

Глава 5

КВАДРАТНЕ КОНГРУЕНЦИЈЕ

Квадратне конгруенције по простом модулу

Дефиниција 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 $n = 2, 3, 4$ остаци се називају редом **квадратним, кубним, биквадратним**. Ову главу посвећујемо квадратним остацима.

Јасно је да је приликом решавања једначине $x^2 \equiv a \pmod{m}$ довољно наћи њена решења у скупу $\{0, 1, \dots, m-1\}$, 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 увек ограничавати на таква решења.

ТЕОРЕМА 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.*

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 2. *За сваки непаран прост број p међу бројевима $1, 2, \dots, p-1$ има тачно $\frac{p-1}{2}$ квадратних остатака (и исто толико квадратних неостатака). ■*

Дефиниција 2. За дати прост број p и цео број a , **Лежандров¹ симбол** $\left(\frac{a}{p}\right)$ се дефинише као

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

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

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

У даљем, 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. (Ојлеров критеријум) $a^{p'} \equiv \left(\frac{a}{p}\right) \pmod{p}$.

Доказ. Тврђење је тривијално за $p \mid a$. Зато претпостављамо да $p \nmid a$.

Нека је g примитивни корен по модулу p (он постоји на основу теореме 17 треће главе). Тада је сваки остатак по модулу p задат са g^i , $i = 0, 1, \dots, p-2$ (последница 3 теореме 11 у трећој глави). Приметимо да је $(g^i)^{p'} = g^{ip'} \equiv 1$ ако и само ако $p-1 \mid ip'$, тј. ако и само ако $2 \mid i$.

С друге стране, g^i је квадратни остатак по модулу p ако и само ако постоји $j \in \{0, 1, \dots, p-2\}$ 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 $2 \mid i$, дакле управо онда када је $(g^i)^{p'} \equiv 1 \pmod{p}$. ■

Следећа важна својства Лежандровог симбола следе директно из Ојлеровог критеријума.

ТЕОРЕМА 4. Лежандров симбол је мултипликативан, тј. за све целе бројеве a, b и прост број $p > 2$ важи $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$. ■

¹A.-M. Legendre (1752–1833) француски математичар

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

Решење. Нека је a најмањи квадратни неостатак по модулу p и $b = \left\lceil \frac{p}{a} \right\rceil + 1$. Како је $0 < ab - p < a$, $ab - p$ мора бити квадратни остатак. Дакле,

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

Према томе, b је квадратни неостатак, па је $a \leq b < \frac{p}{a} + 1$ одакле следи тврђење. \triangle

ТЕОРЕМА 5. 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 $p \equiv 1 \pmod{4}$. ■

Задатак 2. Ако је p прост број облика $4k + 1$, доказати да је $x = (p)!$ једно решење конгруенције $x^2 + 1 \equiv 0 \pmod{p}$.

Решење. Множењем релација $i \equiv -(p-i) \pmod{p}$ за $i = 1, 2, \dots, p'$, добијемо $(p')! \equiv (-1)^{p'}(p'+1) \cdots (p-2)(p-1)$. Уочимо такође да је због услова задатка p' паран број. Сада имамо

$$\begin{aligned} x^2 &= (p')!^2 \equiv (-1)^{p'} p' \cdot (p'+1) \cdots (p-2)(p-1) \\ &= (-1)^{p'} (p-1)! \equiv (-1)^{p'+1} = -1 \pmod{p} \end{aligned}$$

на основу Вилсонове теореме. \triangle

Из претходног задатка се такође може извести закључак да је сваки прост делилац броја $x^2 + y^2$ (при чему су $x, y \in \mathbf{N}$ узајамно прости бројеви) или облика $4k + 1$, $k \in \mathbf{N}$, или је једнак 2. Сличан закључак се може проширити.

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 .

Специјално, ако $p \mid x^2 - Dy^2$ и $(x, y) = 1$, онда је D квадратни остатак \pmod{p} .

Доказ. Означимо $N = ax^2 + bxy + cy^2$. Како је $4aN = (2ax + by)^2 - Dy^2$, имамо да је

$$(2ax + by)^2 \equiv Dy^2 \pmod{p}.$$

Даље, y није дељиво са p , јер би у супротном и $2ax + by$, а самим тим и x , било дељиво са p , што противречи претпоставци.

Постоји цео број y_1 такав да је $yy_1 \equiv 1 \pmod{p}$. Множењем горње једнакости са y_1^2 добијемо $(2ax_1 + by_1)^2 \equiv D(y_1)^2 \equiv D \pmod{p}$, одакле следи тврђење. ■

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

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

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 $|r_1|, |r_2|, \dots, |r_{p'}|$ заправо пермутација скупа $\{1, 2, \dots, p'\}$. Тада је $a^{p'} = \frac{a \cdot 2a \cdot \dots \cdot p'a}{1 \cdot 2 \cdot \dots \cdot p'} \equiv \frac{r_1 r_2 \dots r_{p'}}{1 \cdot 2 \cdot \dots \cdot p'}$. Ако сада пишемо $r_k = \varepsilon_k |r_k|$ за $k = 1, \dots, p'$, при чему је $\varepsilon_k = \pm 1$, из Ојлеровог критеријума добијамо да важи

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

Приметимо да је $r_k = -1$ ако и само ако је остатак броја ka при дељењу са p већи од $\frac{p}{2}$, 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 теореме 7 добијамо следеће тврђење.

ТЕОРЕМА 8. (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 9. $\left(\frac{2}{p}\right) = (-1)^{\left[\frac{p+1}{4}\right]}$. 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 показати следећа тврђења.

ТЕОРЕМА 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 $p \equiv \pm 1 \pmod{10}$. ■

Задатак 3. Постоји бесконачно много простих бројева облика: (а) $4k+1$; (б) $10k+9$. Доказати.

Решење. (а) Претпоставимо да оваквих простих бројева има коначно много, и да су p_1, p_2, \dots, p_n сви такви бројеви. Тада су на основу теореме 5 сви прости делиоци броја $N = (2p_1 p_2 \dots p_n)^2 + 1$ облика $4k+1$. Међутим, N није дељив ниједним од p_1, p_2, \dots, p_n , што је контрадикција.

(б) Слично делу под (а), само што се посматра број $N = 5(2p_1 p_2 \dots p_n)^2 - 1$. \triangle

Задатак 4. Доказати да је за $n \in \mathbf{N}$ сваки прост делилац p броја $n^4 - n^2 + 1$ облика $12k+1$.

Решење. Приметимо да је

$$n^4 - n^2 + 1 = (n^2 - 1)^2 + n^2 \quad \text{и} \quad n^4 - n^2 + 1 = (n^2 + 1)^2 - 3n^2.$$

Користећи теореме 5, 6 и 10, из прве једнакости добијамо да је $p \equiv 1 \pmod{4}$, а из друге да је $p \equiv \pm 1 \pmod{12}$. Ове две релације дају $p \equiv 1 \pmod{12}$. \triangle

Задатак 5. Израчунати $\left[\frac{1}{2003} \right] + \left[\frac{2}{2003} \right] + \left[\frac{2^2}{2003} \right] + \dots + \left[\frac{2^{2001}}{2003} \right]$.

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

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

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

До сада разрађена теорија нам још увек не олакшава посао ако треба да проверимо, на пример, да ли је 814 квадратни остатак по модулу 2003. То ће учинити следећа чувена теорема, која омогућава овакву проверу приближно брзином Еуклидовога алгоритма.

ТЕОРЕМА 11. (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 $p' = \frac{p-1}{2}$ и $q' = \frac{q-1}{2}$.

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

ЛЕМА 1. $S(p, q) + S(q, p) = p'q'$.

Доказ. Приметимо да је $\left\lfloor \frac{kp}{q} \right\rfloor$ 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 \mathbf{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 \mathbf{N} унутар правоугаоника $ABCD$ које 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

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

а лако се проверава да је $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$. 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 $\left(\frac{p}{q}\right) = (-1)^{S(p, q)}$. Аналогно је $\left(\frac{q}{p}\right) = (-1)^{S(q, p)}$. Множењем ове две једнакости и коришћењем леме добијамо тражену једнакост. ■

Урадимо сада пример наведен пре теореме.

$$\text{ПРИМЕР 3.} \quad \left(\frac{814}{2003}\right) = \left(\frac{2}{2003}\right) \left(\frac{11}{2003}\right) \left(\frac{37}{2003}\right) = - \left(\frac{11}{2003}\right) \left(\frac{37}{2003}\right).$$

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. \triangle

Једну од могућих корисних формулација закона реципроцитета даје и следећа

ПОСЛЕДИЦА 1. Нека су p и q различити прости бројеви. Ако су p и q оба облика $4k + 3$, онда је једна од једначина

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

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

ПРИМЕР 4. 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. \triangle

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

Решење. Претпоставимо да a није потпун квадрат. Без смањења општости (зашто?) 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, \dots, p_k . За сваки прост број p важи

$$(2) \quad \left(\frac{a}{p}\right) = \prod_{i=1}^k \left(\frac{p_i}{p}\right) \quad \text{и} \quad \left(\frac{p_i}{p}\right) = (-1)^{p_i p'} \left(\frac{p}{p_i}\right).$$

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 $i = 1, 2, \dots, k-1$ и $p \equiv a \pmod{p_k}$, где је a произвољан квадратни неостатак по модулу p_k . Овакав прост број p постоји по Дирихлеовој теорему о простим бројевима у аритметичким прогресијама (глава 2). Тада су на основу (2) бројеви p_1, \dots, 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 $a < 0$. Овај случај препуштамо читаоцу. \triangle

Квадратне конгруенције по сложеном модулу

У многим случајевима је потребно испитати да ли је неки број квадратни остатак по сложеном модулу. У том циљу се уводи функција која у извесном смислу уопштава Лежандров симбол на сложене модуле.

Дефиниција 3. Нека су дати цео број a и непаран број b , и нека је $b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ канонска факторизација броја b . **Јакобијев² симбол** $\left(\frac{a}{b}\right)$ се дефинише као

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

Приметимо да чињеница да Јакобијев и Лежандров симбол имају исту ознаку не доводи до конфузије, јер се очигледно у случају да је b прост број претходна дефиниција своди на дефиницију 2.

Лако је видети да из $\left(\frac{a}{b}\right) = -1$ следи да је a квадратни неостатак по модулу b . Заиста, ако је $\left(\frac{a}{b}\right) = -1$, онда је по дефиницији $\left(\frac{a}{p_i}\right) = -1$ за бар једно $p_i \mid b$, па a није квадратни остатак по модулу p_i .

²К. Г. Ј. Јасоби (1804–1851), немачки математичар

Међутим, обрат *више не важи*, као што се види на следећем примеру.

ПРИМЕР 5. Мада је $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$, 2 није квадратни остатак по модулу 15, јер то није ни по његовим простим чиниоцима 3 и 5. \triangle

Заправо, важи следећи став.

ТЕОРЕМА 12. Нека је a цео и $b = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ (канонска факторизација) 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 свако $i = 1, 2, \dots, r$.

Доказ. Ако је a квадратни остатак по модулу b , очигледно то мора бити и по модулу сваког $p_i^{\alpha_i}$, $i = 1, 2, \dots, r$.

Претпоставимо да је a квадратни остатак по модулу сваког $p_i^{\alpha_i}$, и да је x_i цео број такав да је $x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$. По кинеској теореме о остацима (теорема 3 главе 4) постоји број x такав да је $x \equiv x_i \pmod{p_i^{\alpha_i}}$ за $i = 1, 2, \dots, r$. Тада важи $x^2 \equiv x_i^2 \equiv a \pmod{p_i^{\alpha_i}}$ за свако i , па је зато и $x^2 \equiv a \pmod{b}$. ■

ТЕОРЕМА 13. Квадратних остатака по модулу p^n ($n > 0$) има тачно $\left[\frac{2^{n-1}-1}{3}\right] + 2$ за $p = 2$, односно $\left[\frac{p^{n+1}-1}{2(p+1)}\right] + 1$ за $p > 2$.

Доказ. Означимо са k_n број квадратних остатака по модулу p^n .

Нека је p непарно и $n \geq 2$. Број a је квадратни остатак по модулу p^n ако и само ако $p \nmid a$ и a је квадратни остатак по модулу p , или $p^2 \mid a$ и a/p^2 је квадратни остатак по модулу p^{n-2} . Добијамо једнакост $k_n = k_{n-2} + p'p^{n-1}$.

Нека је $p = 2$ и $n \geq 3$. Број a је квадратни остатак по модулу 2^n ако и само ако $a \equiv 1 \pmod{8}$ или $4 \mid a$ и $a/4$ је квадратни остатак по модулу 2^{n-2} . Добијамо једнакост $k_n = k_{n-2} + 2^{n-3}$.

Сада се тврђење показује директно индукцијом по n . ■

Многа правила која важе за Лежандрове симболе преносе се и на Јакобијеве симболе. Тако важе следећа тврђења, која се доказују коришћењем дефиниције Јакобијевог симбола и аналогних тврђења за Лежандрове симболе, па их дајемо без доказа.

ТЕОРЕМА 14. За све целе бројеве a, b и непарне c, d важе једнакости

$$\left(\frac{a+bc}{c}\right) = \left(\frac{a}{c}\right), \quad \left(\frac{ab}{c}\right) = \left(\frac{a}{c}\right) \left(\frac{b}{c}\right), \quad \left(\frac{a}{cd}\right) = \left(\frac{a}{c}\right) \left(\frac{a}{d}\right). \quad \blacksquare$$

ТЕОРЕМА 15. За сваки непаран цео број a важи

$$\left(\frac{-1}{a}\right) = (-1)^{\frac{a-1}{2}}, \quad \left(\frac{2}{a}\right) = (-1)^{\left[\frac{a+1}{4}\right]}. \quad \blacksquare$$

ТЕОРЕМА 16. (Закон реципроцитета) За свака два узајамно проста непарна броја a, b важи

$$\left(\frac{a}{b}\right) \left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}}. \quad \blacksquare$$

Задатак 7. Доказати да једначина $x^2 = y^3 - 5$ нема решења (x, y) у скупу целих бројева.

Решење. Ако је y парно, тада је $x^2 = y^3 - 5 \equiv 3 \pmod{8}$, што је немогуће.

Нека је сада y непарно. Ако је $y \equiv 3 \pmod{4}$, тада је $x^2 = y^3 - 5 \equiv 3^3 - 5 \equiv 2 \pmod{4}$, опет контрадикција. Према томе, y мора бити облика $4z + 1$, $z \in \mathbf{Z}$. Тада задата једначина постаје

$$x^2 + 4 = 64z^3 + 48z^2 + 12z = 4z(16z^2 + 12z + 3).$$

Следи да је $x^2 \equiv 4 \pmod{16z^2 + 12z + 3}$.

Међутим, вредност Јакобијевог симбола

$$\left(\frac{-4}{16z^2 + 12z + 3} \right) = \left(\frac{-1}{16z^2 + 12z + 3} \right)$$

је једнака -1 јер је $16z^2 + 12z + 3 \equiv 3 \pmod{4}$. Контрадикција. \triangle

Задатак 8. Доказати да $4kxy - 1$ није делилац броја $x^m + y^n$ ни за које природне бројеве x, y, k, m, n .

Решење. Приметимо да је $(x^m, y^n, 4kxy - 1) = 1$. Означимо $m' = [m/2]$ и $n' = [n/2]$. Потребно је испитати следеће могућности.

1° $m = 2m'$ и $n = 2n'$. Тада $4kxy - 1 \mid (x^{m'})^2 + (y^{n'})^2$ по теорему 6 повлачи $\left(\frac{-1}{4kxy - 1} \right) = 1$, што је немогуће.

2° $m = 2m'$ и $n = 2n' + 1$ (случај $m = 2m' + 1$, $n = 2n'$ је аналоган). Тада $4kxy - 1 \mid (x^{m'})^2 + y(y^{n'})^2$, па је $\left(\frac{-y}{4kxy - 1} \right) = 1$. Тврдимо да је то немогуће.

Претпоставимо да је y непарно. По закону реципроцитета је

$$\left(\frac{-y}{4kxy - 1} \right) = \left(\frac{-1}{4kxy - 1} \right) \left(\frac{y}{4kxy - 1} \right) = (-1) \cdot (-1)^{\frac{y-1}{2}} \left(\frac{-1}{y} \right) = -1.$$

Претпоставимо да је $y = 2^t y_1$, при чему је $t \geq 1$ цео број и $y_1 \in \mathbf{N}$. По теорему 15 је $\left(\frac{2}{4kxy - 1} \right) = 1$, док је, као у случају непарног y , $\left(\frac{-y_1}{4kxy - 1} \right) = \left(\frac{-y_1}{4 \cdot 2^t kxy_1 - 1} \right) = -1$. Према томе,

$$\left(\frac{-y}{4kxy - 1} \right) = \left(\frac{2}{4kxy - 1} \right)^t \left(\frac{-y_1}{4kxy - 1} \right) = -1.$$

3° Нека $m = 2m' + 1$ и $n = 2n' + 1$. Тада $4kxy - 1 \mid x(x^{m'})^2 + y(y^{n'})^2$, па је $\left(\frac{-xy}{4kxy - 1} \right) = 1$. С друге стране, $\left(\frac{-xy}{4kxy - 1} \right) = \left(\frac{-4xy}{4kxy - 1} \right) = \left(\frac{-1}{4kxy - 1} \right) = -1$, контрадикција.

Овим су испитани сви случајеви. \triangle

Неке суме Лежандрових симбола

Понекад је потребно одредити број вредности $x \in \{0, 1, \dots, p-1\}$ за које је $f(x)$ квадратни остатак по модулу p , где је p непаран прост број и f полином са целобројним коефицијентима. Одговор на ово питање је директно повезан са вредношћу суме

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

Зато се у овом одељку интересујемо првенствено за суме овог типа.

Ако је f линеаран полином, наведена сума се лако израчунава.

ТЕОРЕМА 17. *За произвољне целе бројеве a, b и прост број $p \nmid a$ важи*

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

Доказ. Због услова $p \nmid a$ бројеви $ax + b$ за $x = 0, 1, \dots, p-1$ чине потпун систем остатака по модулу p . Како је међу њима тачно $\frac{p-1}{2}$ квадратних остатака који нису дељиви са p , тачно $\frac{p-1}{2}$ квадратних неостатака и тачно један дељив са p , следи

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

Да бисмо израчунали тражену суму за квадратне полиноме f , требаће нам следеће тврђење.

ТЕОРЕМА 18. *Нека је $f(x)^{p'} = a_0 + a_1x + \dots + a_{kp'}x^{kp'}$, где је k степен полинома f . Тада важи*

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) \equiv -(a_{p-1} + a_{2(p-1)} + \dots + a_{k'(p-1)}) \pmod{p}, \quad \text{где је } k' = \left[\frac{k}{2} \right].$$

Доказ. Означимо $S_n = \sum_{x=0}^{p-1} x^n$ ($n \in \mathbf{N}$) и $S_0 = p$. Као што је већ доказано у одељку о примитивним коренима, $S_n \equiv -1 \pmod{p}$ за $n > 0$, $p-1 \mid n$, и $S_n \equiv 0 \pmod{p}$ у свим осталим случајевима. Сада је на основу Ојлеровог критеријума

$$\begin{aligned} \sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) &\equiv \sum_{x=0}^{p-1} f(x)^{p'} = \sum_{i=0}^{kp'} a_i S_i \\ &\equiv -(a_{p-1} + a_{2(p-1)} + \dots + a_{k'(p-1)}) \pmod{p}. \blacksquare \end{aligned}$$

ТЕОРЕМА 19. *За целе бројеве a, b, c и прост број $p \nmid a$, сума*

$$\sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p} \right)$$

је једнака $-\left(\frac{a}{p}\right)$ ако $p \nmid b^2 - 4ac$, и $(p-1)\left(\frac{a}{p}\right)$ ако $p \mid b^2 - 4ac$.

Доказ. Имамо да је $\left(\frac{4a}{p}\right) \sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{(2ax + b)^2 - D}{p}\right)$, где је $D = b^2 - 4ac$. Како бројеви $ax + b$ за $x = 0, 1, \dots, p-1$ чине потпун систем остатака по модулу p , добијамо

$$\left(\frac{a}{p}\right) \sum_{x=0}^{p-1} \left(\frac{ax^2 + bx + c}{p}\right) = \sum_{x=0}^{p-1} \left(\frac{x^2 - D}{p}\right) = S.$$

По теореме 18 је $S \equiv -1 \pmod{p}$, па како је $|S| \leq p$, следи $S = -1$ или $S = p-1$.

Претпоставимо $S = p-1$. Тада су $p-1$ $\left(\frac{x^2-D}{p}\right)$ -ова једнаки 1, док је тачно један, рецимо за $x = x_0$, једнак 0, тј. $p \mid x_0^2 - D$. Како такође $p \mid (-x_0)^2 - D = x_0^2 - p$, мора бити $x_0 = 0$ одакле $p \mid D$. Обратно, ако $p \mid D$, важи $S = p-1$, док је у супротном $S = -1$, па тврђење следи. ■

Задатак 9. Број решења (x, y) конгруенције $x^2 - y^2 \equiv D \pmod{p}$, за $p \nmid D$, једнак је $p-1$. Доказати.

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

Одређивање сума Лежандрових симбола за полиноме $f(x)$ степена већег од 2 је знатно сложеније. У наставку ћемо испитати случај полинома f степена 3 одређеног типа.

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 добијамо да је за свако $t \in \mathbf{Z}$, $K(at^2) = \left(\frac{t}{p}\right) \sum_{x=0}^{p-1} \left(\frac{\frac{x}{t} \left(\left(\frac{x}{t}\right)^2 + a\right)}{p}\right) = \left(\frac{t}{p}\right) K(a)$. Према томе, $|K(a)|$ зависи само од тога да ли је a квадратни остатак по модулу p или није.

Сада дајемо нови доказ тврђења да је сваки прост број $p \equiv 1 \pmod{4}$ збир два квадрата.

ТЕОРЕМА 20. 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

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

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 $K(0) = 0$. Нађимо $\sum_{n=0}^{p-1} K(n)^2$. За свако n је

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

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

Приметимо да је по теорему 19, $\sum_{n=0}^{p-1} \left(\frac{(n+x^2)(n+y^2)}{p} \right)$ једнако $p-1$ ако $x = \pm y$, и -1 у осталим случајевима. Убацавањем ових вредности горња једнакост постаје

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

Закључујемо да је $K(a)^2 + K(b)^2 = 4p$. Штавише, пошто је $K(a)^2 + K(b)^2$ дељиво са 4, оба $K(a)$ и $K(b)$ морају бити парни, што доказује тврђење. ■

Лагранжова теорема

У задатку 2 и напомени после тог задатка видели смо да је неопходан услов да би природан број N могао да се представи као збир $x^2 + y^2$, где је $(x, y) = 1$, тај да су му сви непарни прости делиоци облика $4k+1$. Другим речима, бројеви N који имају бар један прост делилац облика $4k+3$ не могу се приказати у облику збира два квадрата узajамно простих бројева. Слично, има природник бројева (такав је, на пример, број 7) који се не могу написати ни као збир квадрата три цела броја. Међутим, за збир од четири квадрата важи следећа **Лагранжова**³ **теорема**.

ТЕОРЕМА 21. Сваки природан број се може представити као збир четири квадрата целих бројева.

Доказ. Тврђење следи комбинацијом наредних лема 2 и 4.

ЛЕМА 2. За реалне бројеве a_i, b_i ($i = 1, 2, 3, 4$) важи

$$(a_1^2 + a_2^2 + a_3^2 + a_4^2)(b_1^2 + b_2^2 + b_3^2 + b_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2$$

за $c_1 = a_1b_1 + a_2b_2 + a_3b_3 + a_4b_4$, $c_2 = a_1b_2 - a_2b_1 + a_3b_4 - a_4b_3$, $c_3 = a_1b_3 - a_3b_1 + a_4b_2 - a_2b_4$, $c_4 = a_1b_4 - a_4b_1 + a_2b_3 - a_3b_2$. ■

ЛЕМА 3. За сваки непаран прост број p постоје цели бројеви m, x_0 и y_0 такви да је

$$1 \leq m < \frac{p}{2} \quad \text{и} \quad x_0^2 + y_0^2 + 1 = pm.$$

³J. L. Lagrange (1736–1813), француски математичар

Доказ. Лако се проверава (као у теоремама 1 и 2) да међу бројевима

$$(3) \quad 0^2, 1^2, 2^2, \dots, \left(\frac{p-1}{2}\right)^2$$

не постоје два која су конгруентна по модулу p . Исто онда важи за бројеве

$$(4) \quad -1, -1-1^2, -1-2^2, \dots, -1-\left(\frac{p-1}{2}\right)^2.$$

Међутим, бројева (3) и (4) има укупно $p+1$, те постоје два (један из једног а други из другог скупа) који су конгруентни по модулу p , тј. постоје $x_0, y_0 \in \mathbf{Z}$, $0 \leq x_0, y_0 \leq \frac{p-1}{2}$, такви да је $x_0^2 \equiv -1 - y_0^2 \pmod{p}$, тј. $x_0^2 + y_0^2 + 1 = pt$, при чему је

$$m = \frac{1}{p}(x_0^2 + y_0^2 + 1) \leq \frac{1}{p} \left[\left(\frac{p-1}{2}\right)^2 \cdot 2 + 1 \right] = \frac{p^2 - 2p + 3}{2p} < \frac{p}{2}. \quad \blacksquare$$

ЛЕМА 4. Сваки прост број се може представити као збир четири квадрата целих бројева.

Доказ. За $p = 2$ тврђење очигледно важи. Нека је даље p непаран прост број. На основу леме 3 постоји $m \in \mathbf{Z}$, $1 \leq m < \frac{p}{2}$, тако да је $mp = x_0^2 + y_0^2 + 1^2 + 0^2$, тј. број mp се може приказати као збир четири квадрата. Нека је m_0 најмањи број за који постоји представљање облика

$$(5) \quad m_0 p = a_1^2 + a_2^2 + a_3^2 + a_4^2, \quad 1 \leq m_0 < \frac{p}{2}.$$

Докажимо да је $m_0 = 1$, тј. да се p може представити на захтевани начин.

Најпре докажимо да је m_0 непаран. Када би он био паран, $m_0 = 2m'$, тада би међу бројевима a_1, a_2, a_3, a_4 морало да буде паран број (0, 2 или 4) непарних, па би се они могли нумерисати тако да $2 \mid a_1 \pm a_2$ и $2 \mid a_3 \pm a_4$. Но, онда је

$$m'p = \frac{1}{2}(a_1^2 + a_2^2 + a_3^2 + a_4^2) = \left(\frac{a_1 + a_2}{2}\right)^2 + \left(\frac{a_1 - a_2}{2}\right)^2 + \left(\frac{a_3 + a_4}{2}\right)^2 + \left(\frac{a_3 - a_4}{2}\right)^2,$$

па број m' задовољава исте услове као m_0 , а мањи је од њега.

Нека су сада r_i остаци при дељењу a_i са m_0 , и то најмањи по модулу, тј. $|r_i| < \frac{m_0}{2}$ (m_0 је непаран!). Тада је $r_1^2 + r_2^2 + r_3^2 + r_4^2 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m_0}$, тј.

$$(6) \quad r_1^2 + r_2^2 + r_3^2 + r_4^2 = m_0 t,$$

где је $0 \leq t = \frac{1}{m_0}(r_1^2 + r_2^2 + r_3^2 + r_4^2) < \frac{1}{m_0} \cdot 4 \left(\frac{m_0}{2}\right)^2 = m_0$. Множењем релација

(5) и (6) и користећи лему 2 добијамо

$$m_0^2 p t = (a_1^2 + a_2^2 + a_3^2 + a_4^2)(r_1^2 + r_2^2 + r_3^2 + r_4^2) = c_1^2 + c_2^2 + c_3^2 + c_4^2,$$

где је, на пример, $c_1 = a_1 r_1 + a_2 r_2 + a_3 r_3 + a_4 r_4 \equiv a_1^2 + a_2^2 + a_3^2 + a_4^2 \equiv 0 \pmod{m_0}$ и слично за c_2, c_3 и c_4 . При том је

$$pt = \left(\frac{c_1}{m_0}\right)^2 + \left(\frac{c_2}{m_0}\right)^2 + \left(\frac{c_3}{m_0}\right)^2 + \left(\frac{c_4}{m_0}\right)^2,$$

где су c_i/m_0 цели бројеви. На основу начина избора броја m_0 следи $t = 0$, па и $r_i = 0$, односно $a_i \equiv 0 \pmod{m_0}$. Но, онда је $m_0^2 \mid a_1^2 + a_2^2 + a_3^2 + a_4^2 = m_0 p$, па $m_0 \mid p$. Због $1 \leq m_0 < \frac{p}{2}$, то је могуће једино за $m_0 = 1$, што је требало доказати. ■

З А Д А Ц И

10. (P95.2.2) Нека је p прост број. Доказати да постоји $x \in \mathbf{Z}$ такво да $p \mid x^2 - x + 3$ ако и само ако постоји $y \in \mathbf{Z}$ такво да $p \mid y^2 - y + 25$.

11. Нека је $p = 4k - 1$ прост број, $k \in \mathbf{N}$. Ако је a цео број такав да конгруенција $x^2 \equiv a \pmod{p}$ има решења, доказати да су та решења дата са $x = \pm a^k$.

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

13. Доказати да за сваки прост број p постоје цели бројеви a, b за које је $a^2 + b^2 + 1$ дељиво са p .

14. Доказати да $\frac{x^2 + 1}{y^2 - 5}$ није цео број ни за које природне бројеве $x, y > 2$.

15. Нека је $p > 3$ прост број и $a, b \in \mathbf{N}$ такви да је $1 + \frac{1}{2} + \dots + \frac{1}{p-1} = \frac{a}{b}$. Доказати да тада $p^2 \mid a$.

16. Нека је $P(x) = x^3 + 14x^2 - 2x + 1$. Доказати да постоји природан број n такав да за свако $x \in \mathbf{Z}$,

$$101 \mid \underbrace{P(P(\dots P(x)\dots))}_n - x.$$

17. (C97.3--4.1) Наћи све $n \in \mathbf{N}$ такве да се скуп $A = \{n, n+1, \dots, n+1997\}$ може разложити на неколико подскупова са једнаким производима елемената.

18. (а) Доказати да ни за које $x, y \in \mathbf{N}$ број $4xy - x - y$ није потпун квадрат;

(б) Доказати да ни за које $x, y, z \in \mathbf{N}$ број $4xyz - x - y$ није потпун квадрат.

19. Доказати да су за $n \in \mathbf{N}$ сви прости делиоци броја $n^8 - n^4 + 1$ облика $24k + 1$, $k \in \mathbf{N}$.

20. Ако су m, n такви природни бројеви да је $\varphi(5^m - 1) = 5^n - 1$, доказати да је $(m, n) > 1$.

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

22. Доказати да је за свако $a \in \mathbf{Z}$ број решења (x, y, z) конгруенције $x^2 + y^2 + z^2 \equiv 2axyz \pmod{p}$ једнак $(p + (-1)^{p'})^2$.