МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ХАРКІВСКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

ІМЕНИ СЕМЕНА КУЗНЕЦЯ

Лабораторна робота №4

“Тема №4”

з дисципліни «Математичні основи криптології»

Виконав:

Студент групи 6.04.125.010.21.2

факультету Інформаційних технологій

спеціальності 125

П.І.П. Бойко В.В.

Перевірив:

Чугай А.М.

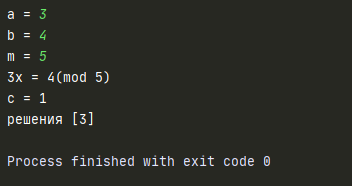
Харків – 2022

1. Знайти всі розв’язки лінійних рівнянь:
   * 

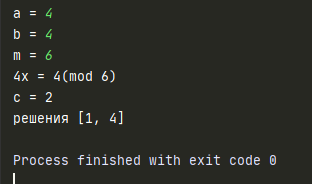
НОД (3, 5) = 1

3x = 4 (mod 5)

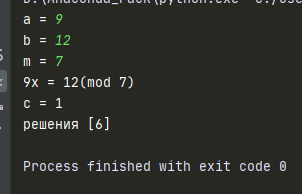
X = 4()(mod 5)  
маємо одне рішення = 3



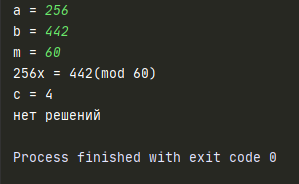
* + 



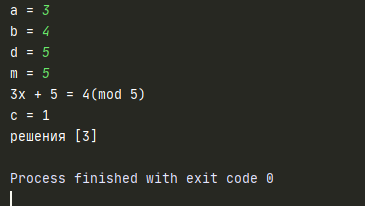
* + 



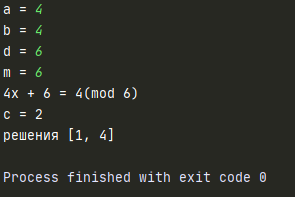
* + 



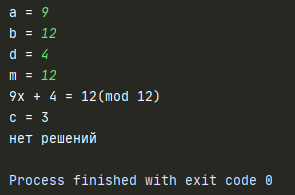
* + 



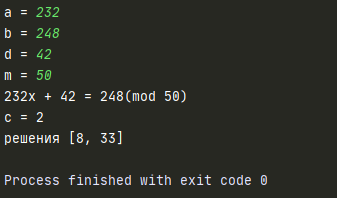
* + 



* + 



* + 



Я написав программу для рішення даного завдання

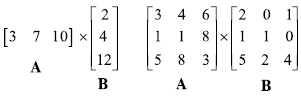
Код:

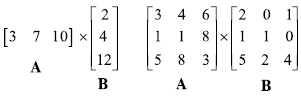
a = int(input('a = '))  
b = int(input('b = '))  
d = int(input('d = '))  
m = int(input('m = '))  
  
*def* nod(*a*, *b*):  
 # if (b > a):  
 # return nod(b, a)  
 *if* (*a* % *b* == 0):  
 *return b  
 return* nod(*b*, *a* % *b*)  
  
  
*def* solution(*a*, *b*, *m*, *d* = 0):  
 *if d* == 0:  
 print(str(*a*) + 'x = ' + str(*b*) + '(mod ' + str(*m*) + ')')  
 *else*:  
 print(str(*a*) + 'x + ' + str(*d*) + ' = ' + str(*b*) + '(mod ' + str(*m*) + ')')  
 b = *b* - *d* c = nod(*a*, *m*)  
 print('c = ' + str(c))  
 *if b* % c != 0:  
 print('нет решений')  
 *return* l = [x *for* x *in* range(*m*)]  
  
 s = []  
  
 *for* i *in* l:  
 *if* (*a* \* i - *b*) % *m* == 0:  
 s.append(i)  
  
 *if* c == len(s):  
 print("решения " + str(s))  
 *else*:  
 print('решай сам')  
  
solution(a, b, m, d)

1. Знайти

,

де

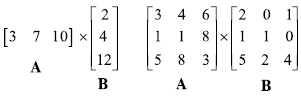


 = [154]

∆ = 154

154 mod 16 = 10

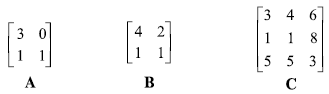
|  |  |  |
| --- | --- | --- |
| 40 | 16 | 27 |
| 43 | 17 | 33 |
| 33 | 14 | 17 |

=

∆ = -85

-85 mod 16 = 11

1. Знайти визначник та мультиплікативну інверсію для матриці вирахувань на множині Z10.



A ∆ = 3

НСД(3, 10) = 1

Транспонована матриця

|  |  |
| --- | --- |
| 3 | 1 |
| 0 | 1 |

Знаходжу матрицю складену з алгебраїчних доповнень A\* =

|  |  |
| --- | --- |
| 1 | 0 |
| -1 | 3 |

Тепер знайдемо обернену

|  |  |
| --- | --- |
| 1 | 0 |
| -1 | 3 |

|  |  |
| --- | --- |
| 1 | 0 |
| -1 | 3 |

|  |  |
| --- | --- |
| 1/3 | 0 |
| -1/3 | 1 |

A\* =

A-1 = (1 \ det(a)) \* A\* = 1 \ 3 \* =

A-1 ∆ = 1/3

А в Z10 = 3 mod 10 = 3

B ∆ = 2

НСД(10, 2) = 2

Ця матриця не буде мати мультиплікативну інверсію

C ∆ = 37

НСД(37, 10) = 1

Транспонована матриця

|  |  |  |
| --- | --- | --- |
| 3 | 1 | 5 |
| 4 | 1 | 5 |
| 6 | 8 | 3 |

|  |  |  |
| --- | --- | --- |
| -37 | 18 | 26 |
| 37 | -21 | -18 |
| 0 | 5 | -1 |

С\* =

|  |  |  |
| --- | --- | --- |
| -37 | 18 | 26 |
| 37 | -21 | -18 |
| 0 | 5 | -1 |

|  |  |  |
| --- | --- | --- |
| -1 | 18/37 | 26/37 |
| 1 | -21/37 | -18/37 |
| 0 | 5/37 | -1/37 |

С-1 = 1/37 \* =

Det(C-1) = 1 / 37

37 mod 10 = 7

1/3 7 В Z10

(det(С-1) mod 10) = 1/37

1. Знайти всі розв’язки систем лінійних рівнянь:
   *  та  

A-1 =

X = 8 (mod 5) = 3

Y = 7 (mod 5) = 2

* +  та 

A-1 =

X = 35 (mod 7) = 0

Y = 45 (mod 7) = 3

* +  та 

A-1 =

X = 13 (mod 7) = 6

Y = 15 (mod 7) = 1

* +  та  

A-1 =

X = 25 (mod 8) = 1

Y = 23 (mod 8) = 7