COURSE TECHNOLOGY
CENGAGE Learning™

BẢO MẬT THÔNG TIN

Đàm Quang Viễn

Chương 1

GIỚI THIỆU

Câu hỏi ôn tập

1. Nêu các hình thức tấn công trong quá trình truyền tin trên mạng.
2. Bảo vệ thông tin trong quá trình truyền đi trên mạng là gì?
3. Bảo vệ hệ thống khỏi sự tấn công bên ngoài là gì?
4. Trình bày mô hình mạng an toàn

Bài tập của học viên

1. Tính giá trị các biểu thức theo modulo sau:

1) 12 mod 8 = 4 vì 12 = 1.8 + 4 (a=qn+b)
2) 23 mod 5
3) 53 mod 7
4) 120 mod 7
5) 520 mod 7
6) 8 mod 9 + 7 mod 9
7) 8 mod 9 * 7 mod 9
8) 5 mod 11 – 9 mod 11
9) 5/6 mod 7

Bài tập của học viên

2. Tính giá trị các biểu thức theo modulo sau

1) (-546) mod 13 - 347 mod 11
2) (1234 + 2345) mod 17
3) (213 * 345) mod 19
4) 15^{-1} mod 101
5) 41^{-1} mod 100
6) 14^{35} mod 11
7) (235*126/13) mod 19
8) 31^{130} mod 23

Bài tập của học viên (VN)

3. Tính hàm Ơle của các số nguyên sau:

- 12, 17, 21, 32, 36, 40, 72, 256.

4. Dùng Định lý Ferma và Định lý Ole tính các biểu thức sau

- 6^{16} mod 17; 15^{15} mod 17; 95^{100} mod 101
- 7^{4} mod 10; 9^{5} mod 10; 10^{12} mod 21; 91^{90} mod 100;

5. Giải các phương trình modulo sau

- x mod 11 = 3; x mod 13 = 6
- y mod 51 = 11; y mod 100 = 15
- z mod 12 = 5; z mod 17 = 8; z mod 23 = 11.

Bài tập của học viên (VN)

6. Sử dụng định lý phần dư Trung Hoa tính giá trị các biểu thức sau

- 25^{30} mod (7*8)
- 70^{254} mod (11*13)
- 60^{-1} mod (11*13)
- $((21^{100} + 33^{-1}).\ 45^{51})$ mod (7.9.11)

Bài tập trắc nghiệm

https://forms.gle/484y434aYy3F7eBK6

Hoặc

https://byvn.net/B5mm

Số học trên Modulo

- **Định nghĩa Modulo**

Cho số tự nhiên n và số nguyên a. Ta định nghĩa:

a mod n là phần dư dương khi chia a cho n.

- Định nghĩa quan hệ tương đương trên tập số nguyên

$$a \equiv b \bmod n$$

khi và chỉ khi a và b có phần dư như nhau khi chia cho n.

Ví dụ: 100 mod 11 = 1; 34 mod 11 = 1,

nên $100 \equiv 34 \bmod 11$

Số học trên Modulo

Số b được gọi là đại diện của a,
nếu $a \equiv b \bmod n$,

$(a = qn + b)$ và $0 \le b < n$.

Ví dụ:

$-12 \bmod 7 \equiv -5 \bmod 7$

$-5 \bmod 7 \equiv 2 \bmod 7$

$2 \bmod 7 \equiv 9 \bmod 7$

Ở đây 2 là đại diện của –12, -5, 2 và 9.

Số học trên Modulo

Ước số

Số b không âm được gọi là ước số của a, nếu có số m sao cho:

$$a = m.b$$

trong đó a, b, m đều nguyên.

Tức là a chia hết cho b, ký hiệu là $b|a$

Số học trên Modulo

Các phép toán số học trên Modulo

- (a+b) mod n = [a mod n + b mod n] mod n   (*)
- (a.b) mod n = [a mod n . b mod n] mod n (**)
- Nếu (a+b)≡(a+c) mod n, thì b≡c mod n
- Nhưng (ab)≡(ac) mod n, thì b≡c mod n ⇔(a,n)=1

  (a là nguyên tố cùng nhau với n)

Số học trên Modulo

Ví dụ:

Tính giá trị các biểu thức theo modulo sau:

$(11*19 + 10^{17}) \bmod 7$

$= ((11*19) \bmod 7 + 10^{17} \bmod 7) \bmod 7$

$= ((11 \bmod 7 * 19 \bmod 7) \bmod 7 \quad +$

$(10 \bmod 7)^{17} \bmod 7) \bmod 7$

$= ((4.(-2)) \bmod 7 + (((3^2)^2)^2)^2 * 3 \bmod 7) \bmod 7$

$= ((-1) \bmod 7 + ((2^2)^2)^2 * 3 \bmod 7) \bmod 7$

$= (-1 + 5) \bmod 7 = 4$

Số học trên Modulo

Ước số chung lớn nhất.

ước chung lớn nhất của hai số nguyên dương là bài toán chung của lý thuyết số. Ta ký hiệu GCD(a, b) là ước số chung dương lớn nhất của a và b, tức là số nguyên dương vừa là ước của a vừa là ước của b và là số nguyên dương lớn nhất có tính chất đó.

Ví dụ

- GCD(60,24) = 12
- GCD (6, 15) = 3
- GCD(8, 21) = 1

Số học trên Modulo

- **Nguyên tố cùng nhau**.

Ta thấy 1 bao giờ cũng là ước số chung của hai số nguyên dương bất kỳ. Nếu GCD(a, b) = 1, thì a, b được gọi là hai số nguyên tố cùng nhau:

Ví dụ: GCD(8,15) = 1, tức là 8 v à 15 là hai số nguyên tố cùng nhau

- **Tìm ước chung lớn nhất**. Bây giờ chúng ta xét bài toán tìm ước số chung lớn nhất của hai số nguyên dương cho trước. Dễ dàng chứng minh được tính chất sau: GCD(a,b) = GCD(b, a mod b)

Số học trên Modulo

- **Thuật toán Ơclit tìm GCD(a, b)** Tính UCLN của 2 số nguyên
- VÀO : Hai số nguyên không âm a và b
- với a > b
- RA : ƯCLN của a và b.
  - (1) While b ≠ 0 do r = a mod b,b←a,b←r
  - (2) Return (a).

Số học trên Modulo

Thuật toán Euclide mở rộng:

- VÀO : Hai số nguyên không âm a và b với a ≥ b RA : d = UCLN (b,a) và các số nguyên x và y thoả mãn d= by+ax
- (1) Nếu b = 0 thì đặt d $\leftarrow$a, x $\leftarrow$ 1, y $\leftarrow$ 0 và return (d,x,y)
- (2) Đặt $x_2 \leftarrow 1$ $x_1 \leftarrow 0, y_1 \leftarrow 0$
- (3) While 0 b > do
  - 3.1. q $\leftarrow$ a int b, r $\leftarrow$ a-qb, x $\leftarrow$ x_2-q$x_{1,}$ y $\leftarrow$ y_2-qy_1
  - 3.2. b $\leftarrow$a,r $\leftarrow$ b,x_2 $\leftarrow$$x_1$,$x_1$ $\leftarrow$x,y_2 $\leftarrow$$y_1$, y_1 $\leftarrow$y

•(4) Đặt d $\leftarrow$a, x $\leftarrow$$x_2$, y $\leftarrow$ y_2 ,dreturn(d,x,y)

Số học trên Modulo

Ví dụ Bảng sau chỉ ra các bước của thuật toán trên với các giá trị vào 4864a = và 3458

q	r	x	y	a	b	x2	x1	y2	y1
				4864	3458	1	0	0	1
1	1406	1	-1	3458	1406	0	1	1	-1
2	646	-2	3	1406	646	1	-2	-1	3
2	114	5	-7	646	114	-2	5	3	-7
5	76	-27	38	114	76	5	-27	-7	38
1	38	32	-45	76	38	-27	32	38	-45
2	0	-91	128	38	0	32	-91	-45	128

Số học trên Modulo

Tìm số nghịch đảo

Định nghĩa: Phần tử nghịch đảo Cho a $\in Z_n$,

Phần tử nghịch đảo (ngược theo phép nhân) của a mod n là một số nguyên x $\in Z_n$ sao cho:

$$ax \equiv 1 \bmod n$$

Nếu x tồn tại thì nó là duy nhất, a được gọi là khả nghịch. Phần tử nghịch đảo của a được ký hiệu là a^{-1}.

Số học trên Modulo

Thuật toán (Tính các nghịch đảo trong Z_n

VÀO : $a \in Z_n$

RA : $a^{-1} \bmod n$ − (nếu tồn tại).

(1) Dùng thuật toán Euclide mở rộng để tìm các số nguyên x và y sao cho

$ax + by = d$ trong đó $d = (n,a)$

(2) Nếu $d > 1$ thì $a^{-1} \bmod n$ không tồn tại. Ngược lại return (x)

Số học trên Modulo

Thuật toán (Tính các nghịch đảo trong Z_n

- **Bước 1**: Xây dựng bảng (gồm 6 cột) như sau:

Dòng	r_0	r_1	r_2	q	t_0	t_1

Trên mỗi dòng, ta có: $r_0 = r_1 \times q + r_2$

- **Bước 2**: Điền giá trị vào dòng đầu tiên $r_0 = n$, $r_1 = a$, $t_0 = 0$, $t_1 = 1$

Dòng	r_0	r_1	r_2	q	t_0	t_1
0	n	a			0	1

Số học trên Modulo

Thuật toán (Tính các nghịch đảo trong Z_n

- **Bước 3**: Trên dòng i đang xét, tính giá trị

  $r_2 = r_0 \bmod r1$,

  $q = \lfloor r_0 / r_1 \rfloor$

Dòng	r_0	r_1	r_2	q	t_0	t_1
...	...	...	...	...	...	...
i			$r_0 \bmod r_1$	$\lfloor r_0 / r_1 \rfloor$		

- **Bước 4**: Tính giá trị t_1 (của dòng i) từ giá trị q, t_0 và t_1 của dòng i-1.

Dòng	r_0	r_1	r_2	q	t_0	t_1
...	...	...	...	...	...	...
i -1				X	Y	Z
i						Y-$X \times Z$ mod n

Số học trên Modulo

Thuật toán (Tính các nghịch đảo trong Z_n

- **Bước 5**: Trên dòng *i* đang xét:
  - **Nếu** $r_2 = 0$ **thì**:
    - **Nếu** $r_1 = 1$ **thì** giá trị t_1 (của dòng đang xét) là phần tử nghịch đảo của *a* trong Z_n
    - **Ngược lại** (tức là $r_1 \neq 1$) **thì** không tồn tại phần tử nghịch đảo của *a* trong Z_n. Rõ ràng trường hợp này chỉ xảy ra khi USCLN$(a, n) \neq 1$
    - Chấm dứt thuật toán
  - **Ngược lại** (tức là $r_2 \neq 0$) thì sang bước 6

Dòng	R_0	r_1	r_2	q	t_0	t_1
...	...	...	...	...	...	...
i		$r_1 = 1$?	$r_2 = 0$?			

Số học trên Modulo

Thuật toán (Tính các nghịch đảo trong Z_n

- **Bước 6**: Sao chép giá trị sang dòng tiếp theo theo quy tắc dưới đây, sau đó, trở lại **bước 3**:

Dòng	r_0	r_1	r_2	q	t_0	t_1
i						

Số học trên Modulo

Dòng	r_0	r_1	r_2	q	t_0	t_1
0	1024	173	159	5	0	1
1	173	159	14	1	1	1019
2	159	14	5	11	1019	6
3	14	5	4	2	6	953
4	5	4	1	1	953	148
5	4	*1*	*0*	4	148	*805*

Vậy $173^{-1} = 805$ (trong Z_{1024})

Giới thiệu lý thuyết số

- **Các số nguyên tố** Như chúng ta đã biết số nguyên tố là các số nguyên dương chỉ có ước số là 1 và chính nó.
- Chúng không thể được viết dưới dạng tích của các số khác. 1 là số nguyên tố, nhưng không quan tâm đến nó. Xét các số nhỏ hơn 10 ta có: 2, 3, 5, 7 là số nguyên tố, vì chúng không có ước số khác 1 và chính nó; 4, 6, 8, 9, 10 không phải là số nguyên tố. Có thể nói 2 là số chẵn duy nhất là số nguyên tố. Các số nguyên tố là trung tâm của lý thuyết số. Số các số nguyên tố là vô hạn

Giới thiệu lý thuyết số

- **Các số nguyên tố cùng nhau và GCD**

Hai số nguyên dương a và b không có ước chung nào ngoài 1, được gọi là nguyên tố cùng nhau. Ví dụ: 8 và 15 là nguyên tố cùng nhau, vì ước của 8 là 1, 2, 4, 8, còn ước của 15 là 1, 3, 5, 15. Chỉ có 1 là ước chung của 8 và 15

- Ví dụ. Ta có phân tích: 300=21×31×52 và 18=21×32.

Vậy GCD(18,300)=21×31×50=6

Giới thiệu lý thuyết số

- **Định lý Ferma (Định lý Ferma nhỏ)**

$$a^{p-1} \bmod p = 1$$

trong đó p là số nguyên tố và a là số nguyên bất kỳ khác bội của p:GCD(a, p) = 1.

Hay với mọi số nguyên tố p và số nguyên a không là bội của p, ta luôn có

$$a^{p} = a \bmod p$$

Công thức trên luôn đúng, nếu p là số nguyên tố, còn a là số nguyên dương nhỏ hơn p.

Giới thiệu lý thuyết số

- **Hàm Ole**

Cho n là một số nguyên dương. Khi thực hiện phép tính đồng dư n của mọi số nguyên khác ta nhận được tập đầy đủ các phần dư có thể có là: 0, 1, 2,…, n-1

Từ tập trên ta tìm tập rút gọn bao gồm các số nguyên tố cùng nhau với n và quan tâm đến số lượng các phần tử như vậy đối với số nguyên dương n cho trước.

Ví dụ. Với n = 10

Tập đầy đủ các phần dư là {0,1,2,3,4,5,6,7,8,9}

Tập rút gọn các phần dư nguyên tố với 10 là {1,3,7,9}

Số các phần tử của tập rút gọn trên là giá trị của hàm Ole $\Phi(n)$.

Như vậy, $\Phi(10) = 4$.

Giới thiệu lý thuyết số

- **Hàm Ole**

Muốn tính $\Phi(n)$ việc đếm số các số nguyên tố cùng nhau với n và nhỏ hơn n được loại bỏ vì đây là bài toán tốn nhiều công sức.

Nói chung có thể tính hàm Ơle của một số dựa trên biểu thức phân tích ra thừa số của số đó.

Dễ dàng thấy, nếu p là số nguyên tố $\Phi(p) = p-1$

Nếu p và q là hai số nguyên tố khác nhau, thì có thể chứng minh được rằng: $\Phi(p.q) = (p-1)(q-1)$

Nếu p là số nguyên tố, thì $\Phi(p^n) = p^n - p^{n-1}$

Nếu s và t là hai số nguyên tố cùng nhau, thì $\Phi(s.t) = \Phi(s).\Phi(t)$

DH22TIN04

Mã lớp

2qfplvyr

DH22TIN04 ATBMTT

Sao chép đường liên kết mời