Miguel Torres Alonso **75939697E**

Entrega de ejercicios de los temas 1, 2 y 3
Aritmética entera y modular. Polinomios y cuerpos finitos. Combinatoria

- **Ejercicio 1:**
  Sea a el número formado por las tres últimas cifras de tu DNI y p el siguiente número primo: Calcula cuántas soluciones del siguiente sistema de congruencias hay entre −100000 y 200000:

$$12x \equiv 18 \text{ mód } 39$$
$$7^{365}x \equiv 16 \text{ mód } 29$$
$$17x \equiv 153 \text{ mód } p$$

3 últimas cifras DNI: 75939**697**
Siguiente número primo = p = 701

$$12x \equiv 18 \text{ mód } 39 \rightarrow mcd(12,39) = 3|18$$

$4x \equiv 6 \text{ mod } 13 \rightarrow 13 = 4*3 +1$

13		0
4		1
1	3	$v_1 = 0-3*1 = -3 = 10$

$4^{-1} \text{ mod } 13 = 10 \rightarrow x \equiv 60 \text{ mod } 13 \rightarrow x \equiv 8 \text{ mod } 13 \rightarrow$ $\underline{x = 8 + 13k_1}$

$$7^{365}x \equiv 16 \text{ mód } 29$$
$7^{\varphi(29)} \text{ mod } 29 = 1$; $\varphi(29) = 28$; $365 = 28*13 + 1 \rightarrow 7x \equiv 16 \text{ mod } 29$
$7(8 + 13k_1) \equiv 16 \text{ mod } 29$; $56 + 91k_1 \equiv 16 \text{ mod } 29$; $91k_1 \equiv 16 - 56 \text{ mod } 29$;
$4k_1 \equiv 18 \text{ mod } 29 \rightarrow mcd(4,29) = 1 \rightarrow 29 = 4*7 + 1$;

29		0
4		1
1	7	$v_1 = 0 - 7*1 = -7 = 22$

$4^{-1} \text{ mod } 29 = 22$; $k_1 \equiv 18*22 \text{ mod } 29$; $k_1 \equiv 19 \text{ mod } 29 \rightarrow k_1 = 19 + 29k_2$
$\underline{x = 8 + 13(19 + 29k_2) = 255 + 377k_2}$

$$17x \equiv 153 \text{ mod } 701$$
Tenemos que $x = 255 + 377k_2$; $17(255 + 377k_2) \equiv 153 \text{ mod } 701$
$100k_2 \equiv 24 \text{ mod } 701 \rightarrow mcd(100,701) = 1|24$
$701 = 100*7 + 1$

701		0
100		1
1	7	v_1 = -7 = 694

$k_2 \equiv 24 * 694 \bmod 701$
$k_2 \equiv 533 \bmod 701$ -> $k_2 = 533 + 701k$

$x = 255 + 377k_2$
$x = 255 + 377(533 + 701k)$; $x = 201196 + 264277$, $k \in \mathbb{Z}$

¿Cuántas soluciones hay entre -100.000 y 200.000?

-100.000 <= x <= 200.000
-100.000 <= 201196 + 264277k <= 200.000
-301.196 <= 264277k <= -1.196
k >= -1.14 y k <= -0.004, por tanto no existen soluciones entre -100.000 y 200.000 con $k \in \mathbb{Z}$

- **<u>Ejercicio 2:</u>**
  - **Sea ‘d’ tu número de DNI (con 8 cifras. Si tuviera menos, completa con ceros). Sea ‘m’ el número que resulta de escribir ‘d’ 10 veces consecutivas, y sea ‘p’ el primer primo fuerte que hay mayor que el número ‘m’. Sea ‘q’ un primo fuerte de 300 bits. A partir de los primos p y q construye una clave RSA, con n = ‘p’ * ‘q’ y e = 65537, y envía a jesusgm@ugr.es la clave pública. Recibirás como respuesta a ese correo un mensaje que tienes que descifrar.**
  - **Elige un mensaje (máximo 400 caracteres) que sólo contenga letras mayúsculas y espacios, y cífralo con la siguiente clave pública:**
    **n=66692299011319053574573175316458307050477179729240556600324522576
    24972579609459132412433416773877843377920115368308659082552721472339
    5183556298859701235135770931232576347098519499649920906695095797156
    9350281579488837706495607915920227347766063044468284030932007924588
    3834239494189279695634494154776560255013702247766725254894323495134
    0429089247404833207650072382156628814432504591543037662171767600144
    0729621615575722552631917766769839563004543335463205676595638075407
    26172713593389351966801195765776916644293251620096945292406087383628
    22400980330763924301823036956316823083404200808621110970241438268910
    96714405277**
    e=65537

d = 75939697
m =
7593969775939697759396977593969775939697759396977593969775939697759396977
5939697

Para la realización de este ejercicio, modifiqué el código proporcionado en SWAD de RSA.

Por ejemplo, para generar las claves RSA, modifiqué el siguiente pedazo de código:

```
def menu():
    print('Introduce una opción:')
    print('   1. Generar claves RSA.')
    print('   2. Cifrar un mensaje')
    print('   3. Descifrar un mensaje')
    print('   4. Salir.')
    op = input("")
    if op == '1':
        d = int(input("Introduce tu DNI: "))
        m = str(d) * 10
        print("\nDNI escrito 10 veces consecutivas: \n")
        print(m)
        p = siguienteprimofuerte(int(m))
        print("\nSiguiente primo fuerte del DNI escrito 10 veces consecutivas: \n")
        print(p)
        print("\nGenerando valor 'q', primo fuerte de 300 bits: \n")
        q = primofuertenbits(300)
        print("\nValor de 'q': \n")
        print(q)
        ……………
        ……………
        ……………
        ……………
```

Lo que hace es a partir de las cifras del DNI, las escribe 10 veces consecutivas y calcula el siguiente primo fuerte de dicho número y lo guarda en p, después genera el valor q aleatorio.

El mensaje cifrado enviado por el profesor es el siguiente:
IMZ KVNCYQQWKÑMFZPKCCLMWLFEAQHKYSWÑNYVTMUQAWUPM
ZQLVLFDUTJHNNQBFSLTHJOLXVVEIVWLHXLZZBÑMÑAHOIYNLUGIVDHFSCHKLVEVJV JÑÑZB

El cual una vez descifrado significa:
BUENAS NOCHES MIGUEL PUEDES PROBAR A HACERLE A TUS COMPAÑEROS EL TRUCO DE LAS CARTAS

Para el apartado 2, el texto cifrado con la clave pública que se indica es este:
SJVFLDEWUGOMPNBMEUFMBYACÑWUYTXWYXAQICGLEXSFXAKJDZJ RJD CPSIF
DJMCÑKEBAMNPCÑCHTNITPALMGJUHSFKUMJFÑTRUJX
MÑXSLLAXZSVDDXRSGRÑLVIRSPPZVÑGWPGMYNJLVPBZDXUWARYYFPJYQUXYÑIL
ÑAMOREMJRMN KOXNEFSSVFWOEONYÑEÑHPDXXATCUWNEGILJYTCWHPDZ IBAN
GÑBRÑGOUMZEHFKZBGUMELQIYMHSFNHAIIYRESWQZYÑFEGXQCCCZQUZPOOILXTOYHIBL
IFÑUGNPNIEFKWKCSMBVBKDMYFYDRTMWPSDFOXQGMFSHPNNPHMQFZCWMQUMG
LOUYIGQK XGHCÑOPÑÑXEOLMBPHNEXMTYHZUDVCC
DJTKSVYKKDWTÑRJQPHQESXUDWLVV Q

- **Ejercicio 3:**
  Una bodega debe entregar un pedido de 81000 litros de vino sin embotellar. Para hacerlo, dispone de camiones cisterna con capacidad de 3500 litros, y remolques con capacidad de 1500 litros. Cada camión puede llevar como mucho un remolque, y tanto los remolques como las cisternas deben ir llenos. ¿Cuántos camiones y remolques se han de utilizar si queremos que el número de viajes sea mínimo?

$3500x + 1500y = 81000$
mcd(3500, 1500) -> 3500 = 1500 * 2 + 500 ; 1500 = 500 * 3 + 0 -> mcd(3500, 1500) = 500|81000

Se divide toda la ecuación entre el mcd.
$7x + 3y = 162$
$7x \equiv 162 \mod 3$; $x \equiv 0 \mod 3$ -> $x = 0 + 3k$ -> $\underline{x = 3k, k \in \mathbb{Z}}$.
$7(3k) + 3y = 162$; $21k + 3y = 162$ -> $\underline{y = 54-7k, k \in \mathbb{Z}}$.

Como cada camión puede llevar como mucho 1 solo remolque, 0 <= y <= x
0 <= 54 - 7k <= 3k ; Resolvemos por un lado 0 <= 54 - 7k y por otro lado 54 - 7k <= 3k
La primera inecuación resulta k <= 7,7 y la segunda inecuación k >= 5,4.
Osea, 5,4 <= k <= 7,7, por lo que si queremos minimizar viajes nos quedamos con k = 6 que se traduce en utilizar 18 camiones cisterna y 12 remolques.

- **Ejercicio 4:**
  Si representamos los números enteros como cadenas de 32 bits, calcula un número entero x, entre 65500 y 65600 tal que al calcular $x^2 + 2^{17}$ dé como resultado 1. Una vez encontrado el número x, realiza los cálculos en complemento a 2 y justifica el resultado obtenido.

Con 32 bits, el bit de mayor peso es 2^{31}. Por tanto, para que $x^2 + 2^{17}$ nos de como resultado 1, habría que igualar dicha ecuación a $2^{32} + 1$, por lo que al ser cadenas de 32 bits se ignoraría el bit de 2^{32} y nos quedarían 31 bits a 0 y el bit de menor peso en 1.
$x^2 + 2^{17} = 2^{32} + 1$; $x^2 = 2^{32} + 1 - 2^{17}$ -> $x = 65535$

Justificación en complemento a 2:

- **Ejercicio 5:**
  Sean $p(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$ y $q(x) = x^6 + x^5 + x^4 + x^2 + x + 1$ dos polinomios con coeficientes en $\mathbb{Z}_3$. Calcula mcd(p(x), q(x)). Factoriza p(x) como producto de irreducibles.

$p(x) = x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$
$q(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$

Primero calculamos mcd(p(x), q(x)) mediante el algoritmo de Euclides.

· $x^7 + x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^6 + x^5 + x^4 + x^2 + x + 1) * c_1(x) + r_1(x)$

	1	1	1	1	1	1	1	1
2 |		2	0					
2 |			2	0				
0 |				0	0			
2 |					2	0		
2 |						2	0	
2 |							2	0
	1	0	0	1	0	0	0	1

$c_1(x) = x$
$r_1(x) = x^4 + 1$

· $x^6 + x^5 + x^4 + x^2 + x + 1 = (x^4 + 1) * c_2(x) + r_2(x)$

	1	1	1	0	1	1	1
0 |		0	0	0			
0 |			0	0	0		
0 |				0	0	0	
2 |					2	2	2
	1	1	1	0	0	0	0

$c_2(x) = x^2 + x + 1$
$r_2(x) = 0$

Por tanto, <u>mcd(p(x), q(x)) = $x^4 + 1$</u>

Para factorizar p(x) como producto de irreducibles, se divide el polinomio por las posibles raíces (polinomios irreducibles) de grado menor que la mitad del grado del polinomio, es decir, las posibles raíces en $\mathbb{Z}_3$ de grado 3 o menor, pues 7/2 = 3,5 ≈ 3

	1	1	1	1	1	1	1	1
|								
|								
2 |		2	0	2	0	2	0	2
	1	0	1	0	1	0	1	0

divisor = $x + 1$
$c_1(x) = x^6 + x^4 + x^2 + 1$
$r_1(x) = 0$

$p(x) = (x + 1)(x^6 + x^4 + x^2 + 1)$, reducimos el segundo paréntesis.

	1	0	1	0	1	0	1
|							
2 |		2	1	0	1	1	
1 |			1	2	0	2	2
	1	2	0	2	2	0	0

divisor = $x^2 + x + 2$
$c_2(x) = x^4 + 2x^3 + 2x + 2$
$r_2(x) = 0$

$x^6 + x^4 + x^2 + 1 = (x^2 + x + 2)(x^4 + 2x^3 + 2x + 2)$, reducimos segundo paréntesis.

	1	2	0	2	2
|					
1 |		1	0	1	
1 |			1	0	1
	1	0	1	0	0

divisor = $x^2 + 2x + 2$
$c_3(x) = x^2 + 1$
$r_3(x) = 0$

Y ya no podemos reducir más, por tanto $p(x) = (x + 1)(x^2 + x + 2)(x^2 + 2x + 2)(x^2 + 1)$

- **Ejercicio 6:**
  Sea A = $\mathbb{Z}_3[x]_{x^4+x^3+3x^2+4}$.
  - **¿Cuántos elementos tiene A?**
  - **¿Es A un cuerpo?**
  - **Realiza en A, si es posible, los siguientes cálculos:**
    - **$(3x^3 + 4x^2 + x + 2) * (4x^3 + x^2 + 2)$.**
    - **$(2x^2 + 1) \cdot (x^3 + 3x^2 + 2) + (2x^3 + 3x + 3)^{-1} (x^3 + 2)^2$.**
    - **$(2x^3 + x^2 + x + 4)^{-1} * (x^3 + x)$.**

A tiene p^n elementos = $5^4 = 625$.
$K[x]_{m(x)}$ es un cuerpo si k es un cuerpo y m(x) es irreducible.

	1	1	3	0	4
2		2	1	3	1
	1	3	4	3	0

Vemos que m(x) no es irreducible, por tanto A no es un cuerpo.

• $(3x^3 + 4x^2 + x + 2) * (4x^3 + x^2 + 2) = 2x^6 + 4x^5 + 3x^4 + 2x + 4$, esto se divide entre m(x) porque es mod m(x) y nos quedamos con el resto.

	2	4	3	0	0	2	4
4		3	3	0			
2			4	4	0		
0				0	0	0	
1					2	2	0
	2	2	0	4	2	4	4

$c(x) = 2x^2 + 2$
$\underline{r(x) = 4x^3 + 2x^2 + 4x + 4}$

• $(2x^2 + 1) \cdot (x^3 + 3x^2 + 2) + (2x^3 + 3x + 3)^{-1} (x^3 + 2)^2$
Para calcular el inverso, mcd(p(x), m(x)) = 1, por tanto vamos a averiguar el mcd.

$x^4 + x^3 + 3x^2 + 4 = (2x^3 + 3x + 3) * c_1(x) + r_1(x)$ -> el divisor tiene que ser mónico, se multiplica todo por el inverso del coeficiente líder al hacer ruffini.

	1	1	3	0	4
$2^{-1} = 3$					
0		0	0		
-3*3=1			1	1	
-3*3=1				1	1
	1	1	4	2	0

$c_1(x) = 3(x+1)$
$r_1(x) = 4x^2 + 2x$

$2x^3 + 3x + 3 = (4x^2 + 2x) * c_2(x) + r_2(x)$

```
            2   0   3   3
4^-1 = 4  |
-2*4=2 |      4   3
       0 |          0   0
—-------------------------------
             2  4   1   3
```

$c_2(x) = 4(2x + 4)$
$r_2(x) = x + 3$

$4x^2 + 2x = (x + 3) * c_3(x) + r_3(x)$

```
            4   2   0
          |
          |
       2 |
—-------------------------------
            4   0   0
```

$c_3(x) = 4x$
$r_3(x) = 0$

$(2x^3 + 3x + 3)^{-1}$ no se puede calcular porque el mcd es distinto de 1.

• $(2x^3 + x^2 + x + 4)^{-1} * (x^3 + x)$.
$(2x^3 + x^2 + x + 4)^{-1}$ se puede calcular si $mcd(p(x), m(x)) = 1$.

$x^4 + x^3 + 3x^2 + 4 = (2x^3 + x^2 + x + 4) * c_1(x) + r_1(x)$

```
           1   1   3   0   4
2^-1 = 3  |
-1*3=2 |      2   1
-1*3=2 |          2   1
-4*3=3 |              3   4
—-------------------------------
           1   3   1   4   3
```

$c_1(x) = 3(x + 3) = 3x + 4$
$r_1(x) = x^2 + 4x + 3$

$2x^3 + x^2 + x + 4 = (x^2 + 4x + 3) * c_2(x) + r_2(x)$

```
     2   1   1   4
   |
1 |      2   3
2 |          4   1
—-----------------------------------
     2   3   3   0
```

$c_2(x) = 2x + 3$
$r_2(x) = 3x$

$x^2 + 4x + 3 = 3x * c_3(x) + r_3(x)$

```
     1   4   3
  |
  |
0 |      0   0
—-----------------------------------
     1   4   3
```

$c_3(x) = 2(x+4)$

$r_3(x) = 3$, siguiente resto va a ser 0

Como el siguiente resto va a ser 0, el mcd es 3. No se puede calcular el inverso.

- **Ejercicio 7:**
  ¿Cuántos números hay de cinco cifras con las cifras en orden estrictamente creciente? ¿Y en orden creciente?

El primer número con 5 cifras es el 10000 y el último es el 99999.
El primer número con 5 cifras estrictamente creciente es el 12345 y el último el 56789.

Apartado 1

```
_   _   _   _   _
1   2   3   4   5
|   |   |   |   |
5   6   7   8   9
```

Tenemos entonces $5*5*5*5*5 = 5^5 =$ 3125.

Apartado 2
El primer número con 5 cifras creciente es el 11111 y el último el 99999

```
_   _   _   _   _
1   1   1   1   1
|   |   |   |   |
9   9   9   9   9
```

Tenemos entonces $9*9*9*9*9 = 9^5 =$ 59049.

- **Ejercicio 8:**
  Consideramos las letras de la palabra SOMETAMOS

1. **¿De cuántas formas las podemos ordenar?**
2. **¿En cuántas ordenaciones están juntas la T y la A?**
3. **¿En cuántas ordenaciones aparecen juntas la E y una S?**
4. **¿En cuántas ordenaciones están juntas todas las vocales?**
5. **¿En cuántas ordenaciones aparece una O inmediatamente después de una S?**

1. ¿De cuántas formas las podemos ordenar?

S - 2
O - 2 PR = 9! / 2! 2! 2! = 45360
M - 2
E - 1
T - 1
A - 1

2. ¿En cuántas ordenaciones están juntas la T y la A?

S - 2
O - 2 PR = 8! / 2! 2! 2! = 5040, multiplicado por 2 porque AT también
M - 2 cuenta, por tanto 10080.
E - 1
x = TA - 1

3. ¿En cuántas ordenaciones aparecen juntas la E y una S?

S - 1
O - 2 PR = 8! / 2! 2! = 10080, por 2 porque SE también cuenta, por tanto
M - 2 20160
ES - 1
T - 1
A - 1

4. ¿En cuántas ordenaciones están juntas todas las vocales?

S - 2
M - 2
T - 1
X - 1
Tenemos con esto 6! / 2! 2! = 180, donde X =
X = O - 2
E - 1
A - 1
Con lo que 4! / 2! = 12, luego 180 * 12 = 2160

5. ¿En cuántas ordenaciones aparece una O inmediatamente después de una S?

SO - 1
M - 2
E - 1
T - 1
A - 1
O - 1
S - 1