Министерство науки и высшего образования Российской Федерации

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«КУБАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»**

**(ФГБОУ ВО «КубГУ»)**

**Факультет компьютерных технологий и прикладной математики**

**Кафедра вычислительных технологий**

**Отчёт**

**по лабораторной работе №2**

**Дисциплина: КРИПТОГРАФИЧЕСКИЕ ПРОТОКОЛЫ**

**Тема: «Китайская теорема об остатках»**

Работу выполнил \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ К. А. Корнилов

Направление подготовки 02.03.02 Фундаментальная информатика и

информационные технологии

Направленность (профиль) Математическое и программное обеспечение

компьютерных технологий

Преподаватель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_А. А. Крамаренко

**Тема:** Теорема об остатках

**Цель:** Изучение теоремы об остатках для решения систем линейных сравнений.

**Ход работы:**

1. Найти решение системы сравнений

Решим задачу с помощью китайской теоремы об остатках.

* 1. Нод(5, 17, 12) = 1 =>взаимно простые модули
  2. M = 5 \* 17 \* 12 = 60 \* 17 = 1020
  3. M1 = 17 \* 12 =204 M2=5 \* 12 = 60 M3 = 5 \* 17 = 85
  4. Решаем отдельно каждое из сравнений и получаем следующие значения b1,b2,b3:
  5. X = (3 \* 204 + 60 \* 10 + 5 \* 85) mod 1020 = 617 + 1020K

1. Найти решение системы сравнений

Решим задачу с помощью китайской теоремы об остатках.

* 1. Нод(6, 35, 11) = 1 =>взаимно простые модули
  2. M = 6 \* 35 \* 11 = 2310
  3. M1 = 385 M2=66 M3 = 210
  4. Решаем отдельно каждое из сравнений и получаем следующие значения b1,b2,b3:
  5. X = (2 \* 385 + 23 \* 66 + 4 \* 210) mod 2310 = 818 + 2310K

1. Решены следующие примеры
   1. Дано НОД(a,b) = 24. Найти НОД(a,b,16)

НОД(a,b,16) <= 16. НОД(a,b) должен делиться на НОД(a,b,16) => Найдем НОД(24,16) => НОД(24,16) = 8 => **НОД(a,b,16) = 8**

* 1. Дано НОД(a,b,c) = 12. Найти НОД(a,b,c,16)

НОД(a,b,16) <= 16. НОД(a,b,c) должен делиться на НОД(a,b,c,16) => Найдем НОД(12,16) => НОД(12,16) = 4 => **НОД(a,b,c,16) = 4**

* 1. Найти НОД(200,180,450)

НОД(200,180) = 20 => НОД(200,180,450) = НОД(20,450) = **10**

* 1. Найти НОД(200,180,450,610)

Из предыдущей задачи НОД(200,180,450) = 10 => НОД(200,180,450,610) = НОД(10, 610) = 10

1. Предположим, что n >=0
   1. Найти НОД(2n+1, n) = 1

|  |  |  |  |
| --- | --- | --- | --- |
| q | R1 | R2 | R |
| 2 | 2n+1 | n | 1 |
| n | n | 1 | 0 |
| 0 | **1** | 0 | 0 |

* 1. Используя результат 4.1. найти:

НОД(201,100) = 1

НОД(81,40) = 1

НОД(501,250) = 1

1. Предположим, что n >=0
   1. Найти НОД(3n+1, 2n+1) = 1

|  |  |  |  |
| --- | --- | --- | --- |
| q | R1 | R2 | R |
| 1 | 3n+1 | 2n+1 | т |
| 2 | 2n+1 | n | 1 |
| n | n | 1 | 0 |
| 0 | **1** | 0 | 0 |

* 1. Используя результат 5.1. найти:

НОД(301,201) = 1

НОД(81,121) = 1

1. Используя расширенный алгоритм Евклида найти НОД и коэффициенты s и t
   1. R1 = 7 R2 = 4

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 1 | 7 | 4 | 3 |
| 1 | 4 | 3 | 1 |
| 0 | 3 | 1 | 0 |

Обратный ход для нахождения коэффициентов s и t:

1 = 4 -3 = 4 – (7 – 4) = 4\*2 – 7

Тогда: Нод(1)

S = -1 + 4k

T = 2 – 7k

* 1. R1 = 291 R2 = 42

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 6 | 291 | 42 | 39 |
| 1 | 42 | 39 | 3 |
| 13 | 39 | 3 | 0 |

Обратный ход для нахождения коэффициентов s и t:

3 = 42 - 39 = 42 – (291 – 42 \* 6) = 42 \* 7 – 291

Тогда: Нод(291,42) = 3

S = -1 + 42k

T = 7 – 291k

* 1. R1 = 320 R2 = 84

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 3 | 320 | 84 | 68 |
| 4 | 68 | 16 | 4 |
| 4 | 16 | 4 | 0 |

Обратный ход для нахождения коэффициентов s и t:

4 = 68 – 16 \* 4 = 68 – 4 \* (84 – 68) = 320 – 3 \* 84 – 4\* ( 84 – 320 + 3 \* 84) = -19\*84 + 5 \* 320

Тогда: Нод(320,84) = 4

S = 5 + -84k

T = -18 + 320k

* 1. R1 = 400 R2 = 60

|  |  |  |  |
| --- | --- | --- | --- |
| Q | R1 | R2 | R |
| 6 | 400 | 60 | 40 |
| 1 | 60 | 40 | 20 |
| 2 | 40 | 20 | 0 |

Обратный ход для нахождения коэффициентов s и t:

20 = 60 – 40 = 60 – (400 – 6 \* 60) = -400 + 7 \* 60

Тогда: Нод(1)

S = -1 + 60k

T = 7 – 400k

1. Перечислите все пары аддитивной инверсии по модулю 20

(1,19), (2,18), (3,17), (4,16), (5,15), (6,14), (7,13), (8,12), (9,11), (10,10)

1. Перечислите все пары мультипликативной инверсии по модулю 20

20 = 2 \* 2 \* 5 => инверсию будут иметь элементы взаимно простые с 20

(1,1), (3,7), (9,9), (11,11), (13,17), (19,19)

1. Найти мультипликативную инверсию каждого из следующих целых чисел в Z180, используя расширенный алгоритм Евклида
   1. 38

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| q | R1 | R2 | r | S1 | S2 | s | T1 | T2 | T |
| 4 | 180 | 38 | 28 | 1 | 0 | 1 | 0 | 1 | -4 |
| 1 | 38 | 28 | 10 | 0 | 1 | -10 | 1 | -4 | 5 |
| 2 | 28 | 10 | 8 | 1 | -10 | 21 | -4 | 5 | -14 |
| 1 | 10 | 8 | 2 | -10 | 21 | -31 | 5 | -14 | 19 |
| 4 | 8 | **2** | 0 | 21 | -31 |  | -14 | 19 |  |

Так как НОД(38,180) = 2, то инверсии нет

* 1. 7

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Q | R1 | R2 | r | S1 | S2 | s | T1 | T2 | T |
| 25 | 180 | 7 | 5 | 1 | 0 | 1 | 0 | 1 | -25 |
| 1 | 7 | 5 | 2 | 0 | 1 | -1 | 1 | -25 | 3 |
| 2 | 5 | 2 | 1 | 1 | -1 | 3 | -25 | 26 | -5 |
| 2 | 2 | **1** | 0 | -1 | 3 | -7 | 26 | -77 |  |

Так как НОД(7,180) = 1, то 7^-1 mod 180 = -77 mod 180 = 103

* 1. 132

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | R1 | R2 | r | T1 | T2 | T |
| 1 | 180 | 132 | 48 | 0 | 1 | -1 |
| 2 | 132 | 48 | 36 | 1 | -1 | 3 |
| 1 | 48 | 36 | 12 | -1 | 3 | -4 |
| 3 | 36 | **12** | 0 | 3 | -4 | 15 |

Так как НОД(132,180) = 12, то инверсии нет

* 1. 24

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Q | R1 | R2 | r | T1 | T2 | T |
| 7 | 180 | 24 | 12 | 0 | 1 | -7 |
| 2 | 24 | 12 | 0 | 1 | -7 |  |

Так как НОД(24,180) = 12, то инверсии нет

1. Найти частное и общее решение следующих линейных Диофантовых уравнений
   1. 25x+10y=15
      1. Нод(25,10) = 5 => 5x+2y = 3
      2. Нод(5,2) = 1 => 1 = 5 – 2\*2
      3. 5\*3 – 6\*2 = 3
      4. Общее решение

X = 3+(-2t)

Y= -6 + 5t

* + 1. Частное решение (3,-6).
  1. 19x+13y=20
     1. Нод(19,13) = 1 => 19x+13y = 20
     2. Нод(19,13) = 1 => 1 = 13 – 6\*2 = 13 – 2 \* (19 – 13) = -2\*19 +3\*13
     3. -40 \* 19 + 60 \* 13 = 20
     4. Общее решение

X = -40+13t

Y= 60 + (-19t)

* + 1. Частное решение (-40,60)
  1. 14x+21y=77
     1. Нод(14,21) = 7 => 2x+3y = 11
     2. Нод(2,3) = 1 => 1 = 3 – 2\*1
     3. -11 \* 2 + 11 \* 3 = 11
     4. Общее решение

X = -11+3t

Y= 11 + (-2t)

* + 1. Частное решение (-11,11)
  1. 40x+16y=88
     1. Нод(40,16) = 8 => 5x+2y = 11
     2. Нод(5,2) = 1 => 1 = 5 – 2\*2
     3. 11 \* 5 - 22 \* 2 = 11
     4. Общее решение

X = 11+(-2t)

Y= -22 + 5t

* + 1. Частное решение (11,-22)

1. Покажите, что нет ни одного решения следующих линейных Диофантовых уравнений
   1. 15x+12y = 13

НОД(15,12) =3 => 13 mod 3 <>0 => нет решения

* 1. 18x+30y = 20

НОД(18,30) =6 => 20 mod 6 <>0 => нет решения

* 1. 15x+25y = 69

НОД(15,25) =5 => 69 mod 5 <>0 => нет решения

* 1. 40x+30y = 98

НОД(40,30) =10 => 98 mod 10 <>0 => нет решения

1. Почтовое отделение продает марки только за 15 центов и за 39 центов. Найдите число марок, которое должен купить клиент, чтобы оплатить пересылку пакета стоимостью 2,7$. Найдите несколько решений

15x + 39y = 270

НОД(15,39) = 3 => 5x + 13y = 90

По обратному ходу расширенного алгоритма Евклида для 5 и 13:

1 = 3 -2 = 3 – (5 – 3) = 13 – 5 \* 2 – (5 – 13 + 5 \* 2) = -5\*5+2\*13

Тогда:

X0 = -450 + 13t

Y0 = 180+(-5t)

Подберем несколько вариантов решения с положительными значениями x и y: (5,5), (18,0). Так как дальше значения y станут отрицательными, то решений больше нет

1. Найдите все решения каждого из следующих линейных уравнений:
   1. 3x = 4 mod 5
      1. НОД(3,5) = 1 => 1 серия
      2. 3\*q+5\*s = 1
      3. По расширенному алгоритму Евклида q = 2 и s = -1
      4. X = (b\*q) mod m +mk = 3 + 5k
   2. 4x = 4 mod 6
      1. НОД(4,6) = 2 => 2 серии => 2x = 2 mod 3
      2. X = 2 \* 2^-1 mod 3
      3. По расширенному алгоритму Евклида 2^-1 = 2
      4. X = 2\*2 mod 3 = 1
      5. X0 = 1 +6k x1 = 4+6k
   3. 9x = 12 mod 7 => 2x = 5 mod 7
      1. НОД(2,7) = 1 => 1 серия
      2. X = 5 \* 2^-1 mod 7
      3. По расширенному алгоритму Евклида 2^-1 = 4
      4. X = 5\*4 mod 7 +7k= 6+7k
   4. 256x = 442 mod 60 => 16x = 22 mod 60
      1. НОД(16,60) = 4 => 22/4 <>0 => нет решения
2. Найдите все решения каждого из следующих линейных уравнений
   1. 3x + 5 = 4 mod 5
      1. 3x + 5 =4 mod 5 => 3x = -1 mod 5 => 3x = 4 mod
      2. Нод(3,5) =1 => x = (4\*3^-1) mod 5 + 5k
      3. По расширенному алгоритму Евклида 3^-1 = 2
      4. X = 3 + 5k
   2. 4x + 6 = 4 mod 6
      1. 4x + 6 =4 mod 6 => 4x = 4 mod 6
      2. Нод(4,6) =2 => 2 серии => 2x = 2 mod 3
      3. x = (2\*2^-1) mod 3 =1
      4. X0 = 1 + 6k X1 = 4+6K
   3. 9x + 4 = 12 mod 7
      1. 9x + 4 =12 mod 7 => 2x+4 = 5 mod 7 => 2x = 1 mod 7
      2. Нод(2,7) =1 => x = (1\*2^-1) mod 7 + 7k
      3. По расширенному алгоритму Евклида 2^-1 = 4
      4. X = 4 + 7k
   4. 232x + 42 = 248 mod 50
      1. 232x + 42 =248 mod 50 => 32x = 6 mod 50
      2. Нод(32,50) =2 серии => 16x = 3 mod 25
      3. По расширенному алгоритму Евклида x = b\*q mod 25 = 3\*11 mod 25 = 8
      4. X0 = 8 + 50k X1 = 33 + 50K
3. Найдите все подгруппы следующих групп:
   1. П = <Z16,+>
      1. Порядки подгрупп должны быть делителями порядка группы => возможные порядки 1,2,4,8,16
      2. Z1 = {0},
      3. Для порядка 2 решим уравнение 2x = 0 mod 16 => x0 = 0 x1 = 8 =>   
         Z2 = {0,8}
      4. Для порядка 4 решим уравнение 4x = 0 mod 16 => x = 4,8,12,0 =>   
         Z4 = {0,4,8,12}
      5. Для порядка 8 решим уравнение 8x = 0 mod 16 => x = 2,4,6,8,10,12,14,0 =>   
         Z8 = {0,2,4,6,8,10,12,14}
      6. Z16 = Z16
   2. П = <Z23,+>
      1. Порядки подгрупп должны быть делителями порядка группы => возможные порядки 1,23
      2. Z1 = {0},
      3. Z23 = Z23
   3. П = <Z16\*,x>
      1. Z16\* содержит все элементы, имеющие инверсию по умножению в Z16 => все элементы взаимно просты с 16 => найдем ф(16) = 8 – длина группы => порядки подгрупп: 1,2,4,8
      2. Z1 = {1},
      3. Z8 = Z16\*
      4. Для порядка 2 решим уравнение x^2 = 1 mod 16 => x^2 = 1 +16k =>   
         Z2 = {1,7},{1,9},{1,15}
      5. Для порядка 4 найдем просто все элементы с порядком 4, они будут образующими элементами своих подгрупп: {1,3,9,11}, {1,5,9,11}
   4. П=<Z17\*,X>
      1. Z17\* содержит все элементы, имеющие инверсию по умножению в Z17 => все элементы взаимно просты с 17 => найдем ф(17) = 16 – длина группы => порядки подгрупп: 1,2,4,8,16
      2. Z1 = {1},
      3. Z16 = Z17\*
      4. Для порядка 2 найдем все элементы с порядком 2: {1,16},
      5. Для порядка 4 найдем просто все элементы с порядком 4: {1,3,9,11}, {1,5,9,11}
      6. Для порядка 8 найдем просто все элементы с порядком 4: {1,9,13,15,16,8,4,2}
4. Используя теорему Лагранжа, найдите порядок всех потенциальных подгрупп для следующих групп:
   1. G=<Z18,+>

Делители 18 есть порядки подгрупп: 1,2,3,6,9,18

* 1. G=<Z29,+>

Делители 29 есть порядки подгрупп: 1,29

* 1. G=<Z12\*,+>

Делители Ф(12) есть порядки подгрупп: 1,2,4

* 1. G=<Z19,+>

Делители Ф(19) есть порядки подгрупп: 1,2,3,6,9,18

1. Найти порядок всех элементов в следующих группах:
   1. G=<Z8,+>

Ord(1) = 8, ord(2)=4, ord(3)=8, ord(4) = 2, ord(5) = 8, ord(6) = 8, ord(7) = 8, ord(0) = 1

* 1. G=<Z7,+>

Ord(1) = 7, ord(2)=7, ord(3)=7, ord(4) = 7, ord(5) = 7, ord(6) = 7, ord(7) = 7, ord(1) = 1

* 1. G=<Z9\*,x>

Ord(1) = 1, ord(2)=6, ord(4)=3, ord(5) = 6, ord(7) = 3, ord(8) = 2

* 1. G=<Z7\*,x>

Ord(1) = 1, ord(2)=3, ord(3)=6, ord(4) = 3, ord(5) = 6, ord(6) = 4

1. Найдите результаты после использования малой теоремы Ферма:
   1. 5^15 mod 13 = 5^12 \* 5^3 mod 13 = 5^3 mod 13 = 12\*5 mod 13 = 8
   2. 15^18 mod 17 = 15^16 \* 15^2 mod 17 = 225 mod 17 = 4
   3. 456^17 mod 17 = 456 mod 17 = 14
   4. 145 mod 101 = 44
2. Найдите, используя Малую теорему Ферма, результаты выражений, приведенных ниже:
   1. 5^-1 mod 13 = 5^11 mod 13 = 12^5 \* 5 mod 13 = 12\*5 mod 13 = 8
   2. 15^-1 mod 17 = 15^15 mod 17 = 8
   3. 27^-1 mod 41 = 27^39 mod 41 = 38
   4. 70^-1 mod 101 = 70^100 mod 101 = 13
3. Найдите, используя теорему Эйлера, результаты выражений, приведенных ниже:
   1. 12^-1 mod 77 = 12^59 mod 77 = 45
   2. 16^-1 mod 323 = 16^287 mod 323 = 25
   3. 20^-1 mod 403 = 20^359 mod 403 = 262
   4. 44^-1 mod 667 = 44^615 mod 101 = 379
4. Найдите весь QRs и QNRs в Z13\*,Z17\*,Z23\*.
   1. Z13\*

p = 13

1^6 = 1 mod 13 – QR

2^6 = 12 MOD 13 – QNR

3^6 = 1 MOD 13 – QR

4^6 = 1 MOD 13 – QR

5^6 = 12 MOD 13 – QNR

6^6 = 12 MOD 13 – QNR

7^6 = 12 MOD 13 – QNR

8^6 = 12 MOD 13 – QNR

9^6 = 1 MOD 13 – QR

10^6 = 1 MOD 13 – QR

11^6 = 12 MOD 13 – QNR

12^6 = 1 MOD 13 - QR

* 1. Z17\*

QR:1,2,4,8,9,13,15,16

QNR:3,5,6,7,10,11,12,14

* 1. Z23\*

QR:1,2,3,4,6,8,9,12,13,16,18

QNR:5,7,10,11,14,15,17,19,20,21,22

1. Используя квадратичные вычеты, решите следующие сравнения
   1. x^2 = 4 mod 7

7 = 4 \* 1 + 3 => 2 случай => x = 4^2 mod 7 =2 x = -4^2 mod 7 = 12

* 1. x^2 = 5 mod 11

7 = 4 \* 2 + 3 => 2 случай => x = 5^3 mod 11 =4 x = -5^3 mod 11 = 7

* 1. x^2 = 7 mod 13

7 – QNR => нет решений

* 1. x^2 = 12 mod 17

12 – QNR => нет решений

1. Используя квадратичные вычеты, решите следующие сравнения
   1. x^2 = 4 mod 14

x^2 = 4 mod 2 и x^2 = 4 mod 7

Для первого уравнения: x = 0

Для второго x =2 или x = 5

Составим две системы:

1. x = 0 mod 2 и x = 2 mod 7

x = 2

1. x = 0 mod 2 и x = 5 mod 7

x = 12

Тогда ответ: x = 2 + 14k и x = 12 + 14k

* 1. x^2 = 5 mod 10

x^2 = 5 mod 2 и x^2 = 5 mod 5

Для первого уравнения: x = 1

Для второго x =0

Составим систему:

x = 1 mod 2 и x = 0 mod 5

x = 5

Тогда ответ: x = 5 + 10k

* 1. x^2 = 7 mod 3

x^2 = 7 mod 11 и x^2 = 7 mod 3

Для первого уравнения: 7 – QNR => решения нет

* 1. x^2 = 12 mod 34

x^2 = 12 mod 17 и x^2 = 12 mod 2

Для первого уравнения: 12 – QNR => нет решения

1. Для группы G=<Z19\*,X>
   1. Найдите порядок группы

Ф(19) = 18 => порядок равен 18,так как каждый элемент от 1 до 18 будет иметь обратный по умножению элемент

* 1. Найдите прядок каждого элемента

Ord(1) = 1 ord(2) = 18 ord(3) = 18 ord(4) = 9 ord(5) = 9 ord(6) = 9 ord(7) = 3 ord(8) = 6 ord(9) = 9 ord(10) = 18 ord(11) = 3 ord(12) = 6 ord(13) = 18 ord(14) = 18 ord(15) = 18 ord(16) = 9 ord(17) = 9 ord(18) = 2

* 1. Найти число первообразных корней в группе: ф(ф(19)) = ф(18) = 18 \* ½ \* 2/3 = 6
  2. Найти первообразные корни в группе: 2, 3, 7, 10, 14, 15
  3. У нас есть первообразный корень 2. Все элементы группы являются его степенью => группы циклична

1. Реализовать класс вычисления целых степеней по заданному модулю(для вычисления положительной степени воспользоваться малой теоремой Ферма и реализованными отдельном методами умножения и сложения по заданному модулю, для вычисления отрицательной степени воспользоваться теоремой Эйлера).

Для решения данной задачи был реализован класс с функциями сложения и умножения по модулю.

Сначала отрицательная степень сдвигается в положительную сторону. Затем по малой Теореме Ферма происходит ее сокращение. После этого оставшуюся степень получают через умножение по модулю

**Вывод:** Было изучено применение китайской теоремы об остатках.