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

**Nhóm 1**

* Hồ Phan Tấn Khoa
* Trần Minh Bảo Long
* Lê Văn Hiếu
* Phan Minh Thuận
* Trịnh Thanh Hải
* Nguyễn Minh Sang
* Phan Hoàng Triều
* Lê Trương Minh Hoàng
* **1. Hãy tìm số nghịch đảo modulo 26 của 3 bằng thuật toán Euclide mở rộng**

**3(-1) mod 26 Hoàng**

**USCLN(26, 3) = 1 => Có nghịch đảo modulo 26 của 3**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **3** |  | **0** | **1** |
| **1** | **2** | **8** | **1** | **-8** |
| **2** | **1** | **1** | **-1** | **9** |
| **3** | **0** | **2** | **3** | **-26** |

**Kết quả: 3(-1) mod 26 = 9**

* **2. Hãy tìm số nghịch đảo modulo 26 của 5 bằng thuật toán Euclide mở rộng (Hải)**

**5(-1) mod 26**

**USCLN(26, 5) = 1 => Có nghịch đảo modulo 26 của 5**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **5** |  | **0** | **1** |
| **1** | **1** | **5** | **1** | **-5** |
| **2** | **0** | **5** | **-5** | **26** |

**Kết quả: 5(-1) mod 26 = -5 (-mod 26) = -5 + 26 = 21**

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

**23(-1) mod 26 Hoàng**

**USCLN(26, 23) = 1 => Có nghịch đảo**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **23** |  | **0** | **1** |
| **1** | **3** | **1** | **1** | **-1** |
| **2** | **2** | **7** | **-7** | **8** |
| **3** | **1** | **1** | **8** | **-9** |
| **4** | **0** | **2** | **-23** | **26** |

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

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

**25(-1) mod 26 (Hải)**

**USCLN(26, 25) = 1**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **25** |  | **0** | **1** |
| **1** | **1** | **1** | **1** | **-1** |
| **2** | **0** | **25** | **-25** | **26** |

**Kết quả: 25(-1) mod 26 = -1 + (-mod 26) = -1 + 26 = 25**

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

**13(-1) mod 26**

**USCLN(26, 13) = 13 # 1 => Không có nghịch đảo modulo 26 của 13**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **13** |  | **0** | **1** |
| **1** | **0** | **2** |  |  |

**Kết quả: 13(-1) mod 26 = Không tồn tại nghịch đảo modulo 26 của 13**

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

**11(-1) mod 26**

**USCLN(26, 11) = 1 => Có nghịch đảo modulo 26 của 11**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **11** |  | **0** | **1** |
| **1** | **4** | **2** | **1** | **-2** |
| **2** | **3** | **2** | **-2** | **5** |
| **3** | **1** | **1** | **3** | **-7** |
| **4** | **0** | **3** | **-11** | **26** |

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

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

**17(-1) mod 26**

**USCLN(26, 17) = 1 => Có nghịch đảo**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **17** |  | **0** | **1** |
| **1** | **9** | **1** | **1** | **-1** |
| **2** | **8** | **1** | **-1** | **2** |
| **3** | **1** | **1** | **2** | **-3** |
| **4** | **0** | **8** | **-17** | **26** |

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

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

**19(-1) mod 26 (Long)**

**USCLN(26, 19) = 1**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **19** |  | **0** | **1** |
| **1** | **7** | **1** | **1** | **-1** |
| **2** | **5** | **2** | **-2** | **3** |
| **3** | **2** | **1** | **3** | **-4** |
| **4** | **1** | **2** | **-8** | **11** |
| **5** | **0** | **2** | **19** | **-26** |

**Kết quả: 19(-1) mod 26 = 11**

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

**23(-1) mod 26 Hoàng**

**USCLN(26, 23) = 1 => Có nghịch đảo**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **23** |  | **0** | **1** |
| **1** | **3** | **1** | **1** | **-1** |
| **2** | **2** | **7** | **-7** | **8** |
| **3** | **1** | **1** | **8** | **-9** |
| **4** | **0** | **2** | **-23** | **26** |

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

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

**21(-1) mod 26**

**USCLN(26, 21) = 1 => Có nghịch đảo modulo 26 của 11**

**y(i) = y(i-2) - q(i)\*y(i-1)**

**x(i) = x(i-2) - q(i)\*x(i-1)**

| **i** | **ri** | **qi** | **xi** | **yi** |
| --- | --- | --- | --- | --- |
| **-1** | **26** |  | **1** | **0** |
| **0** | **21** |  | **0** | **1** |
| **1** | **5** | **1** | **1** | **-1** |
| **2** | **1** | **4** | **-4** | **5** |
| **3** | **0** | **5** | **21** | **-26** |

**Kết quả: 21(-1) mod 26 = 5**