

Giải thuật Euclid

Phạm Nguyễn Khang

USCLN

- Ước số chung lớn nhất
 - $c = \text{USCLN}(a, b)$
 - c là ước số của a và b
 - Bất cứ ước số chung nào của a và b đều là ước số của c
 - Ví dụ: $\text{USCLN}(60, 24) = \text{USCLN}(60, -24) = 12$
 - $\text{USCLN}(0, a) = a$

Giải thuật Euclid tìm USCLN

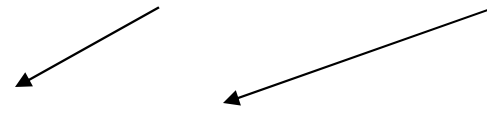
- USCLN(a,b)

1. $A = a, B = b$
2. If $B = 0$ return A
3. $R = A \bmod B$
4. $A = B$
5. $B = R$
6. Lặp lại bước 2

```
int USCLN(int a, int b)
{
    while (b != 0) {
        int r = a%b;
        a = b;
        b = r;
    }
    return a;
}
```

Giải thuật Euclid tìm USCLN

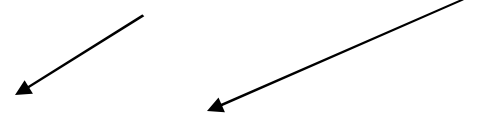
- $A_1 = B_1 * Q_1 + R_1$



- $A_2 = B_2 * Q_2 + R_2$



- $A_3 = B_3 * Q_3 + R_3$



- $A_4 = B_4 * Q_4 + R_4$

- ...

- Tìm USCLN(12,8)

- $12 = 8 * 1 + 4$

- $8 = 4 * 2 + 0$

- Vậy USCLN(12,8) = 4

Số nghịch đảo theo modulo n

- Nếu $\text{USCLN}(a, n) = 1$ thì luôn tồn tại b ($b < n$) sao cho:
 - $b = a^{-1} \pmod n$ hay $ab \equiv 1 \pmod n$
 - Ta gọi b là số nghịch đảo của a theo modulo n .
- Ví dụ:
 - $5 * 2 \equiv 1 \pmod 9$ hay $2 = 5^{-1} \pmod 9$

Giải thuật Euclid tìm số nghịch đảo theo modulo n

- USCLN(n, a)

1. $(A1, A2, A3) = (1, 0, n), (B1, B2, B3) = (0, 1, a)$
2. if $(B3 = 0)$ return A3, không tồn tại a^{-1}
3. if $(B3 = 1)$ return B3, $a^{-1} = B2$
4. $Q = A3 \text{ div } B3$ //chia lấy phần nguyên
5. $(T1, T2, T3) =$
 $(A1 - Q*B1, A2 - Q*B2, A3 - Q*B3)$
 1. $(A1, A2, A3) = (B1, B2, B3)$
 2. $(B1, B2, B3) = (T1, T2, T3)$
 3. Lặp lại bước 2

Ví dụ

- Tính $b = 7^{-1} \bmod 187$

Q	A1	A2	A3	B1	B2	B3	T1	T2	T3
	1	0	187	0	1	7			
26	0	1	7	1	-26	5	1	-26	5
1	1	-26	5	-1	27	2	-1	27	2
2	-1	27	2	3	-80	1	3	-80	1

- Vậy $b = -80 \bmod 187$ hay $= 187 - 80 = 107$