Conjuntos y Números

LISTA 5 CURSO 2018-19

1) Sabemos que dados dos enteros positivos a y b, existen primos $p_1, \dots, p_s$ de modo que $a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ y $b = p_1^{\beta_1} \cdots p_s^{\beta_s}$ para algunos $\alpha_i, \beta_i \in \mathbb{N}$.

a) Expresa el $\operatorname{mcd}(a, b)$ y el $\operatorname{mcm}(a, b)$ en función de estas factorizaciones.

b) Demuestra que $ab = \operatorname{mcd}(a, b) \cdot \operatorname{mcm}(a, b)$.

c) Halla el máximo común divisor de 1547 y 3059 usando dos procedimientos: el descrito en a) y el algoritmo de Euclides.

2) Encuentra todas las parejas $a, b \in \mathbb{Z}$ tales que $\operatorname{mcd}(a, b) = 10$ y $\operatorname{mcm}(a, b) = 100$.

3) Sea $n = p_1^{n_1} p_2^{n_2} \cdots p_s^{n_s}$ la descomposición de n en factores primos. Utilizando la unicidad de la descomposición en primos, demuestra que n tiene $(n_1 + 1)(n_2 + 1) \cdots (n_s + 1)$ divisores positivos.

4) Demuestra que hay infinitos enteros primos de la forma $4n - 1$ y de la forma $6n - 1$.
`Ayuda`: Recuerda la demostración de Euclides sobre la existencia de infinitos primos.

5) Sea $S \subset \mathbb{Z}$ un subconjunto no vacío que tiene las siguientes dos propiedades:

$$s_1, s_2 \in S \implies s_1 + s_2 \in S$$
$$s \in S \implies -s \in S.$$

Demuestra que $S = \{0\}$ o bien $S = n\mathbb{Z} = \{nk : \ k \in \mathbb{Z}\}$ para algún entero positivo n.

6) Sean a, b, m números naturales con a y b coprimos (primos entre sí). Demuestra que:

$$\text{Si} \quad a \mid m \quad \wedge \quad b \mid m \implies ab \mid m$$

Encuentra un ejemplo que muestre que esto puede no ser cierto si a y b no son coprimos.

7) Halla el conjunto de soluciones de las siguientes ecuaciones diofánticas:
a) $111x + 36y = 15$, b) $10x + 26y = 1224$, c) $6x + 10y = 20$.

8) a) Probar la identidad

$$x^{2k+1} + 1 = (x + 1) \sum_{j=0}^{2k} (-1)^j x^{2k-j}.$$

Utilizar esta identidad para demostrar que si $2^n + 1$ es primo, entonces n es una potencia de 2. Los primos de la forma $2^{2^k} + 1$ se denominan *primos de Fermat*.

b) Probar la identidad

$$x^n - 1 = (x - 1) \sum_{j=0}^{n-1} x^j$$

Utilizar esta identidad para demostrar que si $2^n - 1$ es primo, entonces n es primo. Se denominan *primos de Mersenne* los de la forma $2^n - 1$.

9) Un entero positivo es perfecto si es igual a la suma de sus divisores propios (todos menos él mismo). Demostrar que si $2^n - 1$ es primo entonces $2^{n-1}(2^n - 1)$ es un número perfecto.

10) a) Teniendo en cuenta que $10 \equiv 1 \pmod 9$, prueba que $n \equiv s \pmod 9$ si s es la suma de los dígitos de n; deduce que n es múltiplo de 9 si y sólo si lo es s. ¿Cuándo será n múltiplo de 3?

b) Usando la misma idea, y partiendo de que $10 \equiv -1 \pmod{11}$, deduce qué suma s debemos hacer con los dígitos de n para saber si es múltiplo de 11.

c) Si en vez de dígitos tuviésemos los *bits* del desarrollo de n en base 2, usa: $2 \equiv -1 \pmod 3$ y deduce qué debemos hacer con esos *bits* para saber si n es múltiplo de 3. O con las cifras de n en base $b = 8$ para saber si n es múltiplo de 7.

d) Prueba que, para n, m dados, y si s_n, s_m son las respectivas sumas de sus dígitos, se cumple: $nm \equiv s_n s_m$ mod(9). Deduce qué utilidad puede tener esto si no tenemos la calculadora a mano.

11) a) Sea $\mathcal{U}(\mathbb{Z}_n)$ el subconjunto de $\mathbb{Z}_n$ formado por las unidades de $\mathbb{Z}_n$. Prueba que

$$\overline{a}\overline{b} = \overline{ab} \in \mathcal{U}(\mathbb{Z}_n) \iff \overline{a} \in \mathcal{U}(\mathbb{Z}_n) \text{ y } \overline{b} \in \mathcal{U}(\mathbb{Z}_n)$$

b) Demuestra que la propiedad anterior vale en cualquier anillo conmutativo A (el conjunto $\mathcal{U}(A)$ de unidades es cerrado por el producto).

12) Halla $\mathcal{U}(\mathbb{Z}_7)$ e indica cuál es el inverso multiplicativo de cada uno de sus elementos. Haz lo mismo con $\mathcal{U}(\mathbb{Z}_8)$.

13) a) Demuestra que si $p \in \mathbb{N}$ es primo entonces p divide al número combinatorio $\binom{p}{k}$ para cada $1 \leq k \leq p-1$. ¿Es esto cierto si p no es primo?

b) Probar que si p es primo, en $\mathbb{Z}/p\mathbb{Z}$ se cumple la igualdad $\overline{a}^p + \overline{b}^p = (\overline{a} + \overline{b})^p$.

14) Hallar los inversos de 13 y -15 en $\mathbb{Z}_{23}$ y $\mathbb{Z}_{31}$.

15) Demuestra que la ecuación $13X = 2$ tiene solución única en $\mathbb{Z}_{23}$. Indica cuál es. (Sugerencia: usa el problema anterior).

16) Demuestra que existen infinitos naturales no representables como suma de tres cuadrados.
(Sugerencia: estudia los cuadrados módulo 8).

17) Demuestra que si $n > 1$ y $(n-1)! + 1 \equiv 0 \pmod n$ entonces n es primo.

18) Escribe una sola congruencia que sea equivalente al sistema de congruencias:

$$\begin{cases} x \equiv 1 \pmod 4 \\ x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 7 \end{cases}$$

19) Demuestra que $2222^{5555} + 5555^{2222}$ es divisible por 7.

20) Prueba que $n^7 - n$ es divisible entre 42, para cualquier entero n.

21) Probar que $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es un entero para todo n.

22) He comprado bolígrafos a 55 céntimos y rotuladores a 71 céntimos. Si me he gastado en total 20 euros, ¿cuántos he comprado de cada?

23) Calcula el resto que queda al dividir 3^{2011} entre 11.

24) Tengo una bolsa con 30 caramelos y los voy a repartir entre mis sobrinos, dándoles 2 caramelos a cada niño y 7 a cada niña. ¿Cuántos sobrinos tengo si la menor de mis sobrinas se llama Silvia y los mayores de mis sobrinos se llaman Pablo y Julián?

25) Resolver los sistemas de congruencias:

$$a) \begin{cases} x \equiv -5 \pmod{77} \\ x \equiv 17 \pmod{143} \end{cases} \qquad b) \begin{cases} x \equiv 7 \pmod 8 \\ x \equiv 3 \pmod{12} \end{cases}$$