Математичка гимназија
Београд, 11. и 12. 3. 2014.
Припреме за државно такмичење (а и после)
Предавач: Стеван Гајовић

Квадратне конгруенције

Дефиниције, сновна својства и теореме:

Дефиниција 1. Нека су a и m цели бројеви. Број a називамо *квадратним остатком по модулу* m, ако конгруенција $x^2 \equiv a \pmod{m}$ има решења у $\mathbb{Z}$, у супроном, број a називамо *квадратним неостатком по модулу* m.

Дефиниција 2. Нека је p прост број, $p \neq 2$, и a цео број, $p \nmid a$. *Лежандров симбол* се дефинише са

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & , \quad a \text{ је квадратни остатак} \\ -1 & , \quad a \text{ је квадратни неостатак.} \end{cases}$$

Напомена: Понекад се дефинише и $\left(\frac{a}{p}\right) = 0$, ако $p \mid a$.

Дефиниција 3. Нека су a и n узајамно прости цели бројеви, n непаран, и нека је канонска факторизација броја $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$. *Јакобијев симбол* се дефинише са

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdot \left(\frac{a}{p_2}\right)^{\alpha_2} \cdot \ldots \cdot \left(\frac{a}{p_k}\right)^{\alpha_k}.$$

Теорема 1. Ако је p прост број, $p \neq 2$, и ако је a квадратни остатак по модулу p, $p \nmid a$ онда конгруенција $x^2 \equiv a \pmod{p}$ има тачно два решења.

Теорема 2. Ако је p прост број, $p \neq 2$, онда међу бројевима из скупа $\{1, 2, \ldots, p-1\}$ постоји тачно $\frac{p-1}{2}$ квадратних остатака и то су остаци које дају бројеви 1^2, 2^2, ... , $\left(\frac{p-1}{2}\right)^2$.

Теорема 3. *(Ојлер)* Нека је p прост број, $p \neq 2$, и нека је a цео број, $p \nmid a$. Тада је

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

Специјално: Нека је p прост број, $p \neq 2$. Тада је

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

Другим речима, -1 је квадратни остатак по модулу p, ако и само ако је p облика $4k+1$, за $k \in \mathbb{N}$.

Теорема 4. Нека је p прост број, $p \neq 2$, и нека су a и b цели бројеви, $p \nmid a$, $p \nmid b$. Тада $a \equiv b \pmod{p}$ повлачи

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

Теорема 5. Нека је p прост број, $p \neq 2$, и нека је c цео број, $p \nmid c$. Тада је

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

Теорема 6. Нека су a и b цели бројеви и p прост број $p \neq 2$, $p \nmid ab$. Тада је

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

Теорема 7. (*Гаусова лема*) Нека је p прост број, $p \neq 2$, и нека је a цео број, $p \nmid a$. Ако је μ број негативних остатака међу најмањим по апсолутној вредности остацима бројева a, $2a$, ... , $\frac{p-1}{2}a$ по модулу p, онда је

$$\left(\frac{a}{p}\right) \equiv (-1)^{\mu}.$$

Теорема 8. Нека је p прост број, $p \neq 2$. Тада је

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

Теорема 9. (*Закон квадратног реципроцитета*) Ако су p и q прости бројеви $p \neq q$, $p, q \neq 2$, онда је

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

Напомена: Аналогна својства важе и за Јакобијеве симболе (када су лепо дефинисани).

Задаци:

Уводни задаци - за вежбу
(важно је упамтити бар идеје како се раде)

1. Проверити да ли следеће једначине имају решења:
а) $x^2 \equiv 3 \pmod{11}$;
б) $x^2 \equiv 13 \pmod{19}$;
в) $x^4 \equiv -1 \pmod{53}$.

2. Израчунати
а) $\left(\frac{350}{2011}\right)$;
б) $\left(\frac{858}{2011}\right)$;
в) $\left(\frac{1001}{1111111111111}\right)$, ако знамо да је 1111111111111 прост број.

3. Извести по којим простим модулима су -2, 3, -3, 13 квадратни остаци.

4. Доказати да је за свако $n \in \mathbb{N}$ сваки непаран прост делилац броја n^2+1 облика $4k+1$.

5. Доказати да је за свако $n \in \mathbb{N}$ сваки делилац броја n^4-n^2+1 облика $12k+1$.

6. Доказати да је за свако $n \in \mathbb{N}$ сваки делилац броја n^8-n^4+1 облика $24k+1$.

7. Ако за природне бројеве a, b, c, који су међусобно узајамно прости, важи $a^2-ab+b^2=c^2$, онда је сваки прост делилац броја c облика $6k+1$.

8. Нека је p прост број. Доказати да постоји цео број x такав да $p \mid x^2-x+3$ ако и само ако постоји цео број y, такав да $p \mid y^2+y+25$.

9. **(теорема-задатак)** Нека су x и y узајамно прости цели бројеви и $a, b, c \in \mathbb{Z}$, произвољни. Ако је p непаран прост број, такав да $p \nmid abc$ и $p \mid ax^2+bxy+cy^2$, тада је $D=b^2-4ac$ квадратни остатак по модулу p.

10. Ако $p \mid x^2-Dy^2$, при чему су x и y узајамно прости цели бројеви, тада је D квадратни остатак по модулу p.

11. Нека је p прост број облика $4k-1$, и a цео број, такав да је квадратни остатак по модулу p. Доказати да су онда решења једначине $x^2 \equiv a \pmod{p}$ дата са $\pm a^k$.

12. Доказати да за сваки природан број n, постоји бесконачно много простих бројева p, тако да су бројеви ± 1, ± 2, ... , $\pm n$ квадратни остаци по модулу p.

13. Доказати да је збир свих различитих квадратних остатака по простом модулу $p > 3$ дељив са p.

14. Доказати да за сваки прост број p, постоје цели бројеви a и b, такви да $p \mid a^2 + b^2 + 1$.

15. Доказати да је 16 остатак осмог степена по сваком непарном простом модулу.

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

17. Ако је низ дефинисан са $x_1 = 1111$, $x_{n+1} = 2x_n^2 - 1$, доказати да за ни један од бројева 2011, 2012, 2013, 2014, 2015 не важи да дели неки члан овог низа.

18. Дати су природни бројеви за које важи $\sqrt{7} - \dfrac{m}{n} > 0$. Доказати да важи $\sqrt{7} - \dfrac{m}{n} > \dfrac{1}{mn}$.

19. Природни бројеви a и b су такви да су и $15a + 16b$ и $16a - 15b$ потпуни квадрати. Колику најмању вредност може узети мањи од та два квадрата?

20. Нека је p прост број облика $4k + 1$.

а) Доказати да је $x = \left(\dfrac{p-1}{2}\right)!$ решење једначине $x^2 + 1 \equiv 0 \pmod{p}$;

б) **(Туова теорема)** За сваки природан број n и сваки цео број a, такав да $(a, n) = 1$, постоје природни бројеви $x, y \leq \sqrt{n}$, такви да $xa \equiv \pm y \pmod{n}$, за одговарајући избор знака + или −;

в) Доказати да постоје природни бројеви a и b, тако да је $p = a^2 + b^2$.

г) Доказати да се природан број n може представити као збир 2 квадрата ако и само ако за сваки q прост фактор броја n, $q \equiv 3 \pmod{4}$, важи да $q^{2l} \parallel n$, за неко $l \in \mathbb{N}$.

21. Доказати да за свако $n \in \mathbb{N}$ постоји n узастопних природних бројева, таквих да међу њима не постоји број који може да се запише као збир два квадрата.

22. Доказати да ако за природан број m важи да се за сваки природан број n број $n^2 + m$ може записати као збир два квадрата, онда то важи и за m.

23. **(теорема-задатак)** Доказати да је a квадратни остатак по модулу p^k ако и само ако је a квадратни остатак по модулу p, где је p непаран прост број.

24. **(теорема-задатак)** Нека је a цео број и нека је $b = p_1^{k_1} p_2^{k_2} \ldots p_l^{k_l}$ факторизација на просте факторе природног броја b. Тада је a квадратни остатак по модулу b ако и само ако је a квадратни остатак по сваком модулу $p_i^{k_i}$, за $1 \leq i \leq l$.

25. **(теорема-задатак)** Нека је p прост број и n природан број. Квадратних остатака по модулу p^n (рачунајући све, и оне који нису узајамно прости са p^n) има тачно $\left[\dfrac{2^{n-1} - 1}{3}\right] + 2$, ако је $p = 2$, односно $\left[\dfrac{p^{n+1} - 1}{2(p+1)}\right] + 1$, ако је p непаран.

Једначине и дељивости

26. Доказати да ни за један прост број p, број $3^p + 7p - 4$ не може бити потпун квадрат.

27. Наћи све природне бројеве за које важи $4 \mid a + b$ и $a^2 - 2a = b^2 + c^2$.

28. Доказати да једначина $x^4 = y^2 + z^2 + 4$ нема решења у скупу целих бројева.

29. Доказати да једначина $x^2 = 2y^2 z + 3z + 2$ нема решења у скупу $\mathbb{Z}$.

30. Одредити све парове природних бројева (x, y) за које је $\dfrac{x^2 + y^2}{x - y}$ природан број и дели 1995.

31. Одредити све парове целих бројева (x, y), за које $y^2 - 5 \mid x^2 + 1$.

32. Доказати да ни за које природне бројеве x, y, z, m и n број $4xyz - 1$ не дели $x^m + y^n$.

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

34. Доказати да ни за које природне бројеве x и y и z, број $4xyz - x - y$ није потпун квадрат.

35. Да ли једначина $x^3 + 2014x - y^2 = 1$ има решења у скупу целих бројева?

36. Одредити све тројке природних бројева (x, y, z), $x \leq y \leq z$, такве да $x^3(y^3 + z^3) = 2012(xyz + 2)$.

37. Доказати да једначина $y^5 - x^2 = 4$ нема решења у скупу $\mathbb{Z}$.

38. Доказати да једначина $x^2 = y^3 - 5$ нема решења у скупу $\mathbb{Z}$.

39. Доказати да једначина $y^3 = x^2 + 80$ нема решења у скупу $\mathbb{Z}$.

40. Одредити сва целобројна решења једначине $x^3 + 3 = 4y(y + 1)$.

41. Одредити сва решења једначине $x^2 = y^z - 3$ у скупу $\mathbb{N}$, при чему $4 \nmid z - 1$.

42. Решити у скупу целих бројева $x^2 = y^7 + 7$.

43. Нека је p прост број облика $4k+3$. Ако постоје цели бројеви x, y, z и t, такви да $x^{2p}+y^{2p}+z^{2p} = t^{2p}$, доказати да p мора делити бар једног од x, y, z.

44. Решити једначину у скупу целих бројева $12^x + y^4 = 2008^z$.

45. Решити једначину у скупу природних бројева $x^3 + 2x + 1 = 2^n$.

Суме Лежандрових симбола

46. **(теорема-задатак)** Ако су p прост број и a и b цели бројеви, при чему $p \nmid a$, тада је $\sum_{x=0}^{p-1} \left(\frac{ax+b}{p} \right) = 0$.

47. **(теорема-задатак)** За $f(x)$ полином k-тог степена је $f(x)^{\frac{p-1}{2}} = a_0 + a_1 x + ... + a_{k\frac{p-1}{2}} x^{k\frac{p-1}{2}}$. Тада је:

$$\sum_{x=0}^{p-1} \left(\frac{f(x)}{p} \right) \equiv -(a_{p-1} + a_{2(p-1)} + ... + a_{[\frac{k}{2}](p-1)}) \pmod{p}.$$

48. **(теорема-задатак)** За целе бројеве a, b и c, при чему $p \nmid a$ важи:

$$\sum_{x=0}^{p-1} \left(\frac{ax^2+bx+c}{p} \right) = \begin{cases} -\left(\frac{a}{p}\right), & p \nmid b^2 - 4ac \\ (p-1)\left(\frac{a}{p}\right), & p \mid b^2 - 4ac \end{cases}$$

49. За целобројни полином $f(x) = ax^2+bx+c$ и непаран прост број p важи да постоји $2p-1$ узастопних целих бројева у којима је вредност f потпун квадрат. Доказати да $p \mid b^2 - 4ac$.

50. Одредити број узастопних квадратних остатака по модулу p, где је p непаран прост број, тј. број елемената скупа $\{0 \leq n \leq p-2 | \left(\frac{n}{p}\right) = \left(\frac{n+1}{p}\right) = 1\}$.

51. Нека је $p > 3$ прост број и нека је k било који цео број. Доказати да постоји природан број n, такав да $\left(\frac{n}{p}\right) = \left(\frac{n+k}{p}\right)$.

52. Одредити број решења (x, y) конгруенције $x^2 - y^2 \equiv D \pmod{p}$, за $p \nmid D$, прост број.

53. Одредити број решења једначине $ax^2 + by^2 \equiv 1 \pmod{p}$ за p прост број и $a, b \in \mathbb{Z}$, такве да $p \nmid ab$.

54. Нека су p и q различити прости бројеви. Доказати:

$$\sum_{x_1+x_2+\cdots+x_q \equiv q \pmod{p}, 1 \leq x_i \leq p-1} \left(\frac{x_1 \cdot x_2 \cdots x_q}{p}\right) \equiv 1 \pmod{q}.$$

55. За природан број k и прост p доказати $1+\sum_{x=0}^{p-1}\left(\frac{x^4+k}{p}\right)=\sum_{x=0}^{p-1}\left(\frac{x(x^2+k)}{p}\right)$.

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

57. Доказати да за прост број p, $p\equiv 3 \pmod 4$ важи: $\sum_{k=1}^{p-1}k^2\left(\frac{k}{p}\right)=p\sum_{k=1}^{p-1}k\left(\frac{k}{p}\right)$.

58. Нека је $p=8k+3$ прост број. Доказати $\sum_{i=1}^{2k}\left(\frac{i}{p}\right)=0$.

59. Нека је p прост број. Посматрајмо полином $f(x)=\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)x^{i-1}$. Знамо: $(x-1)\mid f(x)$.

а) Доказати да $(x-1)^2$ дели $f(x)$ ако и само ако је p облика $4k+1$.
б) Доказати да за p облика $8k+5$, $(x-1)^3$ не дели $f(x)$.

60. Ако је $q=2h+1$ прост број, такав да $q\equiv 7 \pmod 8$, доказати $\sum_{r=1}^{h}r\left(\frac{r}{q}\right)=0$.

61. За сваки цео број a дефинишимо $K(a)=\sum_{x=0}^{p-1}\left(\frac{x(a+x^2)}{p}\right)$.

а) Доказати да за свако $t\in\mathbb{Z}$ важи $K(at^2)=\left(\frac{t}{p}\right)K(a)$.
б) Ако је a квадратни остатак, а b квадратни неостатак по модулу p, где је p прост број облика $4k+1$, доказати да су $K(a)$ и $K(b)$ парни бројеви за које важи:

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

62. (Иран 2013.) Нека је $p=3k+1$ прост број. Дефинишимо функцију $L:\mathbb{Z}/p\mathbb{Z}\longrightarrow\mathbb{Z}$ на следећи начин: $L(m)=\sum_{x\in\mathbb{Z}/p\mathbb{Z}}\left(\frac{x(x^3+m)}{p}\right)$. Доказати:

а) За свако $m\in\mathbb{Z}/p\mathbb{Z}$ и $t\in(\mathbb{Z}/p\mathbb{Z})^*$, $t\neq 0$ је $L(mt^3)=L(m)$.
б) Постоји партиција $(\mathbb{Z}/p\mathbb{Z})^*=A\bigsqcup B\bigsqcup C$, тако да је $|A|=|B|=|C|=\frac{p-1}{3}$, тако да је L константна на сваком скупу, тј. да постоје цели бројеви a, b и c тако да важи: $L(x)=\begin{cases}a, & x\in A\\ b, & x\in B\\ c, & x\in C\end{cases}$
в) $a+b+c=-3$.
г) $a^2+b^2+c^2=6p+3$.
д) Ако је $X=\frac{2a+b+3}{3}$ и $Y=\frac{b-a}{3}$, X и Y су цели бројеви и важи $p=X^2+XY+Y^2$.

Разни задаци

63. Израчунати $\left[\frac{1}{2011}\right]+\left[\frac{2}{2011}\right]+\left[\frac{2^2}{2011}\right]+...+\left[\frac{2^{2009}}{2011}\right]$.

64. За $p\equiv 1 \pmod 4$, прост број, израчунати $\sum_{k=1}^{p-1}\left(\left[\frac{2k^2}{p}\right]-2\left[\frac{k^2}{p}\right]\right)$.

65. Доказати да постоји природан број $a<\sqrt{p}+1$, који је квадратни неостатак по простом модулу p.

66. Ако за природан број n и сваки прост број p важи $\left(\frac{n}{p}\right)=1$, тада је n потпун квадрат. Доказати да ако n није потпун квадрат, постоји бесконачно простих бројева тако да $\left(\frac{n}{p}\right)=-1$.

67. Одредити све природне бројеве n, за које постоји n природних бројева a_1, a_2, ... , a_n таквих да је $a_1^k + a_2^k + ... + a_n^k$ потпун квадрат за свако $k \in \mathbb{N}$.

68. Нека је $f(x) = ax^2 + bx + c$, целобројни полином, такав да за сваки прост број p постоји цео број m, такав да $p \mid f(m)$. Доказати да f има рационалне корене.

69. Нека је p прост број облика $4k + 3$. Доказати да број $x^2 - x + \dfrac{p+1}{4}$ не може имати прост фактор облика $kp - 1$.

70. Доказати да за било који природан рбој n, број $3^n + 2$ нема прост фактор облика $24k + 13$.

71. Доказати да ни за које $n \in \mathbb{N}$, број $2^n + 1$ не може имати прост фактор облика $8k - 1$.

72. Доказати да за сваки $n \in \mathbb{N}$, број $2^{3^n} + 1$ има бар n различитих простих делилаца облика $8k + 3$.

73. Доказати да постоји бесконачно много парова узастопних природних бројева $(n, n+1)$, тако да ни n ни $n + 1$ немају прост фактор облика $4k - 1$.

74. Одредити број и решења конгруенције $x^2 + (x + 1)^2 \equiv 0 \pmod{1997}$.

75. Број p је непаран прост број и A и B су подскупови скупа $\{1, 2, ..., p - 1\}$ који задовољавају:
а) $A \cup B = \{1, 2, ..., p - 1\}$;
б) За било које a, b из истог скупа (A или B) $ab \pmod{p} \in A$;
в) За било које $a \in A$ и $b \in B$ је $ab \in B$.
Одредити све овакве скупове A и B.

76. Одредити све природне бројеве n за које $2^n - 1 \mid 3^n - 1$.

77. Ако је $p = 4n + 1$ прост број, доказати да тада за сваки делилац d броја n важи да је d квадратни остатак по модулу p.

78. Ако су a и b природни бројеви за које је $a^2 + b^2 = p$, где је p прост број облика $4k + 1$, и ако је a непаран, доказати да је a квадратни остатак по модулу p.

79. Нека је p непаран прост број, и a, b и c цели бројеви, $a > 0$ и $(a, 2p) = 1$.
а) Ако је $a^2 = 4b^2p^2 + c^2$, доказати да је a квадратни остатак по модулу p;
б) Ако је $a^2 = b^2p^2 + 4c^2$, доказати да је $2a$ квадратни остатак по модулу p.

80. Нека је $(a_n)_{n\in\mathbb{N}}$ низ целих бројева, задат са $a_n = n^6 + 5n^4 - 12n^2 - 36$. Доказати да сваки прост број дели неки члан тог низа, али и да постоји природан број који не дели ни један члан овог низа.

81. Одредити најмањи прост број који дели $n^2 + 5n + 23$, за неки природан број n.

82. Нека је f_n n-ти члан Фибоначијевог низа и $p > 5$ прост број. Доказати $f_p \equiv \left(\dfrac{p}{5}\right) \pmod{p}$.

83. Нека је m природан број чији су сви прости фактори облика $10k \pm 1$. Доказати да постоје природни бројеви a и b, такви да сваки члан низа $x_0 = a$, $x_1 = b$, $x_{n+2} = x_{n+1} + x_n$ је узајамно прост са m.

84. Нека је n природан број, такав да $n \mid 2^n + 2$.
а) Доказати да је $n = 1$ или је n паран;
б) Одредити неко $n < 100$ и неко $n > 100$ за које ово важи.

85. Ако за природан број n важи $\sigma(n) = 2n + 1$, доказати да је n квадрат непарног природног броја.

86. У зависности од непарног природног броја n, одредити остатак производа свих бројева мањих од n, који су узајамно прости са n, при дељењу са n.

87. Да ли постоји неко природан број n, за који се скуп $\{n, n+1, ..., n+1997\}$ може поделити у неколико подскупова, тако да је сви поскупови имају исти производ елемената?

88. Нека је p непаран прост број и означимо са A_p скуп свих ненула квадратних остатака и B_p скуп свих квадратних неостатака по модулу p. Нека је $\xi \in \mathbb{C}$ примитивни p-ти корен из 1 ($\xi^p = 1$ и $\xi^k \neq 1$,

за $0 < k < p$). Тада су $\alpha = \sum_{k \in A_p} \xi^k$ и $\beta = \sum_{k \in B_p} \xi^k$ корени једначине $x^2 + x + \dfrac{1 - p\left(\dfrac{-1}{p}\right)}{4}$.

89. Нека је $p \geq 5$ прост број. Означимо $p' = \dfrac{p-1}{2}$. Нека су a_1, a_2, ... , $a_{p'}$ цели бројеви. Доказати да постоје $\lambda_i \in \{-1, 0, 1\}$, за $1 \leq i \leq p'$, такви да $p \mid \lambda_1 a_1^2 + \lambda_2 a_2^2 + ... + \lambda_{p'} a_{p'}^2$.

90. Функције $f, g : \mathbb{N} \longrightarrow \mathbb{N}$ задовољавају следећа својства:
а) $2f(n)^2 = g(n)^2 + n^2$, за све $n \in \mathbb{N}$;
б) $|f(n) - n| \leq 2014\sqrt{n}$, за све $n \in \mathbb{N}$.
Доказати да онда g има бесконачно фиксних тачака (тј. $m \in \mathbb{N}$ тако да $g(m) = m$).

91. Нека је n фиксиран природан број. Доказати да постоји природан број n са следећим својстима:
(1) $6 \mid p + 1$;
(2) $p \nmid n$;
(3) $n \equiv m^3 \pmod{p}$, за неки број $m \in \{1, 2, ..., p-1\}$.

92. Нека је p прост број такав да је $p = a^2 + 5b^2$, за непаран број a и a и b су природни бројеви. Доказати да је a квадратни остатак по модулу p ако и само ако је $p \equiv 1 \pmod{5}$.

93. Ако за низ x_n природних бројева за свако $n > 1$ важи $x_n = x_1^2 + x_2^2 + ... + x_{n-1}^2$ и $2006 \mid x_{2006}$, одредити минималну вредност коју може имати x_1.

94. Доказати да постоје стого растући низови a_n и b_n за које за свако n важи $a_n(a_n + 1) \mid b_n^2 + 1$.

95. Одредити све природне бројеве n, за које постоји природан број m, тако да $2^n - 1 \mid m^2 + 9$.

96. Природни бројеви a, b и c су такви да $b^2 - 4ac$ није потпун квадрат. Доказати да за сваки природан број $n > 1$ постоји n узастопних природних бројева, таквих да међу њима нема бројева облика $(ax^2 + bxy + cy^2)^z$, за неке целе x и y и природан број z.

97. Нека је $p = 4t + 1$ прост број. Доказати да постоји $k \in \mathbb{N}$, $1 < k < p - 1$ тако да $k^k \equiv 1 \pmod{p}$.

98. Ако је $p \geq 19$ прост број, доказати да постоје три различита квадратна неостатка по модулу p, чији је збир дељив са p. Ово важи и за $p = 7$ и $p = 13$.

99. За прост број $p \equiv 7 \pmod{8}$, израчунати $\sum_{k=1}^{\frac{p-1}{2}} \left[\dfrac{k^2}{p} + \dfrac{1}{2}\right]$.

100. Доказати да, ако је $p = 2^n + 1$, $n \geq 2$, прост број, тада p дели $3^{\frac{p-1}{2}} + 1$. Доказати затим да је 3 примитивни корен по модулу p.

101. За природан број a, дефинише се низ природних бројева $x_1, x_2, ...$ на следећи начин: $x_1 = a$, $x_{n+1} = 2x_n + 1$. Нека је $y_n = 2^{x_n} - 1$, $n \in \mathbb{N}$. Одредити највеће k, тако да су за неки природан број a бројеви y_1, y_2, ... , y_k прости.

102. **(поучан!)** Ако природни бројеви m и n задовољавају $\varphi(5^m - 1) = 5^n - 1$, доказати да је $(m, n) > 1$.

103. Прост број p је облика $4k + 1$ и задовољава $p^2 \mid 2^p - 2$. Доказати да за највећи прост делилац q броја $2^p - 1$ важи неједнакост $2^q > (6p)^p$.

Додатак - за оне који желе више

104. Нека је $p = 4k + 1$ прост број. Дефинишимо следећи скуп $\mathbb{S} = \{(x, y, z) \in \mathbb{N}^3 | x^2 + 4yz = p\}$.
а) Доказати да је скуп $\mathbb{S}$ непразан;
б) Ако је функција $f : \mathbb{S} \longrightarrow \mathbb{S}$ дата са

$$f(x, y, z) = \begin{cases} (x + 2z, z, y - x - z) & , \quad x < y - z \\ (2y - x, y, x - y + z) & , \quad y - z < x < 2y \\ (x - 2y, x - y + z, y) & , \quad x > 2y \end{cases}$$

доказати да је ово добро дефинисана функција (тј. да за $(x,y,z)\in\mathbb{S}$, $f(x,y,z)\in\mathbb{S}$, као и да је немогуће $y-z=x$ и $x=2y$) и да је инволуција (тј. да је бијекција и да је f једнако свом инверзном пресликавању: за $(x,y,z)\in\mathbb{S}$ $f(x,y,z)=f^{-1}(x,y,z)$);
в) Доказати да f има тачно једну фиксну тачку (тј. постоји тачно једна тројка $(x,y,z)\in\mathbb{S}$ за коју је $f(x,y,z)=(x,y,z)$);
г) Доказати да је број елемната скупа $\mathbb{S}$ непаран;
д) Доказати да онда и инволуција $g:\mathbb{S}\longrightarrow\mathbb{S}$ дата са $g(x,y,z)=(x,z,y)$ такође има фиксну тачку;
ђ) Доказати да постоје природни бројеви a и b тако да је $p=a^2+b^2$.

105. За цео број a и непарне просте бројеве $p\neq q$, означимо: $S(p,a)=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{ka}{p}\right]$ и $S'(p,a)=\sum_{k=1}^{\frac{p-1}{2}}\left[\frac{2ka}{p}\right]$.
Доказати:
а) За $p\nmid a$ важи $\left(\frac{a}{p}\right)=(-1)^{S'(p,a)}$;
б) За непарно a и $p\nmid a$ важи $\left(\frac{2a}{p}\right)=(-1)^{\frac{p^2-1}{8}+S(p,a)}$;
в) За непарно a и $p\nmid a$ важи $\left(\frac{a}{p}\right)=(-1)^{S(p,a)}$;
г) $S(p,q)+S(q,p)=\frac{p-1}{2}\cdot\frac{q-1}{2}$;
д) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

106. За непарне различите просте бројеве p и q, доказати:
а) $\frac{\sin px}{\sin x}=(-4)^{\frac{p-1}{2}}\cdot\prod_{j=1}^{\frac{p-1}{2}}\left(\sin^2 x-\sin^2\frac{2j\pi}{p}\right)$;
б) $\left(\frac{p}{q}\right)=\prod_{k=1}^{\frac{q-1}{2}}\frac{\sin\frac{2kp\pi}{q}}{\sin\frac{2k\pi}{q}}$;
в) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

107. Нека је p прост број, $p\neq 2$, нека је a цео број, $p\nmid a$, и нека је $\mathbb{A}$ редукован систем остатака по модулу p без нуле. Пресликавања $Z_a:\mathbb{A}\longrightarrow\mathbb{A}$ и $T_a:\mathbb{A}\longrightarrow\mathbb{A}$ дефинишемо на следећи начин: $Z_a(x)=a\cdot x$ и $T_a(x)=a\cdot x^{-1}$ (множење се врши по модулу p и $x^{-1}=y$ ако и само ако $xy=1$). Доказати:
а) Z_a и T_a су пермутације скупра $\mathbb{A}$;
б) $Z_a=T_a\circ T_1$;
в) $T_a^2=Id$, где је Id идентично пресликавање;
г) $sgn(T_a)=(-1)^{\frac{p-2-(\frac{a}{p})}{2}}$;
д) $sgn(Z_a)=\left(\frac{a}{p}\right)$.

108. Нека су p и q прости бројеви, $p\neq q$, $p,q\neq 2$. Уведимо ознаке $\mathbb{X}=\{0,1,...,p-1\}$, $\mathbb{Y}=\{0,1,...,q-1\}$, $\mathbb{T}=\{0,1,...,pq-1\}$. Нека су $P(x)$ и $Q(y)$ остаци који се добијају приликом дељења бројева x и y са p, односно q, и нека је $R(t)=(P(t),Q(t))$. Пресликавања $U:\mathbb{X}\times\mathbb{Y}\longrightarrow\mathbb{X}\times\mathbb{Y}$ и $V:\mathbb{X}\times\mathbb{Y}\longrightarrow\mathbb{X}\times\mathbb{Y}$ дефинишемо са $U(x,y)=(x,Q(x+py))$ и $V(x,y)=(P(qx+y),y)$. Доказати:
а) $U(x,y)=R(x+py)$ и $V(x,y)=R(qx+y)$;
б) Пресликавања U и V су пермутације, $sgn(U)=\left(\frac{p}{q}\right)$ и $sgn(V)=\left(\frac{q}{p}\right)$;
в) Пресликавање $W=R^{-1}\circ U\circ V^{-1}\circ R$ је пермутација скупа $\mathbb{T}$ и $sgn(W)\equiv\binom{p}{2}\binom{q}{2}\pmod 2$;
г) Пресликавање $U\circ V^{-1}$ је пермутација скупа $\mathbb{X}\times\mathbb{Y}$ и $sgn(U\circ V^{-1})=\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$;
д) $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)=(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.