**AN TOÀN HỆ THỐNG THÔNG TIN**

**Nhóm 2**

**Thành viên nhóm:** + Trần Thanh Hiệp – 2151050469

+ Bùi Thị Ngân – 2151050271

+ Lê Trí Cường – 2151053007

+ Lê Trung Hiếu – 2151050128

+ Nguyễn Song Hậu – 2151050123

+ Nguyễn Văn Cảnh – 2151053005

+ Nguyễn Hữu Toàn – 2151050462

+ Nguyễn Y Khoa – 2151500202

**Bài tập thuật mã 4 - Thuật toán Euclide mở rộng**

ĐỀ BÀI:

1. Hãy tìm số nghịch đảo modulo 26 của 3 bằng thuật toán Euclide mở rộng
2. Hãy tìm số nghịch đảo modulo 26 của 5 bằng thuật toán Euclide mở rộng
3. Hãy tìm số nghịch đảo modulo 26 của 23 bằng thuật toán Euclide mở rộng
4. Hãy tìm số nghịch đảo modulo 26 của 25 bằng thuật toán Euclide mở rộng
5. Hãy tìm số nghịch đảo modulo 26 của 13 bằng thuật toán Euclide mở rộng
6. Hãy tìm số nghịch đảo modulo 26 của 11 bằng thuật toán Euclide mở rộng
7. Hãy tìm số nghịch đảo modulo 26 của 17 bằng thuật toán Euclide mở rộng
8. Hãy tìm số nghịch đảo modulo 26 của 19 bằng thuật toán Euclide mở rộng
9. Hãy tìm số nghịch đảo modulo 26 của 23 bằng thuật toán Euclide mở rộng
10. Hãy tìm số nghịch đảo modulo 26 của 21 bằng thuật toán Euclide mở rộng

BÀI GIẢI:

**Câu 1: Hãy tìm số nghịch đảo modulo 26 của 3 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **X** | **B** | **Y** |
| **1** | 26 | 0 |  |
| **2** | 3 | 1 | **8** |
| **3** | **2** | **-8** | **1** |
| **4** | **1** | **9** | **2** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 3 = 8

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 3 = 2

Y3 = X3-1 div X3 = X2 div X3 = 3 div 2 = 1

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 8) = -8

X4 = X4-2 mod X4-1 = X2 mod X3 = 3 mod 2 = 1

Y4 = X4-1 div X4 = X3 div X4 = 2 div 1 = 2

B4 = B4-2 – (B4-1 \* Y4-1) = B2 – (B3 – Y3) = 1 – (-8 \* 1) = 9

* 3-1 mod 26 = 9

**Câu 2: Hãy tìm số nghịch đảo modulo 26 của 5 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | **X** | **B** | **Y** |
| **1** | 26 | 0 |  |
| **2** | 5 | 1 | **5** |
| **3** | **1** | **-5** | **5** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 5 = 5

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 5 = 1

Y3 = X3-1 div X3 = X2 div X3 = 5 div 1 = 5

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 5) = -5

* 5-1 mod 26 = (-5 + 26) = 21

**Câu 3: Hãy tìm số nghịch đảo modulo 26 của 23 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 23 | 1 | **1** |
| 3 | **3** | **-1** | **7** |
| 4 | **2** | **8** | **1** |
| 5 | **1** | **-9** | **2** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 23 = 1

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 23 = 3

Y3 = X3-1 div X3 = X2 div X3 = 23 div 3 = 7

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 1) = -1

X4 = X4-2 mod X4-1 = X2 mod X3 = 23 mod 3 = 2

Y4 = X4-1 div X4 = X3 div X4 = 3 div 2 = 1

B4 = B4-2 – (B4-1 \* Y4-1) = B2 – (B3 – Y3) = 1 – (-1 \* 7) = 8

X5 = X5-2 mod X5-1 = X3 mod X4 = 3 mod 2 = 1

Y5 = X5-1 div X5 = X4 div X5 = 2 div 1 = 2

B5 = B5-2 – (B5-1 \* Y5-1) = B3 – (B4 \* Y4) = -1 – (8 \* 1) = -9

* 23-1 mod 26 = (-9 + 26) = 17

**Câu 4: Hãy tìm số nghịch đảo modulo 26 của 25 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 25 | 1 | **1** |
| 3 | **1** | **-1** | **25** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 25 = 1

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 25 = 1

Y3 = X3-1 div X3 = X2 div X3 = 25 div 1 = 25

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 1) = -1

* 25-1 mod 26 = (-1 + 26) = 25

**Câu 5: Hãy tìm số nghịch đảo modulo 26 của 13 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 13 | 1 |  |
| 3 |  |  |  |

Để tồn tại số nghịch đảo modulo 26 của 13 thì 13 và 26 phải là số nguyên tố cùng nhau. Có thể thấy GCD (13, 26) = 13. Do đó không có số nghịch đảo modulo 26 của 13

**Câu 6: Hãy tìm số nghịch đảo modulo 26 của 11 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 11 | 1 | **2** |
| 3 | **4** | **-2** | **2** |
| 4 | **3** | **5** | **1** |
| 5 | **1** | **-7** | **3** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 11 = 2

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 11 = 4

Y3 = X3-1 div X3 = X2 div X3 = 11 div 4 = 2

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 2) = -2

X4 = X4-2 mod X4-1 = X2 mod X3 = 11 mod 4 = 3

Y4 = X4-1 div X4 = X3 div X4 = 4 div 3 = 1

B4 = B4-2 – (B4-1 \* Y4-1) = B2 – (B3 – Y3) = 1 – (-2 \* 2) = 5

X5 = X5-2 mod X5-1 = X3 mod X4 = 4 mod 3 = 1

Y5 = X5-1 div X5 = X4 div X5 = 3 div 1 = 3

B5 = B5-2 – (B5-1 \* Y5-1) = B3 – (B4 \* Y4) = -2 – (5 \* 1) = -7

* 11-1 mod 26 = (-7 + 26) = 19

**Câu 7: Hãy tìm số nghịch đảo modulo 26 của 17 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 17 | 1 | **1** |
| 3 | **9** | **-1** | **1** |
| 4 | **8** | **2** | **1** |
| 5 | **1** | **-3** | **8** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 17 = 1

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 17 = 9

Y3 = X3-1 div X3 = X2 div X3 = 17 div 9 = 1

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 1) = -1

X4 = X4-2 mod X4-1 = X2 mod X3 = 17 mod 9 = 8

Y4 = X4-1 div X4 = X3 div X4 = 9 div 8 = 1

B4 = B4-2 – (B4-1 \* Y4-1) = B2 – (B3 – Y3) = 1 – (-1 \* 1) = 2

X5 = X5-2 mod X5-1 = X3 mod X4 = 9 mod 8 = 1

Y5 = X5-1 div X5 = X4 div X5 = 8 div 1 = 8

B5 = B5-2 – (B5-1 \* Y5-1) = B3 – (B4 \* Y4) = -1 – (2 \* 1) = -3

* 17-1 mod 26 = (-3 + 26) = 23

**Câu 8: Hãy tìm số nghịch đảo modulo 26 của 19 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 19 | 1 | **1** |
| 3 | **7** | **-1** | **2** |
| 4 | **5** | **3** | **1** |
| 5 | **2** | **-4** | **2** |
| 6 | **1** | **11** | **2** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 19 = 1

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 19 = 7

Y3 = X3-1 div X3 = X2 div X3 = 19 div 7 = 2

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 1) = -1

X4 = X4-2 mod X4-1 = X2 mod X3 = 19 mod 7 = 5

Y4 = X4-1 div X4 = X3 div X4 = 7 div 5 = 1

B4 = B4-2 – (B4-1 \* Y4-1) = B2 – (B3 – Y3) = 1 – (-1 \* 2) = 3

X5 = X5-2 mod X5-1 = X3 mod X4 = 7 mod 5 = 2

Y5 = X5-1 div X5 = X4 div X5 = 5 div 2 = 2

B5 = B5-2 – (B5-1 \* Y5-1) = B3 – (B4 \* Y4) = -1 – (3 \* 1) = -4

X6 = X6-2 mod X6-1 = X4 mod X5 = 5 mod 2 = 1

Y6 = X6-1 div X6 = X5 div X6 = 2 div 1 = 2

B6 = B6-2 – (B6-1 \* Y6-1) = B4 – (B5 \* Y5) = 3 – (-4 \* 2) = 11

* 19-1 mod 26 = 11

**Câu 9: Hãy tìm số nghịch đảo modulo 26 của 23 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 23 | 1 | **1** |
| 3 | **3** | **-1** | **7** |
| 4 | **2** | **8** | **1** |
| 5 | **1** | **-9** | **2** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 23 = 1

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 23 = 3

Y3 = X3-1 div X3 = X2 div X3 = 23 div 3 = 7

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 1) = -1

X4 = X4-2 mod X4-1 = X2 mod X3 = 23 mod 3 = 2

Y4 = X4-1 div X4 = X3 div X4 = 3 div 2 = 1

B4 = B4-2 – (B4-1 \* Y4-1) = B2 – (B3 – Y3) = 1 – (-1 \* 7) = 8

X5 = X5-2 mod X5-1 = X3 mod X4 = 3 mod 2 = 1

Y5 = X5-1 div X5 = X4 div X5 = 2 div 1 = 2

B5 = B5-2 – (B5-1 \* Y5-1) = B3 – (B4 \* Y4) = -1 – (8 \* 1) = -9

* 23-1 mod 26 = (-9 + 26) = 17

**Câu 10: Hãy tìm số nghịch đảo modulo 26 của 21 bằng thuật toán Euclide mở rộng**

|  |  |  |  |
| --- | --- | --- | --- |
|  | X | B | Y |
| 1 | 26 | 0 |  |
| 2 | 21 | 1 | **1** |
| 3 | **5** | **-1** | **4** |
| 4 | **1** | **5** | **5** |

Y2 = X2-1 div X2 = X1 div X2 = 26 div 21 = 1

X3 = X3-2 mod X3-1 = X1 mod X2 = 26 mod 21 = 5

Y3 = X3-1 div X3 = X2 div X3 = 21 div 5 = 4

B3 = B3-2 – (B3-1 \* Y3-1) = B1 – (B2 \* Y2) = 0 – (1 \* 1) = -1

X4 = X4-2 mod X4-1 = X2 mod X3 = 21 mod 5 = 1

Y4 = X4-1 div X4 = X3 div X4 = 5 div 1 = 5

B4 = B4-2 – (B4-1 \* Y4-1) = B2 – (B3 – Y3) = 1 – (-1 \* 4) = 5

* 21-1 mod 26 = 5