ENTREGA 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:

$$\begin{array}{rcll} 12x & \equiv & 18 & \text{mód } 39 \\ 7^{365}x & \equiv & 16 & \text{mód } 29 \\ 17x & \equiv & 153 & \text{mód } p \end{array}$$

Ejercicio 2.

- 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 $n = p \cdot q$ y $e = 65537$, y envía a jesusgm@ugr.es la clave pública. Recibirás como respuesta a ese correo un mensanje 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 = 46669229901131905357457317531645830705047717972924055660032452257624972579609485913241243341677387784337792011536830865908255272147233951835562988597012351357709312325763470985194996499209066950957971569350281579488837706495607915920227347766063044468284030932007924588383423949418927969563449415477656025501370224777667252548943234951340429089247404833207650072382156628814432504591543037662171767600144072962161557572255263191776676983956300454333546320567659563807540726172713593389351966801195765776916644293251620096945292406087383628224009803307639243018230369563168230834042008086211109702414382689109671440527 7

  e = 65537

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?

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.

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 $\text{mcd}(p(x), q(x))$.
- Factoriza $p(x)$ como producto de irreducibles.

Ejercicio 6.
Sea $A = \mathbb{Z}_5[x]_{x^4+x^3+3x^2+4}$.

- ¿Cuántos elementos tiene A?
- ¿Es A un cuerpo?
- Realiza en A, si es posible, los siguientes cálculos:

- $(3x^3 + 4x^2 + x + 2) \cdot (4x^3 + x^2 + 2)$.
- $(2x^2 + 1) \cdot (x^3 + 3x^2 + 2) + (2x^3 + 3x + 3)^{-1}(x^3 + 2)^2$.
- $(2x^3 + x^2 + x + 4)^{-1} \cdot (x^3 + x)$.

¿

- Calcula un elemento $\alpha \in A$ tal que

$$(x^3 + x + 2)(\alpha + x) = \alpha(4x^3 + 4x^2 + 3) + (x^2 + 1).$$

Ejercicio 7.
¿Cuántos números hay de cinco cifras con las cifras en orden estrictamente creciente? ¿Y en orden creciente[1]?

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?
6. ¿En cuántas ordenaciones aparecen juntas una S y una O[2]?

[1] El número 34689 tiene las cifras en orden estrictamente creciente (y por tanto en orden creciente). El número 55789 tiene sus cifras en orden creciente, pero no en orden estrictamente creciente. El número 55555 tiene sus cifras en orden creciente.

[2] Este último apartado es opcional