CƠ SỞ TOÁN HỌC

GIẢNG VIÊN: LÊ QUỐC ANH

NỘI DUNG

1. Modulo số học.
2. Vành đồng dư modulo N ($\mathbf{Z_n}$).
3. Phần tử nghịch đảo trên vành $\mathbf{Z_n}$.
4. Thuật toán Ơclid mở rộng.
5. Hàm phi Ơle.
6. Thuật toán lũy thừa nhanh.

1. Modulo số học.

- Ta có a ≡ b(mod n) nếu a = kn + b trong đó k là một số nguyên.
- Nếu a và b dương và a nhỏ hơn n, chúng ta có thể gọi a là phần dư của b khi chia cho n.
- Người ta còn gọi b là thặng dư của a theo modulo n, và a là đồng dư của b theo modulo n

<u>Ví dụ:</u>

- Ta có: 42=4.9+6 vậy 42 ≡6 (mod 9)
- Ta có câu hỏi; -42 ≡? (mod9), ta thấy -42= -4.9-6
- -42 ≡ -6 (mod 9) nhưng -6 ≡ -6+9 ≡ 3 (mod 9)
- Vậy nên -42 ≡ 3 (mod 9)

1. Modulo số học.

- Modulo số học cũng giống như số học bình thường, bao gồm các phép giao hoán, kết hợp và phân phối.

$$(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$$

$$(a \times b) \bmod n = ((a \bmod n) \times (b \bmod n)) \bmod n$$

$$(a \times (b + c)) \bmod n = (((a \times b) \bmod n) + ((a \times c) \bmod n)) \bmod n$$

- Các phép tính trong các hệ mã mật hầu hết đều thực hiện đối với một modulo N nào đó.

2. Vành đồng dư modulo N ($\mathbf{Z_n}$).

Vành:

- ***Định nghĩa:*** Tập hợp **R** được gọi là vành nếu trên đó có hai phép toán hai ngôi mà ta ký hiệu là "+" (phép cộng) và "." (phép nhân) thỏa mãn các điều kiện sau:

1. **R** là một nhóm giao hoán đối với phép cộng, nghĩa là:
    1. Phép cộng có tính kết hợp: $\forall x, y, z \in R$:$(x+y)+z = x+(y+z)$
    2. Phép cộng có phần tử trung hòa, nghĩa là $\exists 0 \in R, \forall x \in R$:$0+x = x+0 = x$
    3. Mọi phần tử của **R** có phần tử đối: $\forall x, \exists x' : x + x' = x' + x = 0$
    4. Phép cộng có tính giao hoán, nghĩa là: $\forall x, y \in R : x + y = y + x$
2. Phép nhân có tính phân phối với phép cộng, nghĩa là $\forall x, y, z \in R : x.(y+z) = x.y + x.z$
3. Phép nhân có tính kết hợp, nghĩa là $\forall x, y, z \in R : (x.y).z = x.(y.z)$
4. Phép nhân có phần tử đơn vị, nghĩa là $\exists 1 \in R, \forall x \in R : 1 * x = x * 1 = x$

2. Vành đồng dư modulo N ($\mathbf{Z_n}$).

- Tập các số nguyên Z_N = {0, 1, …, N-1} trong đó N là một số tự nhiên dương với hai phép toán cộng (+) và nhân (.) được định nghĩa như:
  - **Phép cộng**: $\forall\, a, b \in Z_n : a + b = (a + b) mod\ N$
  - **Phép nhân:** $\forall\, a, b \in Z_n : a.b = (a.b) mod\ N$
- Theo tính chất của modulo số học chúng ta dễ dàng nhận thấy Z_N là một vành giao hoán và kết hợp. Hầu hết các tính toán trong các hệ mã mật đều được thực hiện trên một vành Z_N nào đó.

3. Phần tử nghịch đảo trên vành Z_N

- Trên một vành số nguyên Z_N người ta đưa ra khái niệm về số nghịch đảo của một số như sau:
- **(GCD-Greatest Common Divisor)** ước số chung lớn nhất.

Giả sử a $\in Z_N$ và tồn tại b $\in Z_N$ sao cho a.b = (a*b) mod N = 1. Khi đó b được gọi là phần tử nghịch đảo của a trên Z_N và ký hiệu là a^{-1} = b.

Việc tìm phần tử nghịch đảo của một số a $\in Z_N$ cho trước thực chất tương đương với việc tìm hai số b và k sao cho: a.b = k.N + 1 trong đó b, k $\in Z_N$. Hay viết gọn lại là:

$$a^{-1} \equiv b \pmod N$$

Định lý về sự tồn tại của phần tử nghịch đảo : Nếu GCD(a, N) = 1 thì tồn tại duy nhất 1 số b $\in Z_N$ là phần tử nghịch đảo của a, nghĩa là thỏa mãn a.b = (a*b) mod N = 1.

4. Thuật toán Ơclid mở rộng.

```
Procedure Euclid_Extended (a,m)
int,  y0=0,y1:=1;

While a>0 do {
     r:= m mod a
     if r=0 then Break
     q:= m div a
     y:= y0-y1*q
     m:=a
     a:=r
     y0:=y1
     y1:=y
  }
 If a>1 Then Return "A không khả nghịch theo mođun m"
 else Return " Nghịch đảo modulo m của a là y"
```

Tìm phần tử nghịc đảo của 30 trên Z_{101}

Bước i	m	a	r	q	y0	y1	y
0	101	30	11	3	0	1	-3
1	30	11	8	2	1	-3	7
2	11	8	3	1	-3	7	-10
3	8	3	2	2	7	-10	27
4	3	2	1	1	-10	27	-37
5	2	1	0	.	.	.	.

Nếu y là số âm thì cộng với m chúng ta Thu được giá trị nghịch đảo.

5. Hàm phi Ơle

- Với mỗi số nguyên N, giá trị hàm phi Ơle của N là tổng tất cả các số nguyên $\in Z_N$ nguyên tố cùng nhau với N.
- Nếu N là số nguyên tố: $\emptyset(N) = N - 1$
- Nếu N = p * q, trong đó p,q là số nguyên tố: $\emptyset(N) = (p-1) * (q-1)$
- Trong trường hợp tổng quát: N = $p_1^{\alpha_1}.p_2^{\alpha_2} \dots p_k^{\alpha_k}$ trong đó p_i là các số nguyên tố, α_i là các số nguyên dương. Ta tính được:

$$\emptyset(N) = (p_1 - 1)p_1^{\alpha_1 - 1}(p_2 - 1)p_2^{\alpha_2 - 1} \dots (p_k - 1)p_k^{\alpha_k - 1}$$

5. Hàm phi Ơle

- ***Định lý Ơle***: nếu n là số nguyên dương bất kỳ và a là số nguyên tố cùng nhau với n, thì: $a^{\varphi(n)} \equiv 1 \, mod \, (n)$.
- ***Chứng minh***: Gọi $a_1, a_2, \cdots, a_{\varphi(n)}$ là các số nguyên dương nhỏ hơn n và nguyên tố cùng nhau với n. Với mọi 2 số phân biệt $i, j \in \{1,2, \ldots \varphi(n)\}$.

$$(a_i, n) = (a_j, n) = 1 \Rightarrow (aa_i, n) = (aa_j, n) = 1; aa_i \not\equiv aa_j \pmod{n}$$

- Do vậy $aa_1, aa_2, \cdots, aa_{\varphi(n)}$ là một hoán vị theo mô-đun n của $a_1, a_2, \cdots, a_{\varphi(n)}$
- Suy ra $a_1 a_2 \cdots a_{\varphi(n)} \equiv (aa_1)(aa_2) \cdots (a_{\varphi(n)}) \equiv a^{\varphi(n)} a_1 a_2 \cdots a_{\varphi(n)} \pmod{n}$
- Giản ước đồng dư thức, $a^{\varphi(n)} \equiv 1 \, mod \, (n)$.

5. Hàm phi Ơle

- Trường hợp riêng của định lý Ơle là định lý fecma nhỏ:
- Nếu P là một số nguyên tố thì $\forall a \in Z_P^*$ ta có $a^{p-1} \equiv 1 \, mod \, (p)$

6. Thuật toán lũy thừa nhanh.

Đầu vào: a,n,m.

Đầu ra: a^nmod m

```
Function Power_Modulo(Int x,n,m){
  Var Int Power:=1
  For i=1 to k do {
      Power:=(Power^2) mod m
      If b[i]=1 then
      Power:=(Power*x) mod m
  Return Power
}
```

-Bước 1: Đổi n ra dạng nhị phân.

- Bước 2: Áp dụng giải thuật lũy thừa nhanh.

Ví dụ: Tính 37^{27} mod 101. Đổi $27_2 = 11011$

$b[i]$	$p = p^2$	$p = p \pmod{101}$	$p * x$	$p = \pmod{101}$
1	$1^2 = 1$	1	$1 * 37 = 37$	37
1	$37^2 = 1369$	56	$56 * 37 = 2072$	52
0	$52^2 = 2704$	78	-	78
1	$78^2 = 6084$	24	$24 * 37 = 888$	80
1	$80^2 = 6400$	37	$37 * 37 = 1369$	56

Như vậy ta có: 37^{27} mod 101 = 56