**Họ và tên: Nguyễn Bảo Đạt**

**MSV: AT141010**

**Lớp: AT14L**

**Môn học: Cơ sở Lý thuyết Mật mã**

**CHƯƠNG 1**

**Bài 9:**

a = 1573; b = 308

Đặt (A1,A2,A3) = (1,0,1573)

(B1,B2,B3) = (0,1,308)

Q = A3/B3 = 5

Đặt (A1,A2,A3) = (0,1,308)

(B1,B2,B3) = (1,-4,33)

Q = 9

(A1,A2,A3) = (1,-4,33)

(B1,B2,B3) = (-9,37,11)

Q = 3

(A1,A2,A3) = (-9,37,11)

(B1,B2,B3) = (28,-115,0)

Vì B3 = 0 nên UCLN(1573,308) = A3 = 11

**Bài 10:**

3^22 mod 23 = ?

Thuật toán:

a = 3; k=22; n =23

ki = 10110; t=4

Gán b = 1; nếu k = 0 return 1;

Gán A = a; nếu ki = 1 => b = a;

for(i=0; i<=t; i++)

A = A^2 mod n;

Nếu ki=1 => b = A.b mod n;

Return b;

Bảng mô tả các bước trên:

i | 0 1 2 3 4

ki| 0 1 1 0 1

A| 3 9 12 6 13

b | 1 9 16 16 1

Vậy 3^22 mod 23 = 1

**Bài 11:**

Tính các căn bậc 2 của 12 mod 37

(Dùng thuật toán sgk/43)

a = 12, p = 37

Tính Legendre (12/37)

(12/37) = (2/37)^3 \* (4/37) = (-1)^3 \* (37/4)

= -1\* (1/4) = -(1/4) = -1

=> 12 mod 37 không có căn bậc 2

**Bài 12:**

phi(19) = 19-1 = 18 = 2\*3^2

Tìm các phần tử nguyên thủy sao cho:

x^(18/2) mod 37 != 1 <=> x^9 mod 37 != 1

x^(18/3) mod 37 != 1 x^6 mod 37 != 1

Xét x = 2 <=> 2^9 mod 37 = 31 != 1

2^6 mod 37 = 27 != 1

=> 2 là phần tử nguyên thủy của Z19

Để UCLN(i,phi(19)) = 1 thì i thuộc Z18;

Z18 = {1,5,7,11,13,17}

2^1 mod 19 = 2; 2^5 mod 19 = 13

2^7 mod 19 = 14; 2^11 mod 19 = 15

2^13 mod 19 = 3; 2^17 mod 19 = 10

Vậy các phần tử nguyên thủy của nhóm nhân Z19 là:

{2,3,10,13,14,15}

**Bài 13:**

Tìm phần tử nghịch đảo của 3 trong Z31

Gọi x là phần tử nghịch đảo của 3; Ta có:

3x = 1 (mod 31)

<=> 3x - 1 = 31k (k=1,2,3...)

<=> x = 21

**Bài 15:**

Tính phi(490); phi(768)

a/phi(490)

490 = 2\*5\*7^2

phi(490) = 490\*(1-1/2)\*(1-1/5)\*(1-1/7) = 168

b/phi(768)

768 = 2^8\*3

phi(768) = 768\*(1-1/2)\*(1-1/3) = 1024

**Bài 16:**

Giari hệ PT đồng dư:

5x = 20 mod 6

6x = 6 mod 5

4x = 5 mod 77

x = 4 mod 6 (1)

<=> x = 1 mod 5 (2)

x = 3 mod 7 (3)

M = 6\*5\*7 = 210

M1 = 35; M2 = 42; M3 = 30

35y1 = 4 mod 6 <=> y1 = 2

42y2 = 1 mod 5 <=> y2 = 3

30y3 = 3 mod 7 <=> y3 = 5

=> x = M1\*y1 + M2\*y2 + M3\*y3 mod M

= 346 mod 210 = 136 mod 210

**Bài 17:**

Dùng Euclide mở rộng để tính

a/ 17^(-1) mod 101

Đặt (A1,A2,A3) = (1,0,101)

(B1,B2,B3) = (0,1,17)

Q = 5

(A1,A2,A3) = (0,1,17)

(B1,B2,B3) = (1,-5,16)

Q = 1

(A1,A2,A3) = (1,-5,16)

(B1,B2,B3) = (-1,6,1)

Vì B3 = 1 nên 17^(-1) mod 101 = B2 = 6

b/ 357^(-1) mod 1234

Đặt (A1,A2,A3) = (1,0,1234)

(B1,B2,B3) = (0,1,357)

Q = 3

(A1,A2,A3) = (0,1,357)

(B1,B2,B3) = (1,-3,163)

Q = 2

(A1,A2,A3) = (1,-3,163)

(B1,B2,B3) = (-2,7,31)

Q = 5

(A1,A2,A3) = (-2,7,31)

(B1,B2,B3) = (11,-38,8)

Q = 3

(A1,A2,A3) = (11,-38,8)

(B1,B2,B3) = (-35,121,7)

Q = 1

(A1,A2,A3) = (-35,121,7)

(B1,B2,B3) = (-24,-159,1)

Vì B3 = 1 nên 357^(-1) mod 1234 = B2 = -159

c/ 3125^(-1) mod 9987

Đặt (A1,A2,A3) = (1,0,9987)

(B1,B2,B3) = (0,1,3125)

Q = 3

(A1,A2,A3) = (0,1,3125)

(B1,B2,B3) = (1,-3,612)

Q = 5

(A1,A2,A3) = (1,-3,612)

(B1,B2,B3) = (-5,16,65)

Q = 9

(A1,A2,A3) = (-5,16,65)

(B1,B2,B3) = (46,-147,27)

Q = 2

(A1,A2,A3) = (46,-147,27)

(B1,B2,B3) = (-97,310,11)

Q = 2

(A1,A2,A3) = (-97,310,11)

(B1,B2,B3) = (240,-767,5)

Q = 2

(A1,A2,A3) = (240,-767,5)

(B1,B2,B3) = (-577,1844,1)

Vì B3 = 1 nên 3125^(-1) mod 9987 = B2 = 1844