Bài 9. $a = 1573$, $b = 308$. Tìm UCLN

Đặt $(A_1, A_2, A_3) = (1, 0, 1573)$

$(B_1, B_2, B_3) = (0, 1; 308)$

$Q = A3/B3 = 1573/308 = 5$

Đặt $(A_1, A_2, A_3) = (0, 1, 308)$

$(B_1, B_2, B_3) = (1, -4, 33)$

$Q = 9$

$(A_1, A_2, A_3) = (0, -4, 33)$

$(B_1, b_2, b_3) = (-9, 37, 11)$

$Q = 3$

Đặt : $(A_1, A_2, A_3) = (-9, 37, 11)$

$(B_1, B_2, B_3) = (28, -115, 0)$

Vì $B_3 = 0$ nên $UCLN(1573, 308) = A_3 = 11$

Bài 10. Tính $3^{22} \mod 23$

$a = 3$, $k = 22$, $n = 23$, $ki = 10110$, $t = 4$

```
gán $b = 1$ , nếu $k = 0$ return 1;
gán $A = a$ , nếu $ki = 1 \Rightarrow b = a$;
for ($i = 0$; $i <= t$; $i++$)
    $A = A^2 \mod n$
    Nếu $ki = 1 \Rightarrow b = A.b \mod n$;
    returnb;
```

Bảng mô tả các bước trên

i	0	1	2	3	4
ki	0	1	1	0	1
A	3	9	12	6	13
b	1	9	16	16	1

Vậy : $3^{22} \mod 23 = 1$

Bài 16. giải hệ đồng dư

$5x \equiv 20 \mod 6$

$6x \equiv 6 \mod 5$

$4x \equiv 5 \mod 77$

$\Leftrightarrow$ $x \equiv 4 \mod 6$

$x \equiv 1 \mod 5$

$x \equiv 3 \mod 7$

$m = 5.6.7 = 210$

$m_1 = 35$, $m_2 = 42$, $m_3 = 30$

$35 y_1 \equiv 4 \mod 6$ $\qquad y_1 = 2$

$42 y_2 \equiv 1 \mod 5$ $\Leftrightarrow$ $y_2 = 3$

$30 y_3 = 3 \mod 7$ $\qquad y_3 = 5$

$\Rightarrow x = m_1 . y_1 + m_2 . y_2 + m_3 . y_3 \mod m$

$= 346 \mod 210$

$= 136 \mod 210$

Bài 15.

Tính : $f(490)$, $f(768)$

⊛ $490 = 2.5.7^2$

$f(490) = 490.(1 - \frac{1}{2}).(1 - \frac{1}{5}).(1 - \frac{1}{7})$

$=$

⊛ $f(768) =$ ~~28~~ $2^8 . 3$

$f(768) = 768.(1 - \frac{1}{2}).(1 - \frac{1}{3})$

$=$

Bài 12.

$f(19) = 19 - 1 = 18 = 2 . 3^2$

Tìm các phần tử nguyên thuỷ sao cho

$x^{(18/2)} \bmod 37 \;!= 1$

$x^{18/3} \bmod 37 \;!= 1$

$\Leftrightarrow x^9 \bmod 37 \;!= 1$

$x^6 \bmod 37 \;!= 1$

$\Rightarrow$ Xét $x = 2 \Leftrightarrow 2^9 \bmod 37 = 31 \;!= 1$

$2^6 \bmod 37 = 27 \;!= 1$

$\Rightarrow$ 2 phần tử nguyên thuỷ của Z_{19}

Để UCLN $(i, f(19)) = 1$ thì $i \in Z_{18}$

$Z_{18} = (1, 5, 7, 11, 13, 17)$

$2^1 \bmod 19 = 2$ $\qquad 2^{13} \bmod 19 = 3$

$2^5 \bmod 19 = 13$ $\qquad 2^{17} \bmod 19 = 10$

$2^7 \bmod 19 = 14$

$2^{11} \bmod 19 = 15$

Vậy các phần tử nguyên thuỷ của nhóm nhân Z_{19} là: $\{2, 3, 10, 13, 14, 15\}$

Bài 11. Tính căn bậc 2 của 12 mod 37

$a = 12, \quad p = 37$

$$\frac{12}{37} = \frac{4}{37} \cdot \frac{3}{37} = \frac{2^2}{37} \cdot \frac{3}{37}$$

$$= (-1)^2 . 1 = 1$$

$$\Rightarrow d = \frac{12^{37-1}}{4} \bmod 37$$

$$= 12^9 \bmod 37$$

$$= (12^3)^3 \bmod 37 = 1$$

Vậy $r = 12^{37+3/8} \bmod 37 = 12^5 \bmod 37$

$= 7 \qquad \Rightarrow -r = -7$

Vậy căn bậc 2 của 12 mod 37 là $(-7, 7)$

Bài 13.

Tìm phần tử nghịch đảo của 3 trong Z_{31}

- gọi x là phần tử nghịch đảo của 3

$3x = 1 \bmod 31$

$\Leftrightarrow 3x - 1 = 31k \; (k = 1, 2, 3 \ldots)$

$\Leftrightarrow x = 21.$

Bài 17.

a) $17^{-1} \bmod 101$

Đặt $(A_1, A_2, A_3) = (1, 0, 101)$

$(B_1, B_2, B_3) = (0; 1, 17)$

$Q = 5$

Đặt $(A_1, A_2, A_3) = (0, 1, 17)$

$(B_1, B_2, B_3) = (1, -5, 16)$

$Q = 1$

Đặt $(A_1, A_2, A_3) = (1, -5, 16)$

$(B_1, B_2, B_3) = (-1, 6, 1)$

Vì $B_3 = 1$ nên $17^{-1} \bmod 101 = B_2 = 6$

Bài 1.

Chương 2.

Bản mã: PSZI QIERW RIZiV LEZMRK XS WEC CSY EVI WSVVC

Bằng phương pháp vét cạn ta tìm được k = 4

Ta thu được bản rõ: LOVE MEANS NEVER HAViNG TO SAY YOU ARE SORRY

Bài 2:

Bản rõ: I may not be able to grow flowers but my garden produces just as many dead leavesl, old overshoes, pieces of rope, and bushels of dead grass as anybody's. And today I bought a wheelbarrow to help in clearing it up I have always loved and respected the wheelbarrow. It is the one wheled vehicle of which I am perfect master

Ctxt	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq	5		37	8	12	9	24	5	15	7	18	7	5	13	10	6	1		20		14		5	7	15	13
Rank	21		1	13	10	12	2	19	6	14	4	15	20	9	11	17	22		3		7		18	16	5	8
Ptxt	v		e	b	i	w	a	f	d	c	s	y	m	l	n	u	j		o		t		g	p	r	h

C → e : vì C xuất hiện nhiều nhất

Q → j : vì chỉ xuất hiện 1 lần

Z → h : có 7 ZC nhưng chỉ có 1 CZ và HE xuất hiện nhiều thứ 2.

N → i : Dự đoán

U → t : có 2 UZC và THE là trigam thường xuất hiện nhất

2bc)

Bản rõ: This is a the canadian national anthem in French, as might be sung from time to time in Quebec

- Tổng số kí tự là: 198

Order	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
Ctxt	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Freq	13	21	32	19	13	10		1	16	6	20			1	2	20	4	12	1		6	4		2	1	4
Rank	6	2	1	10	7	9			5	11	3					4		8			12					
Ptxt	i	t	e	p	a	l	w	h	s	d	o	z	k	v	g	r	c	n	y	j	u	f	q	b	m	x

C → e highest count

B → t worked

$$\Rightarrow \begin{cases} 4a + b = 12 \\ 19a + b = 10 \end{cases} \Rightarrow \begin{cases} a = 9 \\ b = 4 \end{cases}$$

$$e_k(x) = 19x + 4$$

$$d_k(y) = 11(y-4) = 11y - 44.$$