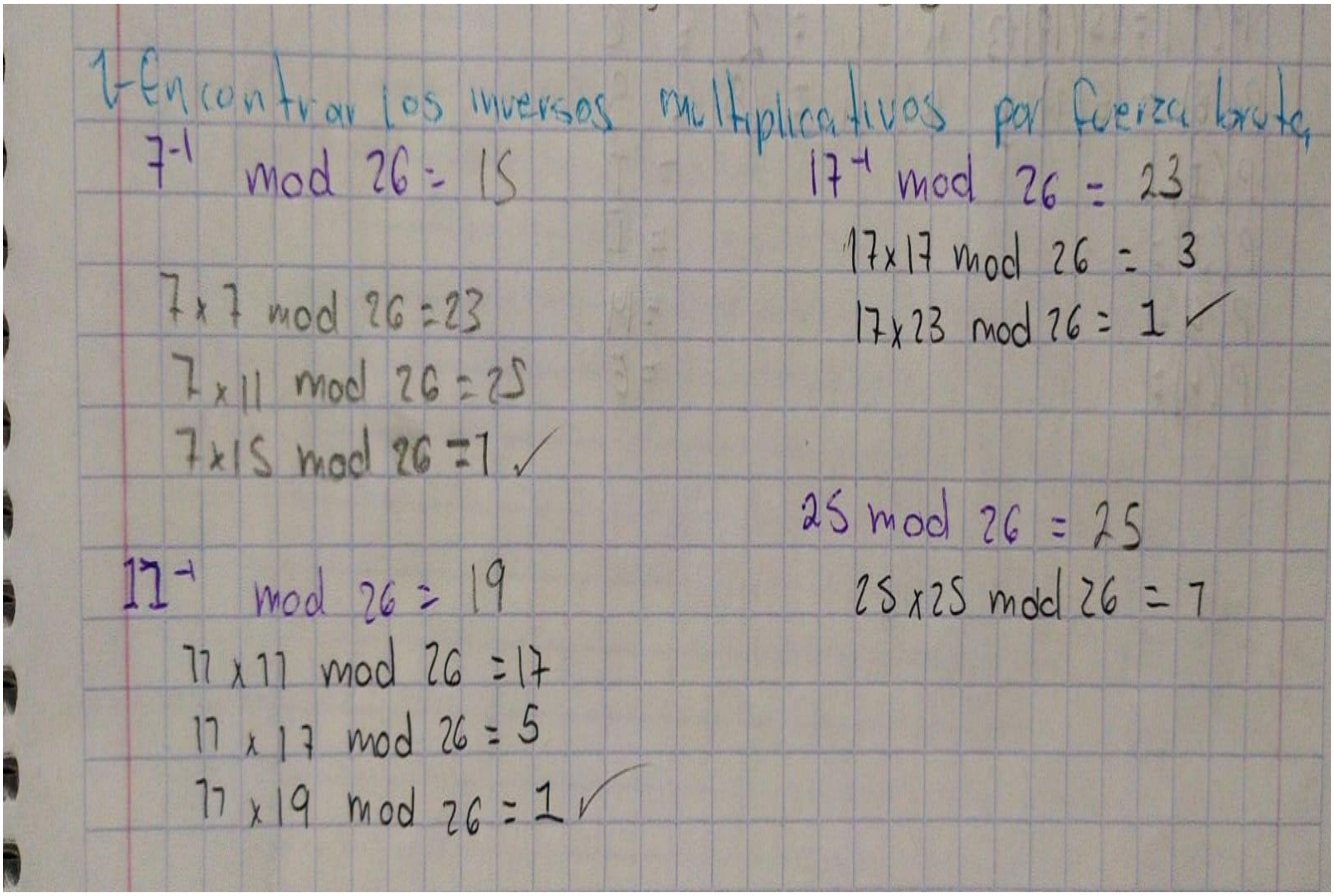


1- Encontrar los inversos multiplicativos por fuerza bruta,

7^{-1} mod 26 = 15

7 x 7 mod 26 = 23

7 x 11 mod 26 = 25

7 x 15 mod 26 = 1 ✓

11^{-1} mod 26 = 19

11 x 11 mod 26 = 17

11 x 17 mod 26 = 5

11 x 19 mod 26 = 1 ✓

17^{-1} mod 26 = 23

17 x 17 mod 26 = 3

17 x 23 mod 26 = 1 ✓

25 mod 26 = 25

25 x 25 mod 26 = 1

α	1	3	5	7	9	11	15	17	19	21	23	25
α^{-1}	1	9	21	15	3	19	7	23	11	5	17	25

gercicio 3 Let encryption function $C = 7p + 5 \mod 26$

Find the decryption Function $p = \quad \mod 26$

Find the plainText

Ciphertext L F I C H L F I J T B I J L H

plainText M A T H E M A T I C S T I M E

$C = 7p + 5 \mod 26$

$p = \frac{C-5}{7}$

$p = 7^{-1}(C + (-5)) \mod 26$ 26-5=21

$p = 15(C + 21) \mod 26$

$p = 15C + 3 \mod 26$

$P(L) = 15(11) + 3 \mod 26 = 12 = M$

$P(F) = 15(5) + 3 \mod 26 = 0 = A$

$P(I) = 15(8) + 3 \mod 26 = 19 = T$

$P(C) = 15(2) + 3$ " " $= 7 = H$

$P(H) = 15(7) + 3$ " " $= 4 = E$

$P(L) = \quad = M$

$P(F) = \quad = A$

$P(I) = \quad = T$

$P(J) = 15(9) + 3$ " " $= 8 = I$

$P(T) = 15(19) + 3$ " " $= 2 = C$

$P(B) = 15(1) + 3$ " " $= 18 = S$

$P(I) = \quad = T$

$P(J) = \quad = I$

$P(L) = \quad = M$

$P(H) = \quad = E$

En los sigtes casos:

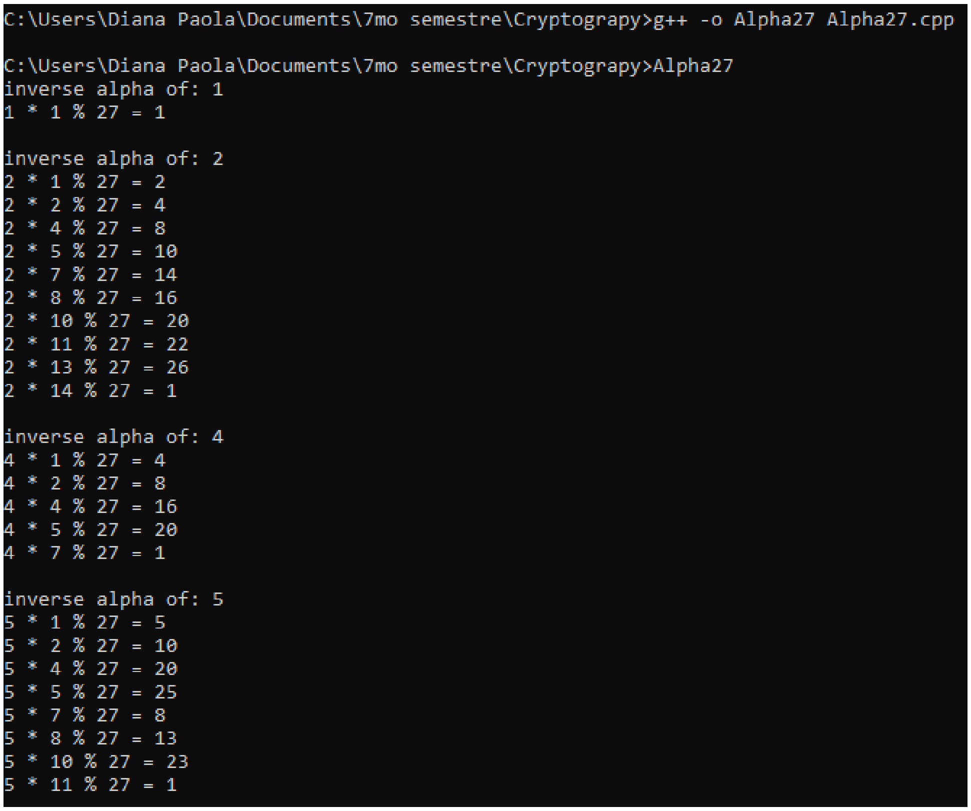
- Listar los valores que puede tomar alpha
- ¿Cuantos serían en total?
- Calcular 3^{-1} mod n (mostrar procedimiento y comprobación

Conjunto	# elementos / descomposición	Conjunto Alpha	total de valores para alpha	3^{-1} mod n
simbolos ¡!¿?{}&	7	"α" = {1, 2, 3, 4, 5, 6}	6	5
Digitos del Ø al 9	10 $10 = 2 \times 5$	"α" = {1, 3, 7, 9}	4	7
letras de la A a la L	12 $12 = 2^2 * 3$	"α" = {1, 5, 7, 11}	4	No existe
Alfabeto en ingles	26 $26 = 2 * 13$	"α" = {1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25}	12	9
Alfabeto en ingles	27 $27 = 3 \times 3 \times 3$	"α" = {1, 2, 4, 5, 7, 8, 10, 11, 13, 14, 16, 17, 19, 20, 22, 23, 25, 26}	18	No existe
Alfabeto en Ingles y los símbolos -, +, *	29	"α" = {1, 2, 3, 4, ... 28}	28	10
ASCII completo	256 $256 = 2^8$	impares "α" = {1, 3, 5, 7, 9, 11, 13, ..., 253, 255}	128	171
Español y 3 símbolos	30 $30 = 2 \times 3 \times 5$	"α" = {1, 7, 11, 13, 17, 19, 23, 29}	8	No existe

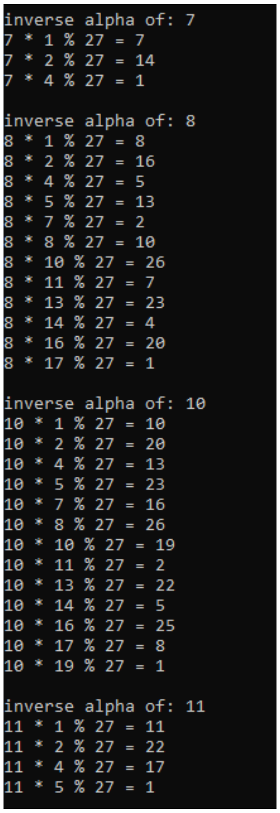
- Observación si los # de elementos es primo α va de 1 hasta el primo - 1 (como 7 y 29)

Ej.2 : Considera el alfabeto en español, encontrar los inversos multiplicativos por fuerza bruta

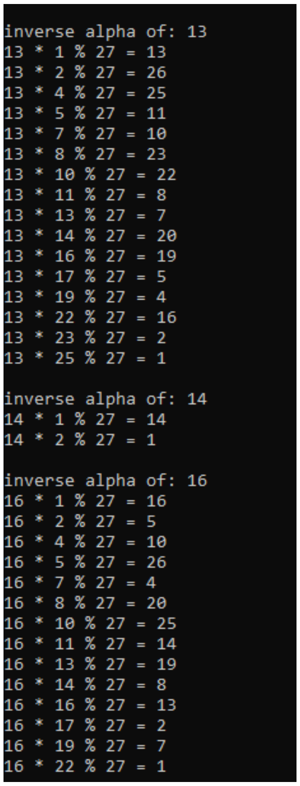
alpha	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23	25	26
Inverse	1	14	7	11	4	17	19	5	25	2	22	8	10	23	16	20	13	26



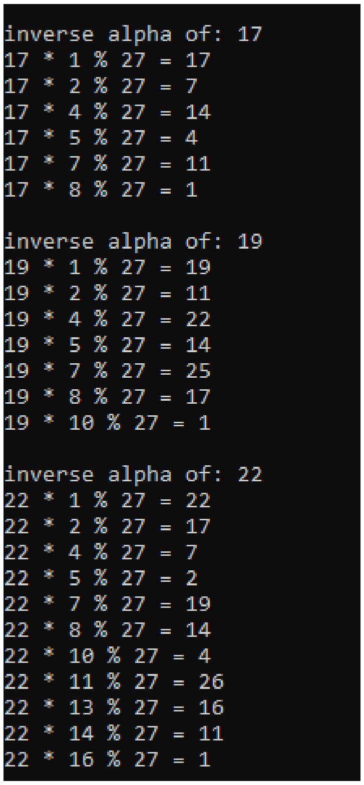
```
C:\Users\Diana Paola\Documents\7mo semestre\Cryptograpy>g++ -o Alpha27 Alpha27.cpp

C:\Users\Diana Paola\Documents\7mo semestre\Cryptograpy>Alpha27
inverse alpha of: 1
1 * 1 % 27 = 1

inverse alpha of: 2
2 * 1 % 27 = 2
2 * 2 % 27 = 4
2 * 4 % 27 = 8
2 * 5 % 27 = 10
2 * 7 % 27 = 14
2 * 8 % 27 = 16
2 * 10 % 27 = 20
2 * 11 % 27 = 22
2 * 13 % 27 = 26
2 * 14 % 27 = 1

inverse alpha of: 4
4 * 1 % 27 = 4
4 * 2 % 27 = 8
4 * 4 % 27 = 16
4 * 5 % 27 = 20
4 * 7 % 27 = 1

inverse alpha of: 5
5 * 1 % 27 = 5
5 * 2 % 27 = 10
5 * 4 % 27 = 20
5 * 5 % 27 = 25
5 * 7 % 27 = 8
5 * 8 % 27 = 13
5 * 10 % 27 = 23
5 * 11 % 27 = 1
```



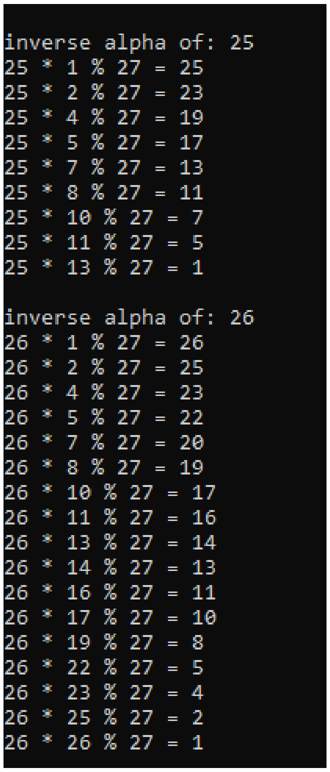
```
inverse alpha of: 7
7 * 1 % 27 = 7
7 * 2 % 27 = 14
7 * 4 % 27 = 1

inverse alpha of: 8
8 * 1 % 27 = 8
8 * 2 % 27 = 16
8 * 4 % 27 = 5
8 * 5 % 27 = 13
8 * 7 % 27 = 2
8 * 8 % 27 = 10
8 * 10 % 27 = 26
8 * 11 % 27 = 7
8 * 13 % 27 = 23
8 * 14 % 27 = 4
8 * 16 % 27 = 20
8 * 17 % 27 = 1

inverse alpha of: 10
10 * 1 % 27 = 10
10 * 2 % 27 = 20
10 * 4 % 27 = 13
10 * 5 % 27 = 23
10 * 7 % 27 = 16
10 * 8 % 27 = 26
10 * 10 % 27 = 19
10 * 11 % 27 = 2
10 * 13 % 27 = 22
10 * 14 % 27 = 5
10 * 16 % 27 = 25
10 * 17 % 27 = 8
10 * 19 % 27 = 1

inverse alpha of: 11
11 * 1 % 27 = 11
11 * 2 % 27 = 22
11 * 4 % 27 = 17
11 * 5 % 27 = 1
```



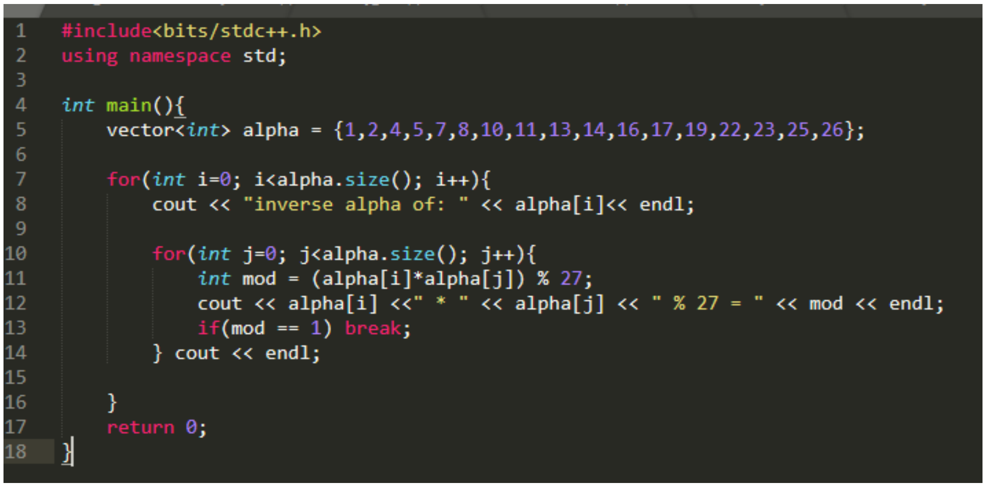
```
inverse alpha of: 13
13 * 1 % 27 = 13
13 * 2 % 27 = 26
13 * 4 % 27 = 25
13 * 5 % 27 = 11
13 * 7 % 27 = 10
13 * 8 % 27 = 23
13 * 10 % 27 = 22
13 * 11 % 27 = 8
13 * 13 % 27 = 7
13 * 14 % 27 = 20
13 * 16 % 27 = 19
13 * 17 % 27 = 5
13 * 19 % 27 = 4
13 * 22 % 27 = 16
13 * 23 % 27 = 2
13 * 25 % 27 = 1

inverse alpha of: 14
14 * 1 % 27 = 14
14 * 2 % 27 = 1

inverse alpha of: 16
16 * 1 % 27 = 16
16 * 2 % 27 = 5
16 * 4 % 27 = 10
16 * 5 % 27 = 26
16 * 7 % 27 = 4
16 * 8 % 27 = 20
16 * 10 % 27 = 25
16 * 11 % 27 = 14
16 * 13 % 27 = 19
16 * 14 % 27 = 8
16 * 16 % 27 = 13
16 * 17 % 27 = 2
16 * 19 % 27 = 7
16 * 22 % 27 = 1
```



```
inverse alpha of: 17
17 * 1 % 27 = 17
17 * 2 % 27 = 7
17 * 4 % 27 = 14
17 * 5 % 27 = 4
17 * 7 % 27 = 11
17 * 8 % 27 = 1

inverse alpha of: 19
19 * 1 % 27 = 19
19 * 2 % 27 = 11
19 * 4 % 27 = 22
19 * 5 % 27 = 14
19 * 7 % 27 = 25
19 * 8 % 27 = 17
19 * 10 % 27 = 1

inverse alpha of: 22
22 * 1 % 27 = 22
22 * 2 % 27 = 17
22 * 4 % 27 = 7
22 * 5 % 27 = 2
22 * 7 % 27 = 19
22 * 8 % 27 = 14
22 * 10 % 27 = 4
22 * 11 % 27 = 26
22 * 13 % 27 = 16
22 * 14 % 27 = 11
22 * 16 % 27 = 1
```



```
inverse alpha of: 25
25 * 1 % 27 = 25
25 * 2 % 27 = 23
25 * 4 % 27 = 19
25 * 5 % 27 = 17
25 * 7 % 27 = 13
25 * 8 % 27 = 11
25 * 10 % 27 = 7
25 * 11 % 27 = 5
25 * 13 % 27 = 1

inverse alpha of: 26
26 * 1 % 27 = 26
26 * 2 % 27 = 25
26 * 4 % 27 = 23
26 * 5 % 27 = 22
26 * 7 % 27 = 20
26 * 8 % 27 = 19
26 * 10 % 27 = 17
26 * 11 % 27 = 16
26 * 13 % 27 = 14
26 * 14 % 27 = 13
26 * 16 % 27 = 11
26 * 17 % 27 = 10
26 * 19 % 27 = 8
26 * 22 % 27 = 5
26 * 23 % 27 = 4
26 * 25 % 27 = 2
26 * 26 % 27 = 1
```



```cpp
#include<bits/stdc++.h>
using namespace std;

int main(){
    vector<int> alpha = {1,2,4,5,7,8,10,11,13,14,16,17,19,22,23,25,26};

    for(int i=0; i<alpha.size(); i++){
        cout << "inverse alpha of: " << alpha[i]<< endl;

        for(int j=0; j<alpha.size(); j++){
            int mod = (alpha[i]*alpha[j]) % 27;
            cout << alpha[i] <<" * " << alpha[j] << " % 27 = " << mod << endl;
            if(mod == 1) break;
        } cout << endl;

    }
    return 0;
}
```