

# Cryptography

## Chapter 1

### Exercise 1

Prime	Non Prime
101	
131	$111 = 3 \times 37$
151	$121 = 11 \times 11$
181	$141 = 3 \times 47$
191	$161 = 7 \times 23$
313	$171 = 3^2 \times 19$
353	$103 = 3 \times 101$
373	$323 = 17 \times 19$
383	$333 = 3^3 \times 37$
	$343 = 7^3$
	$363 = 3 \times 11^2$
	$393 = 3 \times 131$

V	U	W	X
*	0	x	0312
0	*	x	822
*	*	*	820
*	*	*	801
*	0	*	0

### Exercise 2

We have  $792 = 2^3 \times 3^2 \times 11$ .

So there is  $(3+1)(2+1)(1+1) = 4 \times 3 \times 2 = 24$  divisors

### Exercise 3

We want  $axc = b$  with  $a, b, c$  as small as possible

$$x = 13^4 \cdot 11^4 \cdot 3^5$$

### Exercise 4

735 and 133

$$735 = 133 \times 5 + 70$$

$$133 = 70 \times 1 + 63$$

$$70 = 63 \times 1 + 7$$

$$63 = 7 \times 9 + 0$$

r	q	U	V
735	x	0	1
133	x	+1	-0
70	5	-52	-1
63	1	+6	-1
7	1	-11	+2
0	9	+105	-19

# Cryptography

## Chapter 1

### Exercise 1

Prime	Non Prime
101	
131	$111 = 3 \times 37$
151	$121 = 11 \times 11$
181	$141 = 3 \times 47$
191	$161 = 7 \times 23$
313	$171 = 3^2 \times 19$
353	$303 = 3 \times 101$
373	$323 = 17 \times 19$
383	$333 = 3^3 \times 37$
	$343 = 7^3$
	$363 = 3 \times 11^2$
	$393 = 3 \times 131$

V	U	P	Q
1	0	X	0011
0	1	X	0221
1	1	1	220
0	0	1	200
1	0	0	0

### Exercise 2

We have  $792 = 2^3 \times 3^2 \times 11$

So there is  $(3+1)(2+1)(1+1) = 4 \times 3 \times 2 = 24$  divisors

### Exercise 3

We want  $abc = b$

$$x = 13^4 \times 11^4 \times 3^5$$

### Exercise 4

735 and 133

$$735 = 133 \times 5 + 70$$

$$133 = 70 \times 1 + 63$$

$$70 = 63 \times 1 + 7$$

$$63 = 7 \times 9 + 0$$

R	Q	U	V
735	X	0	1
133	X	+1	-0
70	5	-52	+12x
63	1	+6	-1
7	1	-11	+2
0	9	+105	-19

### Exercise 5.

$$2160u + 756v = 2160 \wedge 756$$

$$1) \quad 2160 = 756 \times 2 + 648$$

$$756 = 648 \times 1 + 108$$

$$648 = 108 \times 6 + 0$$

$$\text{So } 2160 \wedge 756 = 108$$

2) Using Euclidean extended Algorithm

$r$	$q$	$u$	$v$
2160	x	0	1
756	x	+1	-0
648	2	-2	+1
108	1	+3	-1
0	6	-20	+7

So  $(-1, 3)$  is a solution.

$$3) \quad 2160x + 756y = 324$$

$$\text{We know that } 2160 \times -1 + 756 \times 3 = 108$$

$$\text{Having: } 3 \times (2160 \times -1 + 756 \times 3) = 324$$

$$\text{We have } 2160 \times -3 + 756 \times 9 = 324$$

Thus  $(-3, 9)$  is a solution

### Exercise 6

$$\bullet \quad \bar{27}^{25} \text{ in } \mathbb{Z}/11\mathbb{Z} \rightarrow \bar{27} = \bar{5}$$

$$25 = 5 \times 5 = (2+3) \times (2+3)$$

$$\left. \begin{array}{l} \bar{5}^2 = \bar{25} = \bar{3} \\ \bar{5}^3 = \bar{125} = \bar{6} \end{array} \right\} \quad \left. \begin{array}{l} \bar{5}^2 \times \bar{5}^3 = \bar{5}^5 = \bar{3} \times \bar{4} = \bar{12} = \bar{1} \\ \text{So } \bar{27}^{25} = \bar{1} \end{array} \right.$$

$$\begin{aligned} \bar{5}^2 &= \bar{25} = \bar{3} \\ \bar{5}^3 &= \bar{125} = \bar{6} \\ \bar{5}^2 \times \bar{5}^3 &= \bar{5}^5 = \bar{3} \times \bar{4} = \bar{12} = \bar{1} \\ \text{So } \bar{27}^{25} &= \bar{1} \end{aligned}$$

$$\cdot \bar{6}^{51} = \bar{6}^{50} \times \bar{6} = \bar{6}^{25 \times 2} \times \bar{6}$$

$$\bar{6}^2 = \bar{36} = \bar{1}$$

$$\bar{1}^{25} = \bar{1}^3 = \bar{3} \times \bar{3} = \bar{3} \times \bar{27} = \bar{243} = \bar{5}$$

$$\text{So } \bar{6}^{51} = \bar{6}$$

$$\cdot \bar{8}^{47} = \bar{8}^{45+2} = \bar{8}^{45} \times \bar{8}^2$$

$$\bar{8}^2 = \bar{64} = \bar{4}$$

$$\bar{8}^5 = \bar{32768} = \bar{8}^{2+18-3+4}$$

$$\bar{8}^9 = (\bar{8}^3)^3 = (\bar{512}) = \bar{8}^3 = \bar{8}$$

$$\text{So } \bar{8}^{47} = \bar{64} \times \bar{8} = \bar{32} = \bar{2}$$

$$\cdot \bar{15}^{2311} = \bar{15}^{5 \times 462} \times \bar{15}$$

$$\left. \begin{array}{l} \bar{15}^{51} = \bar{15} \\ \bar{15}^7 = \bar{15} \\ \bar{15}^6 = \bar{1} \\ \bar{1}^n = \bar{1} \end{array} \right\}$$

$$\bar{15}^{2310} \times \bar{15} = \bar{1} \times \bar{15} = \bar{15}$$

### Exercise 7

In  $(\mathbb{Z}/24\mathbb{Z}, \oplus, \otimes)$

i) Find all  $\bar{a}$  such that  $a \otimes 24 = 1$

We are in  $\bar{24}$  so we are looking for all the elements in  $(\mathbb{Z}/24\mathbb{Z})$  we have  $24 = 2^3 \times 3$

So all the numbers divisible by 2 and 3 cannot be  $a$ :

We have so  $\bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{13}, \bar{17}, \bar{19}, \bar{23}$

$$\begin{aligned} 24 &= 5 \times 4 + 4 \\ 5 &= 4 \times 1 + 1 \end{aligned}$$

r	a	u	v
24	x	0	1
5	x	+1	-0
4	4	-4	+1
1	1	+5	-1

$$5 \times 5 - 24$$

r	a	u	v
24	x	0	1
7	x	+1	-0
3	3	-2	+1
1	2	-7	-2

$$7 \times 7 - 2 \times 24$$

r	a	u	v
24	x	0	1
11	x	+1	-0
2	2	-2	+1
1	5	-11	-5

$$11 \times 11 - 5 \times 24$$

r	a	u	v
24	x	0	1
13	x	+1	-0
11	1	-1	+1
2	1	+2	-1
1	5	-11	+6

$$13 \times (-11) + 6 \times 24$$

r	a	u	v
24	x	0	1
17	x	+1	-0
7	1	-1	+1
3	2	-1	+1
1	2	+3	-2

$$17 \times (-7) + 5 \times 24$$

r	a	u	v
24	x	0	1
19	x	+1	-0
5	1	-1	+1
4	3	+4	-3
1	1	+5	+4

$$19 \times (-5) + 4 \times 24$$

r	a	u	v
24	x	0	1
23	x	+1	-0
1	1	-1	+1

$$23 \times (-1) + 24$$

$$\begin{aligned} 24 &= 7 \times 3 + 3 \\ 7 &= 3 \times 2 + 1 \end{aligned}$$

$$\begin{aligned} 24 &= 11 \times 2 + 2 \\ 11 &= 2 \times 5 + 1 \end{aligned}$$

$$\begin{aligned} 24 &= 13 \times 1 + 11 \\ 13 &= 11 \times 1 + 2 \\ 11 &= 2 \times 5 + 1 \end{aligned}$$

$$\begin{aligned} 24 &= 17 \times 1 + 7 \\ 17 &= 7 \times 2 + 3 \\ 7 &= 3 \times 2 + 1 \end{aligned}$$

$$\begin{aligned} 24 &= 19 \times 1 + 5 \\ 19 &= 5 \times 3 + 4 \\ 5 &= 4 \times 1 + 1 \end{aligned}$$

$$24 = 23 \times 1 + 1$$

$$\{ \bar{1}, \bar{5}, \bar{7}, \bar{11}, \bar{15}, \bar{17}, \bar{23}, \bar{25} \}$$

$$\text{ii) Solve } \bar{7}x = \bar{15}$$

$$x = \bar{15} \times \bar{7} \doteq \bar{105} = \bar{9}$$

$$\text{iii) } \frac{\bar{3}x = \bar{15}}{-2 = 22} \rightarrow \bar{x} = \bar{5} \quad [8] \rightarrow x = \bar{5}$$

$$x = \bar{13}$$

$$x = \bar{21}$$

$$\text{iv) } \bar{3}x = \bar{17} \rightarrow \text{no solutions}$$

$\bar{2} \times \bar{5} = \bar{10}$  even in  $(\bar{5}, \bar{15})$   
 so add  $\bar{2}$  to  $\bar{10}$  and  $\bar{12}$   
 $\bar{12}, \bar{14}, \bar{16}, \bar{18}, \bar{20}, \bar{22}, \bar{24}$  are even and  $\bar{10}$

### Exercise 8

$$\text{i) } \text{Inv}(\mathbb{Z}/28\mathbb{Z}) = \{\bar{1}, \bar{3}, \bar{5}, \bar{9}, \bar{11}, \bar{13}, \bar{15}, \bar{17}, \bar{19}, \bar{23}, \bar{25}, \bar{27}\}$$

$$28 = 2^2 \times 7$$

Euclidean algorithm in  $\mathbb{Z}$  mod 28

$$\text{ii) } \bar{3}x = \bar{17}$$

$$x = \bar{17} \times \bar{3}^{-1} = \bar{15} \quad \left. \begin{array}{l} 28 = 3 \times 9 + 1 \\ 9 = 3 \times 3 + 0 \end{array} \right\} \text{gcd}(28, 3) = 1$$

$$\text{iii) } \bar{4}x = \bar{17}$$

$$28 = 4x + 0$$

$$17 \text{ not divisible by 4} \quad \text{gcd}(28, 4) = 4$$

→ no solutions

$$\text{iv) } x \equiv \bar{3} \pmod{7}$$

$$x = \bar{3} = \bar{10} = \bar{17} = \bar{24}$$

### Exercise 9

$$\begin{cases} x \equiv 3 \pmod{7} \\ x \equiv 4 \pmod{11} \end{cases} \Rightarrow \begin{cases} x = 3 + 7k \\ x = 4 + 11k' \end{cases}$$

We have  $7 \times 11 = 1$  so here

$$11 = 7 \times 1 + 4$$

$$7 = 4 \times 1 + 3$$

$$4 = 3 \times 1 + 1$$

$$\begin{array}{r} 11 \times 0 \ 1 \\ 7 \times 1 \ 0 \ 0 \\ 4 \ 1 \ 1 \ 1 \\ 3 \ 1 \ 2 \ 1 \\ 1 \ 1 \ 3 \ 2 \end{array}$$

$$1 = 7 \times -3 + 2 \times 11$$

$$\text{So } x_1 = -21$$

$$x_2 = 22$$

$$\begin{cases} x \equiv 1 \pmod{7} \\ x \equiv 0 \pmod{11} \end{cases}$$

$$\begin{cases} x \equiv 0 \pmod{7} \\ x \equiv 1 \pmod{11} \end{cases}$$

$$\text{So } x = 22 \times 3 - 21 \times 4 = -18$$

$$\text{with } 7 \times 11 = 77$$

$$x = 59 + 77k$$

$$\begin{cases} y \equiv 7 \pmod{10} \\ y \equiv 2 \pmod{9} \\ y \equiv 6 \pmod{7} \end{cases}$$

On a  $\gcd(9; 10) = 1$   
 $\gcd(7; 9) = 1$   
 $\gcd(7; 10) = 1$

Posons :  $x_1 \equiv a \pmod{n_1}$   
 $x_2 \equiv b \pmod{n_2}$   
 $x_3 \equiv c \pmod{n_3}$

On pose  $n = n_1 n_2 n_3$

On calcule  $y_1 = \frac{n}{n_1}$ ;  $y_2 = \frac{n}{n_2}$ ;  $y_3 = \frac{n}{n_3}$

Ensuite on trouve le  $n_i$  pour lequel  
 $y_1 n_i \equiv 1 \pmod{n_1}$ ;  $y_2 n_i \equiv 1 \pmod{n_2}$ ;  $y_3 n_i \equiv 1 \pmod{n_3}$   
Pour chaque  $y_i$  on calcule son inverse  
Par rapport à  $n_i$  (si négative,  $+ n_i$ )  
[je note chaque inverse  $I_i$ ]

On a  $X = a \times y_1 \times I_1 + b \times y_2 \times I_2 + c \times y_3 \times I_3$

•  $10 \times 9 \times 7 = 630$ ,  $\hat{n}_1 = 63 \Rightarrow 63 \times 10 \equiv 1 \pmod{10}$

•  $\hat{n}_2 = 70$ ,  $70 \times 9 \equiv 1 \pmod{9}$

•  $\hat{n}_3 = 90$ ,  $90 \times 7 \equiv 1 \pmod{7}$

•  $63 = 10 \times 6 + 3$

$10 = 3 \times 3 + 1 \Rightarrow 1 = 10 - 3 \times 3$

$n =$   
 $= 10 - 3(63 - 10 \times 6)$   
 $= 10 \times 18 - 3 \times 63$

$e_1 = -7$

•  $70 = 9 \times 7 + 7$

$9 = 7 \times 1 + 2$

$7 = 2 \times 3 + 1$

Here  $e_2 = -4$

r	9	10	v
9	1	0	+
7	0	1	+
3	1	0	+
2	0	1	+
1	1	0	+
0	0	1	+

$$\begin{aligned} 1 &= 7 - 2 \times 3 \\ &= 7 - 3 \times (9 - 7) \\ &= 7 \times 4 - 3 \times 9 \\ &= (70 - 9 \times 7) \times 4 - 3 \times 9 \\ &= 70 \times 4 - 9 \times 31 \end{aligned}$$

•  $90 = 7 \times 12 + 6$

$7 = 6 + 1$

$e_3 = -1 = 6$

$$\begin{aligned} 1 &= 7 - 6 \\ &= 7 - (90 - 7 \times 12) \\ &= 7 \times 13 - 90 \end{aligned}$$

$x = 7 \times 7 \times 63 + 4 \times 70 \times 2 + 6 \times 90 \times 6$   
 $= 587 + 630k$

# Chapter 2

## Exercise 10

The Enciphering key is  $(\bar{5}, \bar{3})$

i) "DECIDE"  $\rightarrow$  342834

$$ax + b = \bar{5}x + \bar{3}$$

$$\begin{array}{l|l} 18 = 7 & H \\ 23 = 1 & B \\ 13 = 2 & C \\ 43 = 10 & K \\ 18 = 7 & H \\ 23 = 1 & B \end{array}$$

$$y = ax + b$$

$$a^{-1}y - b \equiv a^{-1}$$

E 201902

ii) So we have  $n = 5 \times 2 + 1$  so  $n - 5 \times 2 = 1$   
So  $\bar{5} = \bar{2} = \bar{9}$

So we have  $\bar{5} \times \bar{3} = \bar{15} = \bar{6}$

$$\bar{15} = \bar{4} \quad E$$

$$\bar{33} = \bar{5} = A$$

$$\bar{60} = \bar{5} \quad F$$

$$\bar{24} = \bar{2} \cdot C$$

$$\bar{60} = \bar{5} \quad F$$

$$\bar{15} = \bar{5} \quad E$$

EFFICACE

## Exercise 11

i) We calculate all the determinants

$$i) g \quad \gcd(g) = 1$$

$$ii) 104 \quad \gcd(104) = 13$$

$$iii) 16 \quad \gcd(16) = 2$$

$$iv) 4 \quad \gcd(4) = 4$$

$g$  and  $h$  are coprime

$$i) \bar{g}^{-1} \rightarrow 14 = g + 5$$

$$g = 5 \times 1 + 4$$

$$5 = 4 \times 1 + 1$$

$$\begin{aligned} 1 &= 5 - 4 \\ &= 5 \times 1 - 5 \times 1 \\ &= 14 \times 1 - 5 \times 3 \end{aligned}$$

$$-3 = \bar{11}$$

$$g^{-1} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} \bar{2} & \bar{5} \\ \bar{5} & \bar{7} \end{pmatrix} \begin{pmatrix} \bar{y_1} \\ \bar{y_2} \end{pmatrix} + \begin{pmatrix} \bar{1} \\ \bar{2} \end{pmatrix}$$

Q 20 Ques 10

Ex 20 - 30 x 3

Same for iv)

(Ex 7) w/ out previous solt

## Chapter 3

### Exercise 16

$$\varphi(51) = \varphi(3 \times 17) = 32$$

$$\varphi(93) = 60$$

$$\varphi(135) = \varphi(3^3 \times 5) = 72$$

$$\varphi(200) = \varphi(2^3 \times 5^2) = 80$$

### Exercise 17

$$i) \varphi(165) = 80$$

$$ii) \begin{aligned} 165 &= 14 \times 11 + 11 \\ 14 &= 11 \times 1 + 3 \\ 11 &= 3 \times 3 + 2 \\ 3 &= 2 \times 1 + 1 \end{aligned}$$

r	a	v	v
165	x	0	1
14	x	+1	-0
11	11	+11	+1
3	1	+12	-1
2	3	-67	+4
1	1	59	-5

$$\text{So : } 1 = 59 \times 14 - 5 \times 165.$$

$$\text{So } \overline{59}$$

$$iii) \overline{15}^{1766} = \overline{15}^{2 \times 883} = \overline{60}^{883} = 60^3 \times \overline{60}^{880} = \overline{15}^{176} \times \overline{45}^{16 \times 11} = \overline{15} \times \overline{45}^{11} = \overline{15} \times \overline{65} \times \overline{45}^5 = \overline{15}$$

### Exercise 18 11

i) We have  $p, q$  two prime numbers,  $n = p \times q$

$$\varphi(n) = \varphi(p) \times \varphi(q)$$

$$= (p-1) \times (q-1)$$

$$= pq - p - q + 1$$

$$= pq - (p+q) + 1$$

$$= n - p+q + 1$$

ii)  $p+q = \varphi(n)+1 = \varphi(n)$

iii) We have  $\begin{cases} p+q = 4112 \\ pq = 2851207 \end{cases}$

$$q = 4112 - p$$

$$p(4112 - p) = 2851207 \Rightarrow -p^2 + p \times 4112 = 2851207$$

$$p^2 - 4112p + 2851207 = 0$$

$$(b^2) - 4ac = 5503716 = 2346$$

$$x_1 = \frac{4112 - 2346}{2} = 883$$

$$x_2 = \frac{-4112 - 2346}{2} = -3229$$

So we have  $p = 3229$  and  $q = 883$

### Exercise 19 11

i)  $x^5 = 41$  in  $\mathbb{Z}/165\mathbb{Z}$

$$65 \mid (x^5 - 41)$$

$$41 = 24x_1 + 17$$

$$24 = 17x_1 + 7$$

$$17 = 7x_2 + 3$$

$$7 = 3x_1 + 1$$

$$65 \mid x^5 - 41 \Rightarrow x^5 - 41 = p \times 65$$

$$65 \mid 65 = 1$$

$$\varphi(n) = 48$$

$$5d \equiv 1 [48]$$

$$48 = 5 \times 9 + 3$$

$$5 = 3 \times 1 + 2$$

$$3 = 2 \times 1 + 1$$

$$1 = 3 - 2$$

$$= 3 \times 2 - 5$$

$$= (48 - 5 \times 9) \times 2 - 5$$

$$= 48 \times 2 - 5 \times 19$$

$$(p)q \times (q)r = (qr)p$$

$$(1-p) \times (1-q) =$$

$$1 - p - q + pq =$$

$$p + (1-p) - pq =$$

$$1 + pq - p =$$

$$-5 \times 29 \equiv 1 [48]$$

$$5 \times 67 \equiv 1 [48]$$

$$\begin{aligned} 3) \quad x = \overline{41}^{29} &= \overline{41}^{5+5+5+5+5+4} \\ &= 6 \times 6 \times 6 \times 6 \times 6 \times 16 \\ &= \overline{6} \end{aligned}$$

$$ii) \quad x^9 = \overline{1}$$

$$\varphi(102) = 32$$

$$9d = 1 [32]$$

$$32 = 9 \times 3 + 5$$

$$1 = 5 - 4$$

$$5 = 4 \times 1 + 1$$

$$= 5 \times 2 - 9$$

$$= 32 \times 2 - 9 \times 7$$

$$9 \times 25 \equiv 1 [32]$$

$$So \quad x = \overline{1}^{25} = \overline{11}^{5 \times 5} = \overline{95}^5 = \overline{23}$$

$$iii) \quad \gcd(6, 16) = 2 \equiv p \quad \text{but } p \neq q \pmod{2}$$

3 no. 1 solutions

$$8 = 3 \times 2 + 2$$

$$1 = 3 - 2 \times 1$$

$$3 = 2 \times 1 + 1$$

$$2 \times 9 = 18 \equiv 2 \pmod{16}$$

$$3 \times 3 \equiv 1 [8]$$

$$So \quad x = \overline{6}^3 = \overline{8}$$

## Exercise 20

i)  $ed \equiv 1 [\varphi(n)] \Leftrightarrow 3d \equiv 1 [\varphi(n)]$

$$\varphi(55) = 40$$

$$3 \times (-13) \equiv 1 [\varphi(n)]$$

$$60 = 3 \times 13 + 1$$

$$55 = 5 \times 11 = 88 = 40 \quad (1)$$

$$(\frac{1}{5} - 1)(\frac{1}{11} - 1) \cdot 88 = (88/5)(88/11)$$

$$\gcd(60, 3) = 1$$

✓

2)  $x = 12$

$$y = x^e \\ = 12^7$$

$$\text{so } \overline{12}^7 = \overline{12}$$

$\vee$	$0$	$1$	$2$	$3$
$\wedge$	$0$	$x$	$\overline{y}$	$\overline{z}$
$\oplus$	$0$	$x$	$\overline{y}$	$\overline{z}$
$\ominus$	$0$	$x$	$\overline{y}$	$\overline{z}$
$\otimes$	$0$	$x$	$\overline{y}$	$\overline{z}$
$\overline{\wedge}$	$0$	$x$	$\overline{y}$	$\overline{z}$
$\overline{\oplus}$	$0$	$x$	$\overline{y}$	$\overline{z}$
$\overline{\ominus}$	$0$	$x$	$\overline{y}$	$\overline{z}$
$\overline{\otimes}$	$0$	$x$	$\overline{y}$	$\overline{z}$

3)  $y = 50$

$$x = y^{d_A} = 50^{27} = \overline{50}^2 \times \overline{50}^{5 \times 5} \\ = \overline{25} \times \overline{10}^5 = \overline{250} = \overline{30}$$

4) we want to find  $d_B$ .

$$7d \equiv 1 [120]$$

$$120 = 7 \times 17 + 1$$

$$7 \times \overline{17} \equiv 1 [120]$$

$$7 \times \overline{103} = 1$$

$$\text{so } d = \overline{103}$$

$$\overline{7} \times \overline{17} \times \overline{103} = \overline{103} \times \overline{17} \times \overline{7} = \overline{01} = 01 \quad (iii)$$

$$\overline{01} =$$

$$-(2 \times 01 - 001) + 0 = 0 \quad (iv)$$

$$001 - 01 \times 0 =$$

$$001 - 01 \times (2 \times 01 - 001) =$$

$$001 - 01 \times 001 = 001 - 001 =$$

$$(001) \cdot 1 = 001 \quad (v)$$

$$001 + 2 \times 001 = 001$$

$$2 \times 001 + 001 = 001$$

## Exercise 2)

i)  $n_A = 133 = 7 \times 19 = 23$

$$\varphi(133) = 133 \left(1 - \frac{1}{7}\right) \left(1 - \frac{1}{19}\right) = 108 = (3 \times 2) \times 18$$

$$u_1 d \equiv 1 \pmod{108}$$

$$108 = u_1 \times 2 + 26$$

$$u_1 = 26 \times 1 + 15$$

$$26 = 15 \times 1 + 11$$

$$15 = 11 \times 1 + 4$$

$$11 = 4 \times 2 + 3$$

$$4 = 3 \times 1 + 1$$

r	q	u	v
108	x	0	1
41	x	+1	-1
26	2	-2	1
15	1	+3	-1
11	1	-5	+2
9	1	+8	-3
3	2	+21	+8
1	1	+29	-11

$$29 \times u_1 - 11 \times 108 = 1$$

$$u_1 \times 29 \equiv 1 \pmod{108}$$

✓

ii)  $x = 3$

$$y = x^{\frac{e_B}{n_B}} \pmod{n_B}$$

$$= 3^{77} \pmod{187}$$

$$= 3^{7 \times 11} \pmod{187}$$

$$= \overline{130}^{11} \pmod{187}$$

$$= \overline{130}^{4 \times 2} \times \overline{130}^4 \times \overline{130}^3 \pmod{187} = 38 \times 38 \times 124 = \overline{97}$$

iii)  $y = 10$

$$x = y^{d_A} \Rightarrow x = 10^{29} = (10^5)^5 \times 10^4 = \overline{117}^5 \times \overline{25}$$

$$= \overline{123} \times \overline{27} \times \overline{25}$$

$$= \overline{33}$$

iv)  $ed \equiv 1 \pmod{160}$

$$160 = 77 \times 2 + 6$$

$$177 = 77 \times 2 + 23$$

$$6 = 5 + 1 \quad | \quad 1 = 6 - (77 - 6 \times 12)^2$$

$$= 6 \times 13 - 77$$

$$= (160 - 77 \times 2) \times 13 - 77$$

$$= 160 \times 13 - 77 \times 27$$

$$s_0 : 77 \times (-\overline{7}) \equiv 1 [160]$$

$$77 \times \overline{33} \equiv 1 [160]$$

133

### Exercise 23

$$i) \varphi(209) = 180 \quad \varphi(221) = 192$$

$$13d \equiv 1 [180]$$

$$25d \equiv 1 [192]$$

$$s_0 : 180 = 13 \times 13 + 11$$

$$13 = 11 \times 1 + 2$$

$$11 = 2 \times 5 + 1$$

$$192 = 25 \times 7 + 17$$

$$25 = 17 \times 1 + 8$$

$$17 = 8 \times 2 + 1$$

$$1 = 11 - 2 \times 5$$

$$= 11 - 5 \times (13 - 11)$$

$$= 11 \times 6 - 5 \times 13$$

$$= (180 - 13 \times 13) \times 6 - 5 \times 13$$

$$= 180 \times 6 - 13 \times 83$$

$$1 = 17 - 8 \times 2$$

$$= 17 - (25 - 17) \times 2$$

$$= 17 \times 3 - 25 \times 2$$

$$= (192 - 25 \times 7) \times 3 - 25 \times 2$$

$$= 192 \times 3 - 25 \times 23$$

$$s_0 d = -\overline{83} = \overline{97}$$

$$s_0 d = -\overline{23} = \overline{169}$$

ii) we have  $n_A < n_B$ .

A sends to B

$$\begin{aligned} s &= \left( (s_A)^{e_A} [n_A] \right)^{e_B} [n_B] \\ &= \left( (\overline{10}^{97}) [209] \right)^{e_B} [221] \\ &= \left( (\overline{10}^{9 \times 10} \times \overline{10}^3) [209] \right)^{e_B} [221] \\ &= \overline{186}^{25} [221] \\ &= \overline{120} \times \overline{186} = 1 \times \overline{186} = \overline{186} \end{aligned}$$

(iii)

A checked B

$$S_B = \left( (y_{BA})^{e_B} [n_B] \right)^{d_A} [n_A]$$

$$= (98^{25} [221])^{97} [209]$$

$$= \overline{98}^{97} [209]$$

$$= \overline{98}^{5 \times 19 + 2}$$

$$= \overline{186}^{19} \times \overline{98}^2$$

$$= 186 \times \overline{164}^6 \times \overline{98}^2$$

$$= \overline{186} \times \overline{199}$$

$$= \overline{21}$$

Yes!

$$5 \times 8 - 61 = 1$$

$$3 \times (61 - 78) = -61 =$$

$$5 \times 78 - 3 \times 61 =$$

$$5 \times 78 - 3 \times (61 - 78) =$$

$$5 \times 78 - 3 \times 571 =$$

$$S_B = (10039 \quad \text{or} \quad (1005) \times 100)$$

$$[0913] \times 031$$

$$[0813] \times 072$$

$$11 \times 81 \times 8 = 081 \times 02$$

$$2 + 1 \times 11 = 61$$

$$1 + 7 \times 3 = 21$$

$$7 \times 8 - 11 = 1$$

$$(11-21) \times 2 - 11 =$$

$$3 \times 2 - 3 \times 11 =$$

$$21 \times 7 - 3 \times (30021 - 081) =$$

$$63 \times 81 - 3 \times 081 =$$

$$\overline{201} = \overline{21} = 02$$

$$50 \times \overline{01} = 01 \times 02$$

Answer and sol (ii)

a) &amp; b) done

$$[e_{01}]^{**} ([e_{01}]^{**} [e_{12}]) = e_{12}$$

$$[e_{123}]^{**} ([e_{012}] ([e_{01}])) =$$

$$[e_{123}]^{**} ([e_{012}] ([e_{01} \times e_{01}])) =$$

$$[e_{123}]^{**} \overline{021} =$$

$$\overline{201} = \overline{21} \times 1 = \overline{201} \times \overline{01} =$$