1.

(1). gcd(179,17)

q r1 r2 r s1 s2 s t1 t2 t

10 179 17 9 1 0 1 0 1 -10

1 17 9 8 0 1 -1 1 -10 11

1 9 8 1 1 -1 2 -10 11 -21

8 8 1 0 -1 2 -17 11 -21 179

1 0 2 -17 -21 179

=> gcd(179,17) = 1, s = 2, t = -21

--------------------------------------------------------------------------------------

(2). gcd(229,119)

q r1 r2 r s1 s2 s t1 t2 t

1 229 119 110 1 0 1 0 1 -1

1 119 110 9 0 1 -1 1 -1 2

12 110 9 2 1 -1 13 -1 2 -25

4 9 2 1 -1 13 -53 2 -25 102

2 2 1 0 13 -53 119 -25 102 -229

1 0 -53 119 102 -229

=> gcd(229,119) = 1, s = -53, t = 102

--------------------------------------------------------------------------------------

(3). gcd(359,78)

q r1 r2 r s1 s2 s t1 t2 t

4 359 78 47 1 0 1 0 1 -4

1 78 47 31 0 1 -1 1 -4 5

1 47 31 16 1 -1 2 -4 5 -9

1 31 16 15 -1 2 -3 5 -9 14

1 16 15 1 2 -3 5 -9 14 -23

15 15 1 0 -3 5 -78 14 -23 359

1 0 5 -78 -23 359

=> gcd(359,78) = 1, s = 5, t = -23

--------------------------------------------------------------------------------------

(4). gcd(487,157)

q r1 r2 r s1 s2 s t1 t2 t

3 487 157 16 1 0 1 0 1 -3

9 157 16 13 0 1 -9 1 -3 28

1 16 13 3 1 -9 10 -3 28 -31

4 13 3 1 -9 10 -49 28 -31 152

3 3 1 0 10 -49 157 -31 152 -487

1 0 -49 157 152 -487

=> gcd(487,157) = 1, s = -49, t = 152

--------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------

2.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

~ 乘法反元素(Multiplicative Inverse) ~

~ Zn:　a x b = 1 (mod n) ~

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

(1) 𝛼 =7, 𝑛 =31

gcd(31, 7) = 1 => 有乘法反元素

q r1 r2 r t1 t2 t

4 31 7 3 0 1 -4

2 7 3 1 1 -4 9

3 3 1 0 -4 9 -31

1 0 9 -31

=> gcd(31,7) = 1, 7的乘法反元素 = 9

--------------------------------------------------------------------------------------

(2) 𝛼 =11, 𝑛 =29

gcd(29,11) = 1 => 有乘法反元素

q r1 r2 r t1 t2 t

2 29 11 7 0 1 -2

1 11 7 4 1 -2 3

1 7 4 3 -2 3 -5

1 4 3 1 3 -5 8

3 3 1 0 -5 8 -29

1 0 8 -29

=> gcd(29,11) = 1, 11的乘法反元素 = 8

--------------------------------------------------------------------------------------

(3) 𝛼 =31, 𝑛 =199

gcd(199,31) = 1 => 有乘法反元素

q r1 r2 r t1 t2 t

6 199 31 13 0 1 -6

2 31 13 5 1 -6 13

2 13 5 3 -6 13 -32

1 5 3 2 13 -32 45

1 3 2 1 -32 45 -77

2 2 1 0 45 -77 199

1 0 -77 199

=> gcd(199,31) = 1, 31的乘法反元素 = -77 or 122

--------------------------------------------------------------------------------------

(4) 𝛼 =27, 𝑛 =666

gcd(666,27) = 9

q r1 r2 r t1 t2 t

24 666 27 18 0 1 -24

1 27 18 9 1 -24 25

2 18 9 0 -24 25 -74

9 0 25 -74

=> gcd(666,27) = 9, 27的乘法反元素不存在

--------------------------------------------------------------------------------------

--------------------------------------------------------------------------------------

3.

(1) 4𝑥 −19 ≡6 (mod 29)

4x ≡ 25 (mod 29)

gcd(4,29) = 1, 只有一解

q r1 r2 r s1 s2 s t1 t2 t

7 29 4 1 1 0 1 0 1 -7

4 4 1 0 0 1 -4 1 -7 25

1 0 1 -4 -7 25

=> 1 = 29 x 1 + 4 x (-7)

=> 25 = 29 x 25 + 4 x (-175)

=> (29 會消掉)

=> x = -175 = 28 (mod 29)

=> x = 28 + 29k

--------------------------------------------------------------------------------------

(2) 8𝑥 +7 ≡ 4 (mod 17)

8x ≡ -3 (mod 17) => 8x ≡ 14 (mod 17)

gcd(8,17) = 1, 只有一解

q r1 r2 r s1 s2 s t1 t2 t

2 17 8 1 1 0 1 0 1 -2

8 8 1 0 0 1 -8 1 -2 17

1 0 1 -8 -2 17

=> 1 = 17 x 1 + 8 x (-2)

=> 14 = 17 x (1 x 14) + 8 x (-2 x 14)

=> (17會消掉)

=> x = -28 = 6 (mod 17)

=> x = 6 + 17k

--------------------------------------------------------------------------------------

(3) 10𝑥 −1 ≡ 4 (mod 23)

10x ≡ 5(mod 23)

gcd(10,23) = 1, 只有一解

q r1 r2 r s1 s2 s t1 t2 t

2 23 10 3 1 0 1 0 1 -2

3 10 3 1 0 1 -3 1 -2 7

3 3 1 0 1 -3 10 -2 7 -23

1 0 -3 10 7 -23

=> 1 = 10 x 7 + 23 x (-3)

=> 5 = 10 x 35 + 23 x (-3 x 5)

=> (23會消掉)

=> x = 35 = 12 (mod 23)

=> x = 12 + 23k

--------------------------------------------------------------------------------------

(4) 7𝑥 ≡ 2 (mod 31)

gcd(7,31) = 1, 只有一解

q r1 r2 r s1 s2 s t1 t2 t

4 31 7 3 1 0 1 0 1 -4

2 7 3 1 0 1 -2 1 -4 9

3 3 1 0 1 -2 7 -4 9 -31

1 0 -2 7 9 -31

=> 1 = 7 x 9 + 31 x (-2)

=> 2 = 7 x 18 + 31 x (-2 x 2)

=> (31會消掉)

=> x = 18 (mod 31)

=> x = 18 + 31k

--------------------------------------------------------------------------------------

(5) { 2𝑥 ≡ 4 (mod 7)

{9𝑥 ≡5 (mod 8)

=>{𝑥 ≡ 2 (mod 7)

{𝑥 ≡5 (mod 8)

=> Chinese Remainder Theorem

n1 = 7, n2 = 8

r1 = 2, r2 = 5, n = n1n2 = 56

N1 = n/n1 = 8,

N2 = n/n2 = 7

M1 ≡ N1^-1 ≡ 8^-1 (mod 7) ≡ 1,

M2 ≡ N2^-1 ≡ 7^-1 (mod 8) ≡ -1

取x ≡ r1M1N1 + r2M2N2 ≡ 2 x 1 x 8 + 5 x (-1) x 7 ≡ 16 + (-35) ≡ -19 (mod 56) ≡ 37 (mod 56)