Теорія чисел і криптографія: подільність і модульна арифметика; прості числа

1. Знайти частку та остачу, коли:

а) 44 поділити на 8; б) 777 поділити на 21; в) –123 поділити на 19; г) –1 поділити на 23; д) –2002 поділити на 87; е) 0 поділити на 17; є) 1234567 поділити на 1001; ж) –100 поділити на 101.

2.Який час на 24-часовому годиннику?

а) через 100 годин після того, як на ньому є 2:00;

б) за 45 годин перед тим, як на ньому є 12:00;

в) через 168 годин після того, як на ньому є 19:00.

3.Нехай a і b цілі числа, $a \equiv 11 \pmod{19}$, $b \equiv 3 \pmod{19}$.

Знайти ціле число c таке, що $0 \le c \le 18$ і, окрім того:

а) $c \equiv 13a \pmod{19}$;

б) $c \equiv 8b \pmod{19}$;

в) $c \equiv a - b \pmod{19}$;

г) $c \equiv 7a + 3b \pmod{19}$;

д) $c \equiv 2a^2 + 3b^2 \pmod{19}$;

е) $c \equiv a^3 + 4b^3 \pmod{19}$.

4.Обчислити значення: а) –17 **mod** 2; б) 144 **mod** 7; в) –101 **mod** 13; г) 199 **mod** 19.

5. Знайти a **div** m та a **mod** m, коли: а) a = –111; m = 99; б) a = –9999; m = 101; в) a = 10299; m = 999; г) a = 123456; m = 1001.

6.Знайти ціле число a таке, що:

а) $a \equiv 43 \pmod{23}$ і $-22 \le a \le 0$;

б) $a \equiv 17 \pmod{29}$ і $-14 \le a \le 14$;

в) $a \equiv -11 \pmod{21}$ і $90 \le a \le 110$.

7. З’ясувати, які з наступних чисел конгруентні до 3 за модулем 7. а) 37; б) 66; в) –17; г) –67.

8. Знайти значення виразів:

а) (177 **mod** 31 + 270 **mod** 31) **mod** 31;

б) (177 **mod** 31 · 270 **mod** 31) **mod** 31.

9. Знайти значення виразів:

а) (19^2 **mod** 41) **mod** 9;

б) (32^3 **mod** 13)^2 **mod** 11;

в) (7^3 **mod** 23)^2 **mod** 31;

г) (21^2 **mod** 15)^3 **mod** 22.

10. Для кожного з поданих нижче чисел визначити, чи є воно простим.

а) 19; б) 27; в) 93; г) 101; д) 107; е) 113.

11.Розкласти кожне із поданих нижче чисел на прості множники.

а) 39; б) 81; в) 101; г) 143; д) 289; е) 899.

12. Обчислити значення функції Ейлера $\phi(10)$.

13. Обчислити значення функції Ейлера $\phi(13)$.

14.Використати алгоритм Евкліда для знаходження

А)gcd(1001, 1331).

Б) gcd(12345, 54321).

15. Використати розширений алгоритм Евкліда для подання gcd(26, 91) як лінійної комбінації $s\cdot 26 + t\cdot 91$.

16. Використати розширений алгоритм Евкліда для подання gcd(144, 89) як лінійної комбінації $s\cdot 144 + t\cdot 89$.

17. Знайти єдине (тобто додатне і таке, що менше ніж m) обернене до a за модулем m,

якщо а) $a = 4$, $m = 9$.

б) $a = 2$, $m = 17$

18. Використати розширений алгоритм Евкліда для подання gcd(203, 101) як лінійної комбінації $s\cdot 203 + t\cdot 101$. Відповідь: $1\cdot 203 + (-2)\cdot 101$. Те саме зробити за звичайним алгоритмом Евкліда.

19. Знайти обернене до 19 за модулем 141.

20. Знайти обернене до 55 за модулем 89

21. Знайти обернене до 89 за модулем 232.

22. Розв’язати конгруенцію

а)$2x \equiv 7 \pmod{17}$

б) $19x \equiv 4 \pmod{141}$

в) $55x \equiv 34 \pmod{89}$.

г) $89x \equiv 2 \pmod{232}$

23.Розв'язати систему конгруенцій:

А) $x \equiv 2 \pmod{3}$; $x \equiv 1 \pmod{4}$; $x \equiv 3 \pmod{5}$. Відповідь: $x \equiv 53 \pmod{60}$.

Б) $x \equiv 1 \pmod{2}$; $x \equiv 2 \pmod{3}$; $x \equiv 3 \pmod{5}$ і $x \equiv 4 \pmod{11}$. Відповідь: $x \equiv 323 \pmod{330}$.

24. Використавши малу теорему Ферма, знайти

А) 7^{121} **mod** 13.

Б) 3^{302} **mod** 5

В) 5^{2003} **mod** 13

23^{1002} **mod** 41.