Математичка гимназија

Гаусов закон реципроцитета

-Матурски рад из математике-

Ученик:
Ана Ђулинац

Ментор:
Милица Мисојчић

Београд 2020.

Садржај

1 Увод

Као једна од најстаријих математичких дисциплина, која своје корене полеже још пре 2000 година, теорија бројева је једна од најважнијих области математике. Проучавајући целе бројеве, вековима је постављала многа питања и проблеме, тако да су се њом бавили неки од највећих математичара попут Питагоре, Еуклида, Ојлера, Гауса и других.

Карл Фридрих Гаус (1777-1855) био је немачки математичар, физи чар и астроном. Дао је кључна открића у готово свим областима математике. Теорија бројева му је била једна од омиљених области математике и својим радом је допринео у њеном развоју. Колико је ову дисциплину сматрао важном показује и његова изјава да је математика краљица свих наука, док је теорија бројева краљица математике. Наставио је рад Ојлера и Лежандра и доказао је једну од најважнијих теорема у области теорије бројева - Гаусов закон реципроцитета. Иако је свако од ових математичара имао различит запис ове теореме, она се сада формулише уз помоћ Лежандровог симбола.

У овом раду је приказан један доказ ове теореме, као и неке од важнијих теорема из ове области. Следеће теореме ће се подразумевати у даљем раду и наводе се даље без доказа.

Теорема 1.1. *Ако је d највећи заједнички делилац целих бројева a и b, онда постоје бројеви α и β такви да је $\alpha a + \beta b = d$.*

Специјално, a и b су узајамно прости ако и само ако постоје цели бројеви α и β такви да је $\alpha a + \beta b = 1$.

Бројеви $(r_1, r_2, ..., r_m)$ чине потпун систем остатака по модулу m ако дају различите остатке при дељењу са m.
Када се из сведеног скупа остатака избаце сви бројеви који нису узајамно прости са m, добија се **сведени систем остатака**.

Теорема 1.2. *Нека је цео број k узајамно прост са датим модулом m. Ако бројеви $s_1, s_2, ..., s_\phi(m)$ чине сведен систем остатака по модулу m, бројеви $ks_1, ks_2, ..., ks_\phi(m)$ такође чине сведен систем остатака по модулу m.*

Дефиниција 1.1. *Број природних бројева који нису већи од датог природног броја n и узајамно су прости са њим, тј. број елемената произвољног сведеног система остатака по модулу n означава се са $\varphi(n)$. Функција φ зове се* **Ојлерова функција**.

Теорема 1.3. *Ако је* $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m}$ *канонска факторизација броја* n*, онда је*

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

где су $p_1, p_2, ..., p_m$ *различити прости чиниоци броја* n*.*

Теорема 1.4 (Ојлерова теорема)**.** *Ако је* $(a, m) = 1$*,* $a, m \in \mathbb{N}$ *онда је*

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

Теорема 1.5 (Мала Фермаова теорема)**.** *Ако је* p *прост број и* p *не дели* $a, a \in \mathbb{N}$*, онда је*

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

2 Примитивни корен по простом модулу

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 се са $r_m(a)$.*

Пример 2.1. *Поредак броја 3 по модулу 11 је 5, јер је $3^1, 3^2, 3^3, 3^4 \not\equiv 1 \pmod{11}$, а $3^5 \equiv 1 \pmod{11}$.* △

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

Доказ. ⇐ Ако су a и m узајамно прости бројеви, онда из Ојлерове теореме следи да је $a^{\varphi(m)} \equiv 1 \pmod{m}$. Дакле сигурно постоји бар један број $t, t \in \mathbb{N}$ такав да је $a^t \equiv 1 \pmod{m}$. Најмањи број t који задовољава ову једнакост је тражени поредак.
⇒ Ако је $a^t \equiv 1 \pmod{m}$, онда постоји природан број u, такав да је $a^t = mu + 1$, тј. $aa^{t-1} - mu = 1$. На основу теореме 1.2, следи да је $(a, m) = 1$. □

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. ⇐ Ако је $s = tq$, онда је $a^s = (a^t)^q \equiv 1 \pmod{m}$.
⇒ Нека је $s = tq + r$. Тада је $a^s = a^{tq+r} = (a^t)^q a^r \equiv a^r \pmod{m}$. Како је $0 < r < t$, долази до контрадикције са претпоставком да је t поредак броја a по модулу m. □

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

Пример 2.2. *Посматрајмо остатке $-3, -2, -1, 1, 2, 3$ 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. Бројеви који имају поредак по модулу 8 су $1, 3, 5, 7$. Ниједан од њих није примитивни корен јер је поредак сваког од њих једнак 2, а $\varphi(8) = 4$.* △

Теорема 2.3. *Ако је g примитивни корен по модулу m, тада бројеви*

$$g^0,\ g^1,\ g^2,\ \ldots,\ g^{\varphi(m)-1}$$

образују сведени систем остатака по модулу m.

Доказ. Уколико би постојали бројеви k и l, такви да је $0 \leq l < k < \varphi(m)$ и важи

$$g^k \equiv g^l \pmod{m},$$

онда је због $(g, m) = 1$

$$g^{k-l} \equiv 1 \pmod{m}.$$

Како је $0 < k - l < \varphi(m)$, следи да g није примитивни корен што је у супротности са претпоставком. □

Последица 2.1. *Ако је p прост број и g примитивни корен по модулу p, тада бројеви $1, g, g^2, ..., g^{p-2}$ образују свеђени систем остатака по модулу p.*

Пример 2.3. *По модулу 11 број 2 је примитивни корен, па бројеви* $1,\ 2,\ 2^2 = 4,\ 2^3 = 8,\ 2^4 \equiv 5,\ 2^5 \equiv 10,\ 2^6 \equiv 9,\ 2^7 \equiv 7,\ 2^8 \equiv 3,\ 2^9 \equiv 6 \pmod{11}$ *образују свеђени систем остатака по модулу* 11. △

Задатак 2.1. *Нека је $p \geq 3$ прост и n природан број. Доказати да је*

$$1^n + 2^n + ... + (p-1)^n \equiv \begin{cases} -1 \pmod{p}, & \text{ако } p-1 \mid n, \\ 0 \pmod{p}, & \text{иначе} \end{cases}$$

Решење. Ако $p - 1 \mid n$, тврђење следи из мале Фермаове теореме.
Нека $p - 1 \nmid n$ и нека је g примитивни корен по модулу p. Како је $\{1, g, g^2, ..., g^{p-2}\}$ пермутација скупа $\{1, 2, ..., p-1\}$, следи да је

$$1^n + 2^n + ... + (p-1)^n \equiv 1^n + g^n + ... + g^{(p-2)n} \equiv \frac{g^{(p-1)n} - 1}{g^n - 1} \equiv 0 \pmod{p}$$

□

Доказ егзистенције примитивног корена по простом модулу

Лема 2.1. *Ако је $r_m(x) = ab$, онда је $r_m(x^a) = b$.*

Доказ. Означимо $r_m(x^a)$ са γ. Како је $(x^a)^\gamma = x^{a\gamma} \equiv 1 \pmod{m}$, следи да $ab \mid a\gamma$, тј. $b \mid \gamma$.
Такође, из $x^{ab} = (x^a)^b \equiv 1 \pmod{m}$, следи да $\gamma \mid b$. Дакле, $b = \gamma$.

□

Лема 2.2. *Ако је $r_m(x) = a$, $r_m(y) = b$ и $(a, b) = 1$ онда је $r_m(xy) = ab$.*

Доказ. Означимо $r_m(xy)$ са γ. Тада је $xy^\gamma \equiv 1 \pmod{m}$ па је и $(xy)^{\gamma a} \equiv 1 \pmod{m}$, тј. $x^{\gamma a} y^{\gamma a} \equiv 1 \pmod{m}$. Како је $x^{\gamma a} \equiv 1 \pmod{m}$, следи да је $y^{\gamma a} \equiv 1 \pmod{m}$. Из $r_m(y) = b$ закључујемо да $b \mid a\gamma$, а пошто је $(a, b) = 1$, значи да $b \mid \gamma$. Аналогно се доказује да $a \mid \gamma$. Дакле, $ab \mid \gamma$.
Такође, како је $x^a \equiv 1 \pmod{m}$ и $y^b \equiv 1 \pmod{m}$, онда је и $x^{ab} \equiv 1 \pmod{m}$ и $y^{ab} \equiv 1 \pmod{m}$. Даље је $xy^{ab} \equiv 1 \pmod{m}$, следи $\gamma \mid ab$. Дакле, $ab = \gamma$. □

Лема 2.3. *Нека је p прост број, $n \in \mathbb{N}$ и $f(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ је полином са целобројним коефицијентима. Ако конгруенција $f(x) \equiv 0 \pmod{p}$ има више од n решења (различитих по модулу p), онда $p \mid a_k$ за свако $k = 0, 1, ..., n$.*

Доказ. Нека су $x_1, x_2, ..., x_n, x_{n+1}$ решења конгруенције $f(x) \equiv 0 \pmod{p}$. Полином $f(x)$ се може представити као:

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

Изаберимо најпре $b_n = a_n$. Затим бирамо b_{n-1} тако да су коефицијенти уз x_{n-1} са десне стране у збиру једнаки a_{n-1}. На исти начин се добијају коефицијенти $b_{n-2}, ..., b_1, b_0$.
Сада када се у једначини (1) x редом замени са $x_1, x_2, ..., x_{n+1}$, добија се да $p \mid b_0,\ p \mid b_1,\ ...,\ p \mid b_n$, одакле следи да су полазни коефицијенти $a_1, a_2, ..., a_n$ такође дељиви са p. □

Теорема 2.4. *За сваки прост број p постоји примитивни корен по модулу p.*

Доказ. За $p = 2$ доказ је тривијалан. Претпоставимо да је $p > 2$. Нека је

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

тј. $\gamma_1, \gamma_2, ..., \gamma_r$ су сви различити поретци бројева $1,\ 2, ..,\ p-1$. Нека је S најмањи заједнички садржалац бројева $\gamma_1, \gamma_2, ..., \gamma_r$ и нека је $S = {q_1}^{\alpha_1} {q_2}^{\alpha_2} \cdots {q_n}^{\alpha_n}$ његова канонска факторизација. Тада за свако ${q_i}^{\alpha_i}$ постоји бар једно γ_j тако да је $\gamma_j = \beta {q_i}^{\alpha_i}$. Ако сада означимо са c_j онај од бројева $1,\ 2, ..,\ p-1$ за који важи $r_p(c_j) = \gamma_j$ онда је на основу леме 2.1 $r_p({c_j}^{\beta}) = {q_i}^{\alpha_i}$, тј. за $d_j = {c_j}^{\beta}$ $r_p(d_j) = {q_i}^{\alpha_i}$. За број $g = d_1 d_2 \cdots d_k$ из леме 2.2 следи да је $r_p(q) = {q_1}^{\alpha_1} {q_2}^{\alpha_2} ... {q_k}^{\alpha_k} = S$. То значи да $S \mid \varphi(p) = p - 1$. Како сада сви бројеви $\gamma_1, \gamma_2, ..., \gamma_r$ деле S, једначина $x^S \equiv 1 \pmod{p}$ има решење за свако $x \in \{1, 2, ..., p-1\}$. Тада према леми 2.3 мора бити $p - 1 \leq S$, а како $S \mid p - 1$, следи да је $S = p - 1$ и g је примитивни корен по модулу p. □

3 Квадратни остаци

Дефиниција 3.1. *Нека су* m, n *и* a *цели бројеви,* $m > 1, n \geq 1$ *и* $(a, m) = 1$. *Каже се да је* a **остатак** n**-тог степена** *по модулу* m *ако конгруенција* $x^n \equiv a \pmod{m}$ *има целобројних решења. У супротном,* a *је* **неостатак** n**-тог степена**.

Специјално, за $n = 2$ остатак се назива **квадратним**.

Пример 3.1. *Како је* $5^2 \equiv 3 \pmod{11}$, *значи да је* 3 *квадратни остатак по модулу* 11.
Пошто једначина $x^2 \equiv 3 \pmod{7}$, *следи да је* 3 *квадратни неостатак по модулу* 7. △

Теорема 3.1. *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 у скупу* $\{1, 2, ..., p-1\}$.

Доказ. Претпоставимо да дата конгруенција има решења и да је $x \in \{1, 2, ..., p-1\}$ једно од њих. Ако је $y^2 \equiv a \pmod{p}$ за неко $y \in \{1, 2, ..., p-1\}$, ако је $y \neq x$ то значи да је $y^2 - x^2 \equiv 0 \pmod{p}$, тј. $p \mid (y-x)(y+x)$. Како је p прост број онда $p \mid y-x$ или $p \mid y+x$, а пошто је $x, y < p-1$ следи да њихова разлика не може бити дељива са p, тј. $p \mid y+x$ а то је могуће само ако је $x+y = p$. Како је p непаран, x и y морају бити међусобно различити. □

Дефиниција 3.2. *За дати непаран 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 3.2. *Јасно је да је* $(\frac{x^2}{p}) = 1$ *за сваки прост број* p *и цео број* x *за који* $p \nmid x$. △

Пример 3.3. *Пошто је* 2 *квадратни остатак по модулу* 7 ($3^2 \equiv 2$), *а* 3 *то није, имамо* $(\frac{2}{7}) = 1$ *и* $(\frac{3}{7}) = -1$. △

Теорема 3.2. $a \equiv b \pmod{p}$ *повлачи* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Доказ. Тврђење следи из дефиниције. □

Теорема 3.3 (Ојлеров критеријум)**.** $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Доказ. Тврђење је тривијално ако $p \mid a$.
Претпоставимо да $p \nmid a$. Нека је g примитивни корен по модулу p (он постоји на основу теореме 2.4). Тада је сваки остатак по модулу p задат са $g^i,\ i \in \{0, 1, ..., p-2\}$ (последица 2.1). Како је $r_p = p-1$, онда је $(g^i)^{\frac{p-1}{2}} \equiv g^{\frac{i(p-1)}{2}} \equiv 1 \pmod{p}$ ако и само ако $2 \mid i$.
Са друге стране, g^i је квадратни остатак по модулу p ако постоји $j,\ j \in \{0, 1, ..., p-2\}$ такво да је $g^{2j} \equiv g^i \pmod{p}$, тј. $2j \equiv i \pmod{p}$. То важи само ако $2 \mid i$ тј. ако $(g^i)^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. □

Теорема 3.4. *Лежандров симбол је мултипликативан, тј. за све целе бројеве a, b и прост број p, $p > 2$ важи $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.*

Доказ. На основу Ојлеровог критеријума важи $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \pmod{p}$ и $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \pmod{p}$, па је и $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$, тј. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. □

Задатак 3.1. *Постоји природан број $a < \sqrt{p}+1$ који је квадратни неостатак по модулу p. Доказати.*

Решење. Нека је a најмањи квадратни остатак по модулу p и $b = [\frac{p}{a}]+1$. Како је $0 < ab - p < a$, $ab - p$ мора бити квадратни остатак. Тада је

$$1 = \left(\frac{ab-p}{p}\right) = \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = -\left(\frac{b}{p}\right).$$

Према томе, b мора бити квадратни неостатак, па је $a \leq b < \frac{p}{a} + 1 \leq \frac{p-1}{a} + 2$, одакле следи тврђење. □

Теорема 3.5. *За сваки прост број $p > 2$ важи $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$.*

Доказ. Тврђење важи на основу Ојлеровог критеријума за $a = -1$. □

Последица 3.1. *Сваки прост делилац броја $x^2 + y^2$ (при чему су $x, y \in \mathbb{N}$ узајамно прости бројеви) је или облика $4k + 1, k \in \mathbb{N}$, или је једнак 2.*

Доказ. Нека је p непаран прост делилац броја облика $x^2 + y^2$, тада је $x^2 \equiv -y^2 \pmod{p}$. Следи да је $1 = \left(\frac{-y^2}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{y^2}{p}\right) = (-1)^{\frac{p-1}{2}}$. Одатле је $p \equiv 1 \pmod{4}$. □

Теорема 3.6. *Нека је g примитивни корен по непарном простом модулу p. Разматрамо његове експоненте мање од p. Парни експоненти су конгруентни квадратним остацима, а непарни квадратним неостацима по модулу p.*

Доказ. Бројеви облика g^i, $i \in \{0, 1, ..., p-2\}$ образују сведен систем остатака по модулу p. Према Ојлеровом критеријуму, $(g^i)^{\frac{p-1}{2}} = g^{i\frac{p-1}{2}} \equiv \pm 1 \pmod{p}$. Види се да је $g^{i\frac{p-1}{2}} \equiv 1 \pmod{p}$ ако и само ако је $p-1 \mid i\frac{p-1}{2}$, тј. ако и само ако $2 \mid i$. Такође је и $g^{i\frac{p-1}{2}} \equiv 1 \pmod{p}$ ако и само ако $2 \nmid i$. □

Последица 3.2. *За дати прост број p међу бројевима $1, 2, ..., p-1$ има тачно $\frac{p-1}{2}$ квадратних остатака (и исто толико квадратних неостатака).*

За цео број a и $k \in \{1, 2, ..., p'\}$, где је $p' = \frac{p-1}{2}$ постоји јединствено r_k,

$$r_k \in \{-p', ..., -1, 0, 1, ..., p'\}$$

такво да је $ka \equiv r_k \pmod{p}$. Тачније, свако r_k мора бити јединствено по апсолутној вредности, тако да је $|r_1|, |r_2|, ..., |r'_p|$ пермутација скупа $\{1, 2, ..., p'\}$. Тада је $a^{p'} = \frac{1a \cdot 2a \cdot ... \cdot p'a}{1 \cdot 2 \cdot ... \cdot p'} \equiv \frac{r_1 \cdot r_2 \cdot ... \cdot r_{p'}}{1 \cdot 2 \cdot ... \cdot p'} \pmod{p}$. Сада је $r_k = \varepsilon_k |r_k|$, где је $\varepsilon_k \in \{-1, 1\}$.

Теорема 3.7. *Важи* $\left(\frac{a}{p}\right) = \varepsilon_1 \varepsilon_2 \cdots \varepsilon_{p'}$.

Доказ. Теорема важи на основу Ојлеровог критеријума. □

Теорема 3.8 (Гаусова лема)**.** *Важи* $\left(\frac{a}{p}\right) = (-1)^s$, *где је* $s = \sum_{k=1}^{\frac{p-1}{2}} [\frac{2ka}{p}]$.

Доказ. Број s представља број оних бројева из скупа $\{a, 2a, ..., (\frac{p-1}{2})a\}$ који при дељењу са p дају остатак већи од $\frac{p}{2}$. Нека су $r_1, r_2, ..., r_s$ тих s бројева, а $t_1, t_2, ..., t_k$ преосталих $\frac{p-1}{2} - s$. Посматрамо бројеве $p - r_1,\ p - r_2,\ ...,\ p - r_s$. Очигледно је да су сви међусобно различити. Такође важи да за свако i, j важи $p - r_i \neq t_j$. Како су сви бројеви различити, мањи од $\frac{p}{2}$ и има их $\frac{p-1}{2}$ следи да су они пермутација скупа $1, 2, ..., \frac{p-1}{2}$. Тако је:

$$(p - r_1)(p - r_2)...(p - r_s)t_1 t_2 ... t_k = 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2}$$

$$(-1)^s r_1 r_2 ... r_s t_1 t_2 ... t_k \equiv 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2} \pmod{p}$$

$$(-1)^s a \cdot 2a \cdot ... \cdot \left(\frac{p-1}{2}\right) a \equiv 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2} \pmod{p}$$

$$(-1)^s \equiv a^{\frac{p-1}{2}} \pmod{p}$$

□

Теорема 3.9. *Важи* $\left(\frac{2}{p}\right) = (-1)^{[\frac{p+1}{4}]} = (-1)^{\frac{p^2-1}{8}}$.

Доказ. По Гаусовој леми важи $\left(\frac{2}{p}\right) = (-1)^s$, где је $s = \sum_{k=1}^{\frac{p-1}{2}} [\frac{4k}{p}]$. У овој суми је тачно $[\frac{p-1}{4}]$ бројева једнако 0. То значи да је преосталих $\frac{p-1}{2} - [\frac{p-1}{4}]$ једнако 1. Тада је $s = \frac{p-1}{2} - [\frac{p-1}{4}] = [\frac{p+1}{4}]$ што је парно за $p \equiv \pm 1 \pmod 8$, а непарно за $p \equiv \pm 3 \pmod 8$.
Како прост број p може давати остатке ± 1 и ± 3 при дељењу са 8, важи да је за $p \equiv \pm 1 \pmod 8$ израз $\frac{p^2-1}{8}$ паран, а за $p \equiv \pm 3 \pmod 8$ непаран на основу чега следи тврђење. □

Теорема 3.10. 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* $p \equiv \pm 1 \pmod{10}$.

Доказ. Тврђења се показују на сличан начин као претходна теорема. □

Задатак 3.2. *Израчунати* $[\frac{1}{2003}] + [\frac{2}{2003}] + [\frac{2^2}{2003}] + ... + [\frac{2^{2001}}{2003}]$.

Решење. На основу Ојлеровог критеријума и теореме 3.9 важи $2^{1001} \equiv \left(\frac{2}{2003}\right) = -1 \pmod{2003}$. Дакле, $2003 \mid 2^i(2^{1001}+1) = 2^{1001+i}+2^i$, а како 2003 не дели ни 2^{1001+i} ни 2^i следи

$$\left[\frac{2^{1001+i}}{2003}\right] + \left[\frac{2^i}{2003}\right] = \frac{2^{1001+i}+2^i}{2003} - 1.$$

Сабирањем једнакости за $i = 0, 1, ..., 1000$ добијамо да је тражена сума једнака $\frac{1+2+2^2+...+2^{2001}}{2003} - 1001 = \frac{2^{2002}-1}{2003} - 1001$. □

4 Гаусов закон реципроцитета

Многи математичари, укључујући Ојлера и Лежандра имали су своје формулације ове теореме и безуспешно су покушавали да је докажу, све до 1801, када је Гаус објавио први доказ у својој књизи *Disquisitiones Arithmeticae*. Ту је назива фундименталном теоремом говорећи да се она засигурно мора сматрати најелегантнијом теоремом своје врсте. Такође, о важности ове теореме говори и то да ју је Гаус звао својом златном теоремом. Ова теорема омогућава лако израчунавање Лежандровог симбола. Гаус је осмислио укупно осам доказа ове теореме, док их данас постоји преко двеста.

Теорема 4.1 (Гаусов закон реципроцитета)**.** *Нека су p и q различити прости бројеви. Тада важи:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

Доказ. Посматрамо парове облика (qx, py), где је $1 \leq x \leq \frac{p-1}{2}$ и $1 \leq y \leq \frac{q-1}{2}$. Јасно је да ни у једном пару није $qx = py$. Нека су A и B скупови за које важи редом $qx > py$, односно $py > qx$. За скуп A важи $1 \leq x \leq \frac{p-1}{2}$ и $1 \leq y \leq \frac{qx}{p}$ па је кардиналност скупа A једнака

$$C_a = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right].$$

Даље је

$$C_a = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{qx}{p}\right] = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{(p+q)x}{p}\right] - \sum_{x=1}^{\frac{p-1}{2}} x = \sum_{x=1}^{\frac{p-1}{2}} \left[\frac{2\frac{(p+q)}{2}x}{p}\right] - \frac{p^2-1}{8}.$$

Када се -1 степенује добијеном сумом на основу Гаусове леме и теореме 3.9 се добије

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

Сличну ствар урадимо за скуп B. Како парова има $\frac{(p-1)(q-1)}{4}$, следи

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

□

Пример 4.1. $\left(\frac{814}{2003}\right) = \left(\frac{2}{2003}\right)\left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right) = -\left(\frac{11}{2003}\right)\left(\frac{37}{2003}\right)$. *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 *није квадратни остатак по модулу* 2003. △

5 Задаци

Задатак 5.1. *Нека је p непаран прост број, $a, b, c \in \mathbb{Z}$ и претпоставимо да $p \nmid a$. Тада број решења једначине*

$$ax^2 + bx + c \equiv 0 \pmod{p}$$

у скупу $\{0, 1, ..., p-1\}$ износи $1 + \left(\frac{b^2-4ac}{p}\right)$. Доказати.

Решење. Када израз трансформишемо множењем са $4a$ и додавањем и одузимањем b^2 добија се
$ax^2 + bx + c \equiv 0 \pmod{p} \iff 4a^2x^2 + 4abx + b^2 - b^2 + 4ac \equiv 0 \pmod{p} \iff (2ax + b)^2 + 4ac - b^2 \equiv 0 \pmod{p} \iff (2ax + b)^2 \equiv b^2 - 4ac \pmod{p}$, тј. $\left(\frac{b^2-4ac}{p}\right) = 1$. Како ова једначина има или ниједно или тачно два решења, следи да је број решења $1 + \left(\frac{b^2-4ac}{p}\right)$. □

Задатак 5.2. *Доказати да је број решења (x, y) конгруенције $x^2 - y^2 \equiv D \pmod{p}$, за $p \nmid D$, једнак $p - 1$.*

Решење. Тврђење следи из чињенице да је за фиксно y број решења конгруенције $x^2 \equiv y^2 + D \pmod{p}$ једнак $\left(\frac{y^2+D}{p}\right) + 1$. □

Задатак 5.3. *Постоји ли природан број x такав да важи*

$$1999 \mid x^2 + (x+1)^2?$$

Решење. Када трансформишемо израз добијамо

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

што је могуће ако и само ако је p облика $4k + 1$. Дакле, не постоји такав број x. □

Задатак 5.4. *Нека је p непаран прост број већи од 3.*

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

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

Решење. (i) Нека је g примитивни корен по модулу p. Тада је збир свих квадратних остатака по модулу p конгруентан са

$$g^0 + g^2 + ... + g^{p-3} = \frac{g^{p-1} - 1}{g^2 - 1},$$

што је дељиво са p због $p > 3$.

(ii) За свако $k \in 1, 2, ..., \frac{p-1}{2}$ 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 следи да се квадратни остаци по модулу p јављају у међусобно дисјунктним паровима у којима је збир чланова једнак p. Како квадратних остатака има $\frac{p-1}{2}$, значи да парова има $\frac{p-1}{4}$, па је збир свих квадратних остатака по модулу p једнак $\frac{p(p-1)}{4}$.

□

Задатак 5.5. *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^i означимо примитивни корен по модулу p, производ свих квадратних остатака по модулу p ће 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 5.6. *Нека је прост број $p > 3$ облика $4k + 3$ и $q = 2p + 1$ такође прост број. Доказати да је у том случају број $2^p - 1$ сложен.*

Решење. За сваки прост број q важи

$$2^{\frac{q-1}{2}} \equiv \left(\frac{2}{p}\right) \equiv (-1)^{[\frac{q+1}{4}]} \equiv 1 \pmod{q}$$

како је $q \equiv 7 \pmod 8$, следи да је број $2^p - 1$ дељив са q. □

Задатак 5.7. *Израчунати вредност Лежандровог симбола $\left(\frac{-63}{11}\right)$.*

Решење. Како је $-63 = (-1) \cdot 3^2 \cdot 7$, важи

$$\left(\frac{-63}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{3}{11}\right)^2\left(\frac{7}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{7}{11}\right).$$

Даље, знамо да је $\left(\frac{-1}{11}\right) = (-1)^{\frac{11-1}{2}} = -1$. Према Гаусовом закону реципротета следи $\left(\frac{7}{11}\right)\left(\frac{11}{7}\right) = (-1)^{\frac{11-1}{2}\frac{7-1}{2}} = -1$, тј. важи $\left(\frac{7}{11}\right) = -\left(\frac{11}{7}\right) = -\left(\frac{4}{7}\right) = -\left(\frac{2}{11}\right)^2 = -1$. Коначно,

$$\left(\frac{-63}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{7}{11}\right) = 1.$$

□

Задатак 5.8. *Доказати да број* 2^n+1 *није дељив ниједним простим бројем облика* $8k+7$.

Решење. Претпоставимо супротно, нека постоји прост број p облика $8k+7$ такав да $8k+7 \mid 2^n+1$. Нека је n паран број, $n = 2t$. Тада је $(2^t)^2 = 2^n \equiv -1 \pmod{8k+7}$, па је -1 квадратни остатак по модулу p. С друге стране, важи

$$\left(\frac{-1}{8k+7}\right) = (-1)^{\frac{8k+6}{2}} = -1,$$

што је контрадикција. Нека је сада n непаран број, тј. $n = 2t+1$. Сада је $(2^{t+1})^2 = 2 \cdot 2^n \equiv -2 \pmod{8k+7}$, па је -2 квадратни остатак по модулу p. Како је $\left(\frac{2}{8k+7}\right) = (-1)^{[\frac{8k+8}{4}]} = 1$, а $\left(\frac{-1}{8k+7}\right) = -1$, значи

$$\left(\frac{-2}{11}\right) = \left(\frac{-1}{11}\right)\left(\frac{2}{11}\right) = -1,$$

што је контрадикција. □

Задатак 5.9. *Наћи све природне бројеве* n *такве да* $2^n - 1 \mid 3^n - 1$.

Решење. Очигледно, једно решење је $n = 1$. Претпоставимо да има још решења. Нека је $n > 1$. Јасно је да $2^n - 1$ не сме бити дељиво са 3 ($3 \nmid 3^n - 1$). Како остаци степена двојке при дељењу са 3 образују низ $2, 1, 2, 1, ...$, тј. за парно n важи $3 \mid 2^n - 1$, па закључујемо да је n непаран број. Сада посматрамо остатке при дељењу степена двојке са 12. Они образују низ $2, 4, 8, 2, 8, ...$, па за свако непарно n важи $2^n - 1 \equiv 7 \pmod{12}$. Како $2^n - 1$ може имати просте делиоце облика $12k \pm 5$ и $12k \pm 1$, закључујемо да мора имати бар један облика $12k \pm 5$ зато што би у супротном било $2^n - 1 \equiv \pm 1 \pmod{12}$, што смо видели да није случај. Назовимо такав прост делилац p. Из услова задатка следи $p \mid 3^n - 1$, тј. $3^{n+1} \equiv 3 \pmod{p}$. Како је n непаран број, значи да је 3 квадратни остатак по модулу p. Тада је према закону квадратног реципроцитета $\left(\frac{3}{p}\right)\left(\frac{p}{3}\right) = (-1)^{\frac{3-1}{2}\frac{p-1}{2}}$, одакле следи

$$\left(\frac{p}{3}\right) = (-1)^{\frac{12k\pm5-1}{2}} = \pm 1,$$

с друге стране, како је $p = 12k \pm 5 \equiv \mp 1 \pmod 3$, следи

$$\left(\frac{p}{3}\right) = \left(\frac{\mp 1}{3}\right) = \mp 1,$$

што је контрадикција. □

Задатак 5.10. *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 природнне бројеве a и b који нису дељиви са p важи $p \mid a^2 + b^2$. Тада је

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

закључујемо да је

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

С друге стране важи

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

што је контрадикција. □

Задатак 5.11. *Нека је p прост број облика $4k+3$. Доказати да број $x^2 - x + \frac{p+1}{4}$ нема прост фактор облика $kp-1$.*

Решење. Нека је $x^2 - x + \frac{p+1}{4} \equiv 0 \pmod q$, где је прост број и $q = kp-1$. Тада важи $q \mid (2x+1)^2 + p$, тј. $\left(\frac{-p}{q}\right) = 1$.
С друге стране је

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

□

Задатак 5.12. *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. За $p = 3$, тврђење је тривијално. Посматрајмо случајеве када је $p \geq 5$. Како је $p \mid x^2 - x + 3$ еквивалентно са $p \mid 4(x^2 - x + 3) = (2x-1)^2 + 11$, цео број x постоји ако и само ако је -11 квадратни остатак по модулу p. Слично, уколико $p \mid y^2 - y + 25$, значи $p \mid 4(y^2 - y + 25) = (2y-1)^2 + 99$ што је тачно ако и само ако је -99 квадратни остатак. Како је

$$\left(\frac{-11}{p}\right) = \left(\frac{-11 \cdot 3^2}{p}\right) = \left(\frac{-99}{p}\right),$$

важи тврђење задатка. □

Задатак 5.13. *Одредити све парове природних бројева (x, n) који су решења једначине $x^3 + 2x + 1 = 2^n$.*

Решење. Провером се добија да за $n = 1$ једначина нема решења, а да је за $n = 2$ једино решење $x = 1$. Докажимо да за $n \geq 3$ нема решења. Претпоставимо да је (x, n) решење једначине, где је $n \geq 3$. Како $3 \mid x(x^2 + 2)$, (јер $3 \nmid x \Rightarrow 3 \mid x^2 + 2$), мора бити $2^n \equiv 1 \pmod 3$, па је n паран број. Даље, важи $2^n + 2 = x^3 + 2x + 3 = (x + 1)(x^2 - x + 3)$ и 2^n је потпун квадрат, па следи да је -2 квадратни остатак по сваком непарном простом делиоцу броја $(x + 1)(x^2 - x + 3)$. Тада је

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

одакле следи да је p облика $8k + 1$ или $8k + 3$.
Како је $x^2 - x + 3$ увек непаран број, значи да $x + 1$ мора бити дељив са 2, али не сме бити дељив са 4 ($4 \nmid 2^n + 2$ за $n \geq 2$), па даје остатак 1 или 5 при дељењу са 8. Ако је $x \equiv 1 \pmod 8$, тада је $x^2 - x + 3 \equiv 3 \pmod 8$, па је $(x + 1)(x^2 - x + 3) \equiv 6 \pmod 8$. Међутим, за $n \geq 3$ је $2^n + 2 \equiv 2 \pmod 8$, па добијамо контрадикцију.
Ако је $x \equiv 5 \pmod 8$, тада је $x^2 - x + 3 \equiv 7 \pmod 8$. Сви прости делиоци овог броја не могу бити облика $8k + 1$ или $8k + 3$ јер би онда и сам тај број био облика $8k + 1$ или $8k + 3$. Тако добијамо да је једино решење једначине $(x, n) = (1, 2)$. □

Задатак 5.14. *Доказати да за сваки прост број $p > 5$ постоје два узастопна природна броја која су оба квадратни остаци по модулу p.*

Решење. Уколико је 10 квадратни остатак по модулу p, тада су бројеви $(9, 10)$ тражени пар (како је 9 потпун квадрат он је квадратни остатак по модулу p). Претпоставимо да 10 није квадратни остатак по модулу p. Тада је

$$-1 = \left(\frac{10}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{5}{p}\right),$$

па бар један од бројева 2 или 5 мора бити квадратни остатак по модулу p. Уколико је 2 квадратни остатак по модулу p, тада је $(1, 2)$ тражени пар (1 је квадратни остатак), а ако је 5 квадратни остатак по модулу p, тада је (4,5) тражени пар бројева (4 је квадратни остатак). □

Задатак 5.15. *Нека је n природан број облика $n = 4m^2 + 3$, где $3 \nmid m$. Показати да постоји прост делилац броја n облика $12k + 7$.*

Решење. Нека је p неки прост делилац броја n. Како је n непаран број, значи да ће и p бити такође непаран. Важи $-3 \equiv 4m^2 = (2m)^2 \pmod n$, па је -3 квадратни остатак по модулу n. Тада је по Гаусовом закону реципроцитета

$$1 = \left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}\frac{3-1}{2}} = \left(\frac{p}{3}\right).$$

Како је p непаран прост број, он мора бити облика $3k-1$ или $3k+1$. Нека је p облика $3k-1$. Тада важи $\left(\frac{p}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1$, што је контрадикција, тј. p мора бити облика $3k+1$.
Пошто су сви делиоци броја n непарни, сваки од њих даје или остатак 1 или остатак 3 при дељењу са 4. Ако би сваки прост делилац био конгруентан са 1 по модулу 4, онда би важило $n \equiv 1 \cdot 1 \cdot \cdots \cdot 1 = 1 \pmod 4$, што није тачно како је $n \equiv 3 \pmod 4$. Дакле, мора постојати прост делилац p броја n који задовољава следеће конгруенције

$$p \equiv 1 \pmod 3,$$

$$p \equiv 3 \pmod 4.$$

Посматрајући све остатке које p може давати при дељењу са 12, добијамо да је једино могуће $p \equiv 7 \pmod{12}$, тј. $p = 12k+7$, што је и требало доказати. □

Литература

[1] Бојан Башић,Теорија Бројева, збирка решених задатака, Београд, Нови Сад, 2019.

[2] Владимир Мићић, Зоран Каделбург, Душан Ђукић, Увод у теорију бројева, Београд, 2013.

[3] Зоран Каделбург, Владимир Мићић, Срђан Огњановић, Анализа са алгебром 2, Београд, 2014.

[4] Александар Пејчев, Квадратне конгруенције и Гаусов закон реципроцитета, Београд, 2010.