Теория на числата - част 3

Задача 1. Решете сравнението

$$2x^2 + 5x + 13 \equiv 5(\mod 11).$$

Задача 2. Пресметнете $\left(\frac{2008}{257}\right)$.

Задача 3. Нека $\left(\frac{a}{p}\right) = 1$ и p е просто, такова че $p \equiv 3(\mod 4)$.
а) Да се докаже, че $x \equiv a^{(p+1)/4}$ е решение на сравнението $x^2 \equiv a(\mod p)$.
б) Като използвате а), решете сравнението $x^2 \equiv 7(\mod 787)$.

Задача 4. Кои от следните сравнения са решими
а) $x^2 \equiv 10(\mod 127)$;
б) $x^2 \equiv 137(\mod 401)$;

Задача 5. Нека p е просто, $p \equiv 1(\mod 4)$ и $a^2 + b^2 = p$. Докажете, че $\left(\frac{a}{p}\right) = 1$.

Задача 6. Проверете разрешимо ли е сравнението и ако е, намерете решенията му:
а)$2x^2 + 5x + 13 \equiv 5(\mod 11)$;
б)$3x^2 + 5x + 15 \equiv 4(\mod 11)$;

Задача 7. Напишете всички квадратични остатъци по модул 19.

Задача 8. Пресметнете символите на Льожандър $\left(\frac{85}{101}\right)$, $\left(\frac{29}{541}\right)$, $\left(\frac{101}{1987}\right)$, $\left(\frac{31706}{43789}\right)$.

Задача 9. Нека $\left(\frac{a}{p}\right) = 1$ и p е просто, такова че $p \equiv 3(\mod 4)$.
а) Да се докаже, че $x \equiv a^{(p+1)/4}$ е решение на сравнението $x^2 \equiv a(\mod p)$.
б) Като използвате а), решете сравнението $x^2 \equiv 7(\mod 787)$.

Задача 10. Намерете всички прости числа p, които удовлетворяват равенството $\left(\frac{-6}{p}\right) = 1$.

Задача 11. Да се докаже, че ако p е просто число и a принадлежи на показател 3 по модул p, то числото $a + 1$ принадлежи на показател 6 по модул p.

Задача 12. Докажете, че за всяко просто число p от вида $p = 4k + 3$ n сравнението $x^2 + \frac{p+1}{4} \equiv 0(\mod p)$ няма решение.

Задача 13. Пресметнете реда на 2 по модул 19.

Задача 14. Ако редът на b по модул m е 42, то колко е редът на b^{30} по модул m?

Задача 15. Кои от следните сравнения са решими
а) $x^2 \equiv 10(\mod 127)$;
б) $x^2 \equiv 137(\mod 401)$;

Задача 16. Покажете, че диофантовото уравнение $2x^2 - 5y^2 = 1$,няма решение в цели числа.

Задача 17. Проверете кои от следните сравнения са разрешими
а)$x^2 \equiv -1(\mod 5987)$;
б)$x^2 \equiv 6780(\mod 6781)$;
в)$x^2 + 14x - 35 \equiv 0(\mod 337)$;
г)$x^2 - 64x + 943 \equiv 0(\mod 3011)$;
д)$x^2 - 3x - 1 \equiv 0(\mod 31957$;

Задача 18. Вярно ли е, че числата $0, 1, 2, 4, 8, ..., 2^{11}$ образуват пълна система остатъци по модул 13?

Задача 19. Вярно ли е, че 2 е примитивен корен по модул 11?А 3?

Задача 20. Проверете, че ако p е нечетно просто число и a е квадратичен остатък по модул p, то a не е примитивен корен по модул p.

Задача 21. Напишете всички квадратични остатъци по модул 19.

Задача 22. Проверете, че ако и g са примитивни корени модул p, то ag не е примитивен корен по модул p. (p е нечетно просто число)

Задача 23. Нека g е примитивен корен по модул n. Да се докаже, че съществуват $\varphi(\varphi(n))$ на брой примитивни корена по модул n. (Използвайте, че $a \equiv g^i(\mod n)$ за някое i, такова че $(i, \varphi(n))$).

Задача 24. Нека n е безквадратно число. Докажете, че следните две твърдения са еквивалентни:
1) Ако $(a, n) = 1$, то $a^{n-1} \equiv 1(\mod n)$.
2) За всеки прост делител p на n е изпълнено $p - 1 | n - 1$.

Задача 25. Нека p е нечетно просто число и g е примитивен корен по модул p. Покажете, че съществува естетсвено число x, такова че $g^x \equiv x(\mod p)$.

Задача 26. Намерете всички примитивни корени по модул 13.

Теория на числата - част 3

Задача 27. Колко примитивни корени по модул n съществуват, ако
а) $n = 2018$;
б) $n = 97$;

Задача 28. Нека $n \geqq 2$ е естествено число. Докажете, че следните твърдения са еквивалентни:
1) за всяко цяло x, $(x, n) = 1$ е изпълнено сравнението $x^6 \equiv 1(\mod n)$;
2) $n|504$.

Задача 29. Какъв е редът на 3 по модул 29.

Задача 30. Да се докаже, че 3 е примитивен корен по модул 17^2.

Задача 31. Нека $n > 1$ и нека p е прост делител на $2^{2^n} + 1$. Да се докаже, че редът на 2 по модул p е 2^{n+1}.

Задача 32. Нека p е просто число. Докажете, че $p \equiv 1(\mod 8)$ тогава и само тогава, когато съществува цяло число x, такова че $x^4 \equiv -1(\mod p)$.

Задача 33. Пресметнете символите на Льожандър:

$$\left(\frac{10}{19}\right), \quad \left(\frac{7}{11}\right), \quad \left(\frac{2008}{257}\right), \quad \left(\frac{503}{773}\right), \quad \left(\frac{501}{773}\right),$$

Задача 34. Нека $g(p)$ е най-малкият квадратичен неостатък по модул p. Докажете, че $g(p)$ е просто число.

Задача 35. Намерете реда на числото 2 по модул 17, по модул 19 и по модул 23.

Задача 36. За нечетни прости числа p да се докаже равенството

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{ако} p \equiv \pm 1(\mod 12); \\ -1, & \text{ако} p \equiv \pm 5(\mod 12). \end{cases}$$

Задача 37. Нека $g(p)$ е най-малкият квадратичен неостатък по модул p. Докажете, че $g(p) = 5$ тогава и само тогава, когато $p \equiv \pm 23, \pm 47(\mod 120)$.

Задача 38. Нека $g(p)$ е най-малкият квадратичен неостатък по модул p. Докажете, че $g(p) < \sqrt{p} + 1$.

вариант	ф. номер	група	поток	курс	специалност
1					
Име:					

Теория на числата - част 3

Задача 39. Проверете, че 2 е примитивен корен по модул 11.

Задача 40. Проверете, че 2 е примитивен корен по модул 121.

Задача 41. Пресметнете $\left(\frac{2008}{257}\right)$.

Задача 42. Пресметнете символите на Льожандър:

$$\left(\frac{10}{19}\right), \quad \left(\frac{7}{11}\right), \quad \left(\frac{2008}{257}\right), \quad \left(\frac{503}{773}\right), \quad \left(\frac{501}{773}\right),$$

Задача 43. Нека $g(p)$ е най-малкият квадратичен неостатък по модул p. Докажете, че $g(p)$ е просто число.

Задача 44. Нека $\left(\frac{a}{p}\right) = 1$ и p е просто, такова че $p \equiv 3(\mod 4)$.
а) Да се докаже, че $x \equiv a^{(p+1)/4}$ е решение на сравнението $x^2 \equiv a(\mod p)$.
б) Като използвате а), решете сравнението $x^2 \equiv 7(\mod 787)$.

Задача 45. Използвайки, че 3 е примитивен корен по модул 43 намерете
а) всички естествени числа по-малки от 43, които имат ред 6 по модул 43;
б)всички естествени числа по-малки от 43, които имат ред 21 по модул 43.

Задача 46. Проверете, че 3 е примитивен корен по модул 17.

вариант	ф. номер	група	поток	курс	специалност
2					
Име:					

Теория на числата - част 3

Задача 1. Нека p е просто, $p \equiv 1(\mod 4)$ и $a^2 + b^2 = p$. Докажете, че $\left(\frac{a}{p}\right) = 1$.

Задача 2. Колко примитивни корени по модул n съществуват, ако
а) $n = 2018$;
б) $n = 97$;

Задача 3. Нека $n \geqq 2$ е естествено число. Докажете, че следните твърдения са еквивалентни:
1) за всяко цяло x, $(x, n) = 1$ е изпълнено сравнението $x^6 \equiv 1(\mod n)$;
2) $n|504$.

Задача 4. Какъв е редът на 3 по модул 29.

Задача 5. Да се докаже, че 3 е примитивен корен по модул 17^2.

Задача 6. Напишете всички квадратични остатъци по модул 19.

Задача 7. Пресметнете символите на Льожандър $\left(\frac{85}{101}\right)$, $\left(\frac{29}{541}\right)$, $\left(\frac{101}{1987}\right)$, $\left(\frac{31706}{43789}\right)$.

Задача 8. Нека $\left(\frac{a}{p}\right) = 1$ и p е просто, такова че $p \equiv 3(\mod 4)$.
а) Да се докаже, че $x \equiv a^{(p+1)/4}$ е решение на сравнението $x^2 \equiv a(\mod p)$.
б) Като използвате а), решете сравнението $x^2 \equiv 7(\mod 787)$.

Задача 9. Намерете всички прости числа p, които удовлетворяват равенството $\left(\frac{-6}{p}\right) = 1$.

Теория на числата - част 3

Задача 14. Намерете реда на числото 2 по модул 17, по модул 19 и по модул 23.

Задача 15. Да се докаже, че ако p е просто число и a принадлежи на показател 3 по модул p, то числото $a + 1$ принадлежи на показател 6 по модул p.

Теория на числата - част 3

вариант	ф. номер	група	поток	курс	специалност
3					
Име:					

Теория на числата - част 3

Задача 1. Нека $n > 1$ и нека p е прост делител на $2^{2^n} + 1$. Да се докаже, че редът на 2 по модул p е 2^{n+1}.

Задача 2. Нека p е просто число. Докажете, че $p \equiv 1(\mod 8)$ тогава и само тогава, когато съществува цяло число x, такова че $x^4 \equiv -1(\mod p)$.

Задача 3. Вярно ли е, че числата $0, 1, 2, 4, 8, ..., 2^{11}$ образуват пълна система остатъци по модул 13?

Задача 4. Вярно ли е, че 2 е примитивен корен по модул 11?А 3?

Задача 5. Пресметнете символите на Льожандър $\left(\frac{85}{101}\right)$, $\left(\frac{29}{541}\right)$, $\left(\frac{101}{1987}\right)$, $\left(\frac{31706}{43789}\right)$.

Задача 6. Нека $\left(\frac{a}{p}\right) = 1$ и p е просто, такова че $p \equiv 3(\mod 4)$.
а) Да се докаже, че $x \equiv a^{(p+1)/4}$ е решение на сравнението $x^2 \equiv a(\mod p)$.
б) Като използвате а), решете сравнението $x^2 \equiv 7(\mod 787)$.

Задача 7. Намерете всички прости числа p, които удовлетворяват равенството $\left(\frac{-6}{p}\right) = 1$.

Задача 8. Намерете показателя на 2 по модул 9, показателя на 2 по модул 15, показателя на 3 по модул 16 и показателя на 3 по модул 10.

Задача 9. Намерете примитивните корени по модул 13.

Задача 10. Нека p и q са прости числа, такива че $p = 2q + 1$. Колко примитивни корена по модул p има?

Задача 11. Нека g е примитивен корен по модул 37. Кои от числата g^2, g^3, ..., g^8 са също примитивни корени по модул 37?

Задача 12. Проверете, че ако числото a е точен квадрат, а p е нечетно просто число, то a не е промитивен корен по модул p.

Задача 13. Проверете, че 19 не дели никое от числата $4n^2 + 4$ за $n \in \mathbb{N}$.

Теория на числата - част 3

Задача 16. Използвайки, че 3 е примитивен корен по модул 43 намерете
а) всички естествени числа по-малки от 43, които имат ред 6 по модул 43;
б)всички естествени числа по-малки от 43, които имат ред 21 по модул 43.

Задача 17. Проверете, че 3 е примитивен корен по модул 17.

Задача 18. Кои от следните сравнения са решими
а) $x^2 \equiv 10(\mod 127)$;
б) $x^2 \equiv 137(\mod 401)$;

Задача 19. Докажете, че за всяко просто число p от вида $p = 4k + 3$ n сравнението $x^2 + \frac{p+1}{4} \equiv 0(\mod p)$ няма решение.

вариант	ф. номер	група	поток	курс	специалност
1					
Име:					

Теория на числата - част 3

Задача 3. Пресметнете символите на Льожандър:

$$\left(\frac{10}{19}\right), \quad \left(\frac{7}{11}\right), \quad \left(\frac{2008}{257}\right), \quad \left(\frac{503}{773}\right), \quad \left(\frac{501}{773}\right),$$

Задача 4. Нека $g(p)$ е най-малкият квадратичен неостатък по модул p. Докажете, че $g(p)$ е просто число.

Задача 5. За нечетни прости числа p да се докаже равенството

$$\left(\frac{3}{p}\right) = \begin{cases} 1, & \text{ако} p \equiv \pm 1(\mod 12); \\ -1, & \text{ако} p \equiv \pm 5(\mod 12). \end{cases}$$

Задача 6. Нека $g(p)$ е най-малкият квадратичен неостатък по модул p. Докажете, че $g(p) = 5$ тогава и само тогава, когато $p \equiv \pm 23, \pm 47(\mod 120)$.

Задача 7. Нека $g(p)$ е най-малкият квадратичен неостатък по модул p. Докажете, че $g(p) < \sqrt{p} + 1$.

Задача 8. За всеки остатък x по модул 11 пресметнете остатъкът на x^3 по модул 11.

Задача 9. Проверете, че 2 е примитивен корен по модул 11.

Задача 10. Проверете, че 2 е примитивен корен по модул 121.

вариант	ф. номер	група	поток	курс	специалност
4					
Име:					

Теория на числата - част 3

Задача 1. Пресметнете реда на 2 по модул 19.

Задача 2. Ако редът на b по модул m е 42, то колко е редът на b^{30} по модул m?

вариант	ф. номер	група	поток	курс	специалност
2					
Име:					

Теория на числата - част 3

Задача 1. Проверете, че ако p е нечетно просто число и a е квадратичен остатък по модул p, то a не е примитивен корен по модул p.

Задача 2. Проверете, че ако a и g са примитивни корени модул p, то ag не е примитивен корен по модул p. (p е нечетно просто число)

Задача 3. Нека g е примитивен корен по модул n. Да се докаже, че съществуват $\varphi(\varphi(n))$ на брой примитивни корена по модул n. (Използвайте, че $a \equiv g^i(\mod n)$ за някое i, такова че $(i, \varphi(n)))$.

Задача 4. Нека n е безквадратно число. Докажете, че следните две твърдения са еквивалентни:
1) Ако $(a, n) = 1$, то $a^{n-1} \equiv 1(\mod n)$.
2) За всеки прост делител p на n е изпълнено $p - 1 | n - 1$.

Задача 5. Нека p е нечетно просто число и g е примитивен корен по модул p. Покажете, че съществува естествено число x, такова че $g^x \equiv x(\mod p)$.

Задача 6. Намерете всички примитивни корени по модул 13.