(\frac{3}{211}\right)\left(\frac{5}{211}\right)$.
Како је $211 \equiv 3 \pmod 8$, добијамо $\left(\frac{2}{211}\right) = -1$.

За $\left(\frac{3}{211}\right)$, примењујемо квадратни реципроцитет да бисмо добили

$$\left(\frac{3}{211}\right) = \left(\frac{211}{3}\right)(-1)^{105} = -\left(\frac{211}{3}\right) = -\left(\frac{1}{3}\right) = -1.$$

На крају, имамо $\left(\frac{5}{211}\right) = \left(\frac{211}{5}\right)(-1)^{105\cdot 2} = \left(\frac{211}{5}\right) = \left(\frac{1}{5}\right) = 1$.
Користећи све претходно, добијамо $\left(\frac{30}{211}\right) = (-1)(-1)(+1) = 1$.

2. Нека су a и b позитивни цели бројеви такви да су бројеви $15a+16b$ и $16a-15b$ квадрати позитивних целих бројева. Која је најмања могућа вредност коју може имати мањи од та два квадрата?

Решење. Нека је $15a + 16b = k^2$ и $16a - 15b = l^2$. Тада је

$$a = \frac{15k^2 + 16l^2}{481},\ b = \frac{16k^2 - 15l^2}{481},\ k, l \in \mathbb{N}.$$

Како је $481 = 13 \cdot 37$, имамо

$$15k^2+16l^2 \equiv 0 \pmod{13}, \quad 2k^2 \equiv -3l^2 \pmod{13}, \quad k^2 \equiv 5l^2 \pmod{13}.$$

Након тога, добијамо $\left(\frac{5}{13}\right) = -1$, из чега следи да $13 \mid l$ и $13 \mid k$. Приметимо да

$$\begin{aligned} 15k^2 + 16l^2 &\equiv 0 \pmod{37}, \\ 32l^2 &\equiv -30k^2 \pmod{37}, \\ -5l^2 &\equiv -30k^2 \pmod{37}, \\ l^2 &\equiv 6k^2 \pmod{37}. \end{aligned}$$

У комбинацији са тим да је $\left(\frac{6}{37}\right) = -1$, добијамо да $37 \mid k$ и $37 \mid l$. Најмања могућа вредност за l је $13 \cdot 37 = 481$. Моземо узети да је $k = l = 481$ и тако добијамо да је $a = 31 \cdot 481,\ b = 481$.

3. Доказати да број облика $2^n + 1$ нема простих чинилаца облика $8k + 7$.

Решење. Претпоставимо да постоји прост број p такав да $p \mid 2^n + 1$ и $p \equiv 7 \pmod 8$. Ако је n паран, $\left(\frac{-1}{p}\right) = 1$, али

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

пошто $p \equiv 3 \pmod 4$, па смо добили контрадикцију.
Ако је n непаран, добијамо да је $2^{n+1} \equiv -2 \pmod p$, па је -2 квадратни остатак по модулу p, пошто је $n + 1$ паран број, па $\left(\frac{-2}{p}\right) = 1$, али

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

што је такође контрадикција.

4. За позитиван цео број a дефинишимо низ позитивних целих бројева $x_1, x_2, \ldots$ таквих да је $x_1 = a$ и $x_{n+1} = 2x_n + 1$ за $n \geq 1$. Нека је $y_n = 2^{x_n} - 1$. Одредити највећи могући број k такав да су за неки позитиван цео број a бројеви $y_1, \ldots, y_k$ сви прости.

Решење. Доказаћемо да је решење 2. Претпоставимо да постоји број a такав да је $k \geq 3$. Бројеви $2^a - 1, 2^{2a+1} - 1, 2^{4a+3} - 1$ су прости, па су и бројеви $a, 2a + 1, 4a + 3$ такође прости (због тога што важи - ако је број $2^M - 1$ прост, тада је M такође прост; у супротном би, да постоји природан број d такав да $d \mid M$, $2^d - 1$ делило $2^M - 1$). Искористимо сада Ојлеров критеријум:

$$2^{\frac{4a+3-1}{2}} \equiv \left(\frac{2}{4a+3}\right) \pmod{4a+3} \Rightarrow 2^{2a+1} \equiv \left(\frac{2}{4a+3}\right) \pmod{4a+3}.$$

Како је $2^{2a+1} - 1$ прост број, тада је $2^{2a+1} \not\equiv 1 \pmod{4a+3}$, јер би у супротном било $2^{2a+1} = 4a + 4$, што би значило да је $a = 1$, што је немогуће. Дакле, имамо

$$\left(\frac{2}{4a+3}\right) = -1 \Rightarrow -1 = (-1)^{\frac{(4a+2)(4a+4)}{8}} = (-1)^{(2a+1)(a+1)},$$

што имплицира да је број $a+1$ непаран. Пошто је a прост број, то значи да је $a = 2$. Ако је $a = 2$, имамо да $2^{11} - 1 = 23 \cdot 87$ није прост број, што је немогуће. Дакле, добијамо да је одговор 2 што се постиже за $a = 2$.

5. Претпоставимо да позитиван цео број a није потпун квадрат. Тада је $\left(\frac{a}{b}\right) = -1$ за бесконачно много простих бројева p.

Решење. Претпоставимо да је тврдња нетачна. То би значило да постоји број r такав да за сваки прост број $q > r$ важи $\left(\frac{a}{q}\right) = 1$. Пошто a није потпун квадрат, можемо да га представимо као $a = x^2 p_1 p_2 \dots p_k$, где су $p_1, p_2 \dots p_k$ прости бројеви у растућем редоследу. Узмимо прост број $p > r, p \equiv 5 \pmod 8$. Имамо да је

$$\left(\frac{a}{b}\right) = \left(\frac{p_1}{p}\right)\left(\frac{p_2}{p}\right)\dots\left(\frac{p_k}{p}\right).$$

Ако је p_i непаран, онда је, због Гаусовог закона реципроцитета $\left(\frac{p_i}{p}\right) = \left(\frac{p}{p_i}\right)$.

Ако је $p_1 = 2$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = -1$, па је

$$\left(\frac{a}{b}\right) = \left(\frac{p}{p_1}\right)\dots\left(\frac{p}{p_k}\right) \text{ ili } \left(\frac{a}{b}\right) = -\left(\frac{p}{p_2}\right)\dots\left(\frac{p}{p_k}\right).$$

Можемо узети остатке $r_2, r_3, \dots, r_k \pmod{p_2, p_3, \dots, p_k}$ такве да је $\left(\frac{r_2}{p_2}\right)\dots\left(\frac{r_k}{p_k}\right)$ једнако 1 или -1. По Кинеској теореми о остацима, имамо коначно много бројева t за које важи

$$t \equiv 5 \pmod 8,\ t \equiv r_i \pmod{p_i},\ 2 \le i \le k.$$

Сада посматрамо прогресију $t + l8p_2p_3\dots p_k$, где по Дирихлеовој теореми има коначно много простих бројева q. Узмимо да је $q > r$. Приметимо да имамо $\left(\frac{a}{q}\right) = 1$, али како је већ поменуто, можемо изабрати $r_2, r_3, \dots, r_k$ тако да $\left(\frac{a}{q}\right) = -1$, што је контрадикција.

Задатак 6. Доказати да је цео број q квадратни остатак по сваком простом модулу ако и само ако је a потпун квадрат.

Решење. Претпоставимо да a није потпун квадрат. Без смањења општости можемо претпоставити да a није дељиво квадратом.

Претпоставимо да је $a > 0$. Тада је $a = p_1 p_2 \cdots p_k$ за неке просте бројеве $p_1, \ldots, p_k$. За сваки прост број p важи

$$\left(\frac{a}{p}\right) = \prod_{i=1}^{k} \left(\frac{p_i}{p}\right) \qquad \text{и} \qquad \left(\frac{p_i}{p}\right) = (-1)^{p_i' p'} \left(\frac{p}{p_i}\right). \tag{1}$$

Ако је $a = 2$, одаберимо $p = 5$. У супротном, постоји непаран прост делилац броја a, рецимо p_k. Одаберимо такав прост број p да важи $p \equiv 1 \pmod 8$, $p \equiv 1 \pmod{p_i}$, за свако $i = 1, 2, \ldots, k-1$ и $p \equiv a \pmod{p_k}$, где је a произвољан квадратни неостатак по модулу p_k. Овакав прост број p постоји по Дирихлеовој теореми о простим бројевима у аритметичким прогресијама. Тада су на основу (1) бројеви $p_1, \ldots, p_{k-1}$ квадратни остаци, док је p_k квадратни неостатак $\pmod p$. Према томе, a је квадратни неостатак по модулу p. Сличан доказ се може спровести у случају да је $a < 0$.

Задатак 7. Нека је p непаран прост број већи од 3.

а) Доказати да је сума свих квадратних остатака по модулу p дељива са p.

б) Ако је $p \equiv 1 \pmod 4$, доказати да је сума свих квадратних остатака по модулу p једнака $\dfrac{p(p-1)}{4}$.

Решење. а) Нека је g примитиван корен по модулу p. Збир свих квадратних остатака је по модулу p конгруентан са

$$1 + g^2 + \cdots + g^{p-3} = (g^{p-1} - 1)/(g^2 - 1),$$

што је дељиво са p због $p > 3$. Доказ ја аналоган и у случају квадратних неостатака.

б) Приметимо да за свако $k \in \left\{1, 2, \ldots, \dfrac{p-1}{2}\right\}$ важи

$$\left(\frac{p-k}{p}\right) = \left(\frac{-k}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{k}{p}\right) = \left(\frac{k}{p}\right),$$

одакле закључујемо да се квадратни остаци по модулу p јављају у међусобно дисјунктним паровима тако да је збир елемената у сваком пару једнак p. Како квадратних остатака има укупно $\dfrac{p-1}{2}$, парова ће бити $\dfrac{p-1}{4}$, па ће збир свих квадратних остатака бити једнак $\dfrac{p(p-1)}{4}$.

Задатак 8. Ако је p непаран прост број, доказати да је производ свих квадратних остатака по модулу p по истом конгруентан са $(-1)^{\frac{p+1}{2}}$.

Решење. Ако са g означимо примитивни корен по модулу p, производ свих квадратних остатака по модулу p ће по истом бити конгруентан са

$$\prod_{i=1}^{\frac{p-1}{2}} g^{2i} = g^{\frac{(p-1)(p+1)}{4}} = (g^{\frac{p-1}{2}})^{\frac{p+1}{2}} \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

Задатак 9. (Вијетнамска средњошколска математичка олимпијада) Доказати да ни за један природан број n број $2^n + 1$ не може имати прост фактор облика $8k - 1$.

Решење. Нека је $p = 8k-1$ и $2^n+1 \equiv 0 \pmod{p}$. Нека је g примитивни корен по модулу p и $g^t \equiv 2 \pmod{p}$. Тада је

$$tn = (2m + 1)\frac{p-1}{2}.$$

за неко целобројно m, па ни $tn\dfrac{p-1}{2}$ није дељиво са $p - 1$, али јесте са $\dfrac{p-1}{2}$. Зато је

$$2^{n\frac{p-1}{2}} \equiv g^{tn\frac{p-1}{2}} \equiv -1 \pmod{p}$$

и због тога

$$2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

тј. $\left(\dfrac{2}{p}\right) = -1$, што је контрадикција.

За претходно решење се не може рећи да је "лепо и природно" обзиром да је у њему на груб начин демонстрирана моћ примитивног корена. Тачно је да се овај задатак могао и елегантније решити. Наиме, полазећи поново од претпоставке да је могуће да прост број p облика $8k - 1$ буде делилац броја $2^n + 1$, можемо прво закључити да број n мора бити непаран јер би у супротном број -1 био квадратни остатак по простом модулу конгруентном са -1 по модулу 4. Ако је n непаран број, услов дат у задатку можемо на врло једноставан начин поново да преведемо на обичну квадратну конгруенцију - помоножићемо све са 2. Тако добијамо да је $2^{n+1} \equiv -2 \pmod{p}$, односно $\left(\dfrac{-2}{p}\right) = 1$, што је контрадикција обзиром на Теорему 3.9. и облик броја p дат у услову задатка.

Задатак 10. Ако прост број p облика $4k - 1$ дели збир квадрата два природна броја, доказати да су онда ти бројеви дељиви са p.

Решење. Претпоставимо супротно, тј. да за неке природне бројеве a и b који нису дељиви са p важи да $p \mid a^2 + b^2$. Ако ово запишемо у облику

$$a^2 \equiv -b^2 \pmod{p},$$

закључујемо да је

$$\left(\frac{-b^2}{p}\right) = 1.$$

Међутим, са друге стране имамо

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

што је контрадикција.

Задатак 11. (Мађарска средњошколска математичка олимпијада) Нека је p прост број облика $4k+3$. Доказати да број $x^2 - x + \dfrac{p+1}{4}$ нема прост фактор облика $kp - 1$.

Решење. Нека је $x^2 + x + \dfrac{p+1}{4} \pmod{q}$ и $q = kp - 1$ прост број. То значи да $q \mid (2x+1)^2 + p$, тј. $\left(\dfrac{-p}{q}\right) = 1$.
С друге стране је

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

Задатак 12. Нека је p прост број. Доказати да постоји $x \in \mathbb{Z}$ такво да $p \mid x^2 - x + 3$ ако и само ако постоји $y \in \mathbb{Z}$ такво да $p \mid y^2 - y + 25$.

Решење. Тврђење је тривијално за $p \leq 3$, па можемо претпоставити да је $p \geq 5$.
Како је $p \mid x^2 - x + 3$ еквивалентно са $p \mid 4(x^2 - x + 3) = (2x-1)^2 + 11$, овакав цео број x постоји ако и само ако је -11 квадратни остатак по модулу p. Слично, због $4(y^2 - y + 25) - (2y-1)^2 + 99$, овакав y постоји ако и само ако је -99 квадратни остатак по модулу p. Сада тврђење задатка следи из чињенице да је $\left(\dfrac{-11}{p}\right) = \left(\dfrac{-11 \cdot 3^2}{p}\right) = \left(\dfrac{-99}{p}\right)$.

Задатак 13. Доказати да сви непарни делиоци броја $5x^2 + 1$ имају парну цифру десетица.

Решење. Ако $p \mid 5x^2+1$, онда је $\left(\frac{-5}{p}\right) = 1$. На основу закона реципроцитета важи $\left(\frac{-5}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{5}\right)$. Лако је проверити да је последњи израз једнак 1 ако и само ако је p конгруентно 1, 3, 7 или 9 по модулу 20.

Задатак 14. Наћи све $n \in \mathbb{N}$ такве да се скуп $A = \{n, n+1, \ldots, n+1997\}$ може разложити на неколико подскупова са једнаким производима елемената.

Решење. Претпоставимо да се A може разложити на k подскупова $A_1, \ldots, A_k$ са једнаким производом елемената m. Како је број елемената A дељивих простим бројем 1997 једнак 1 или 2, имамо $1997 \mid m$, па је $k = 1$ или $k = 2$. Даље, како је број елемената дељивих простим бројем 1999 једнак 0 или 1, имамо $1999 \nmid m$, па зато ниједан елемент A није дељив са 1999, тј. елементи A су конгруентни $1, 2, 3, \ldots, 1998$. Међутим, тада је $m^2 \equiv 1 \cdot 2 \cdot 3 \cdots 1998 \equiv -1 \pmod{1999}$, што није могуће јер -1 није квадратни остатак по модулу $1999 = 4 \cdot 499 + 3$.

Задатак 15. Доказати да не постоје природни бројеви a, b, c за које је $\dfrac{a^2+b^2+c^2}{3(ab+bc+ca)}$ цео број.

Решење. Претпоставимо да су a, b, c, n такви природни бројеви да је $a^2+b^2+c^2 = 3n(ab+bc+ca)$. Ову једнакост можемо написати као

$$(a+b+c)^2 = (3n+2)(ab+bc+ca).$$

Нека је $p \equiv 2 \pmod 3$ прост број такав да за неко $i \in \mathbb{N}$, $p^{2i-1} \mid 3n+2$ и $p^{2i} \nmid 3n+2$ (такво p мора да постоји). Тада $p^i \mid a+b+c$, одакле $p \mid ab+bc+ca$. Ако у последњу једнакост ставимо $c \equiv -a-b \pmod p$, добијамо $p \mid a^2+ab+b^2$, одакле $p \mid (2a+b)^2+3b^2$. Следи да је $\left(\frac{-3}{p}\right) = 1$, што није тачно јер је $p \equiv 2 \pmod 3$.

Задатак 16. Доказати да постоји бесконачно много позитивних целих бројева n, таквих да n^2+1 има прост делилац већи од $2n+\sqrt{2n}$.

Решење. Нека је p прост број и $p = 8k+1$. Приметимо да је $4^{-1} \equiv 6k+1 \pmod p$. Нека је $n = 4k-a,\ 0 \le a < 4k$. Тада је:

$$\left(\frac{p-1}{2} - a\right)^2 + 1 \equiv 0 \pmod p \Leftrightarrow 4^{-1} + a + a^2 + 1 \equiv 0 \pmod p,$$

па је

$$a(a+1) \equiv -6k - 2 \equiv 2k - 1 \pmod{p}.$$

Како је $a(a+1)$ парно и позитивно, онда је $a(a+1) \geq 10k$. Имамо да је

$$(a+1)^2 > a(a+1) \geq 10k > p,$$

па је

$$n = \frac{p+1}{2} - (a+1) < \frac{p+1}{2} - \sqrt{p} < \frac{p+1}{2} - \sqrt{2n},$$

и даље $2n + 2\sqrt{2n} - 1 > p$. Приметимо да је добијени резултат јачи од почетне неједнакости.

Задатак 17. Нека је p прост број такав да је $p \equiv 1 \pmod{4}$. Израчунати

$$S = \sum_{k=1}^{\frac{p-1}{2}} \left(\left[\frac{2k^2}{p} \right] - 2 \cdot \left[\frac{k^2}{p} \right] \right).$$

Решење. Нека су $r_1, r_2, \ldots, r_{\frac{p-1}{2}}$ квадратни остаци по модулу p. Прво, видимо да је тражена сума еквивалентна

$$\sum_{i=1}^{\frac{p-2}{2}} 2\left(\left\{ \frac{r_i}{p} \right\} - \left\{ \frac{2r_i}{p} \right\} \right).$$

Вредност $2\left\{ \frac{r_i}{p} \right\} - \left\{ \frac{2r_i}{p} \right\}$ је 0 ако је $r_i \leq \frac{p-1}{2}$, а 1 ако је $r_1 > \frac{p-1}{2}$. Дакле, S је број квадратних остатака који су већи од $\frac{p-1}{2}$. Како је $p \equiv 1 \pmod{4}$, ако је r_i квадратни остатак, онда је и $p - r_i$ квадратни остатак, па су пола целих бројева већих од $\frac{p-1}{2}$ такође квадратни остаци $\Rightarrow S = \frac{p-1}{4}$.

Задатак 18. Доказати да за сваки прост број p постоје цели бројеви a и b такви да је $a^2 + b^2 + 1$ умножак броја p.

Решење. Очигледно, $p \mid a^2 + b^2 + 1$ ако и само ако $a^2 \equiv -b^2 - 1 \pmod{p}$. Скупови $\{a^2 \mid a \in \mathbb{Z}\}$ и $\{-b^2 - 1 \mid b \in \mathbb{Z}\}$ по модулу p имају тачно $\frac{p+1}{2}$ чланова, тако да имају један заједнички члан, на пример постоје $a, b \in \mathbb{Z}$ такви да су a^2 и $-b^2 - 1$ једнаки по модулу p.

На крају, посматраћемо опште конгруенције другог степена - квадратне конгруенције,

$$f(x) = ax^2 + bx + c \equiv 0 \pmod{p},$$

где је $a \not\equiv 0 \pmod{p}$. Уколико није наглашено другачије, сматраћемо да је p непаран прост број.

Да бисмо решили ову конгруенцију, поступићемо као и код решавања квадратних једначина - свођењем на квадрат бинома. Дакле имамо:

$$\begin{aligned} ax^2 + bx + c &\equiv a\left(x^2 + \frac{bx}{a} + \frac{c}{a}\right) \\ &\equiv a\left(\left(x + \frac{b}{2a}\right)^2 + \frac{c}{a} - \frac{b^2}{4a^2}\right) \pmod{p}. \end{aligned}$$

Дакле, $f(x) \equiv 0 \pmod{p}$ ако и само ако је

$$\left(x + \frac{b}{2a}\right)^2 \equiv \frac{b^2}{4a^2} - \frac{c}{a} \pmod{p}.$$

Ако изаберемо $y = x + \dfrac{b}{2a}$ и $d = \dfrac{b^2}{4a^2} - \dfrac{c}{a}$, тада $f(x) \equiv 0 \pmod{p}$ има решење ако и само ако

$$y^2 \equiv d \pmod{p}$$

има решења, и тиме смо свели наш проблем на проблем квадратних остатака.

5 Литература

1. Jay R. Goldman: *The Queen of Mathematics, A historically Motivated Guide to Number Theory*, A K Peters, Wellesley, Massachusetts, 1998.

2. Душан Ђукић, Владимир Јанковић, Иван Матић, Никола Петровић: *The IMO Compendium - A collection of problems Suggested for the International Mathematical Olympiads: 1959 - 2004*, Springer, 2006.

3. Владимир Мићић, Зоран Каделбург, Душан Ђукић: *Увод у теорију бројева*, Београд, 2006.

4. И. М. Виноградов: *Основе теорије бројева*, М.Л. Гостехиздат, Москва, 1972.

5. *Квадратне конгруенције и Гаусов закон реципроцитета*, мастер рад, Александар Пејчев, Београд, 2010.

6. *Quadratic Congruences in Olympiad Problems,* Paul Stoinescu and Tudor-Dimitrie Popescu, Canadian Mathematical Society, 2017