CONJUNTOS Y NÚMEROS. Curso 2014-2015. **HOJA 4.**

1) Sean A, B y C tres conjuntos tales que $A \subset B \subset C$ y A equipotente a C. Demostrar que también B es equipotente a los otros dos.
Sugerencia: Aplicar uno de los teoremas del curso.

2) Definimos la siguiente relación en $\mathbb{R}$: $x\mathcal{R}y \iff x - y \in \mathbb{Q}$. Demostrar que es una relación de equivalencia. ¿Cuántos elementos tiene cada clase de equivalencia? ¿Cuál es el cardinal del conjunto cociente?

3) Sea $S \subset \mathbb{Z}$ un subconjunto no vacío que tiene las dos siguientes 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.

4) Sean a, b, m números naturales con a y b coprimos (primos entre sí).
Demuestra que *si* $a \mid m \wedge b \mid m$, entonces $ab \mid m$.
Encuentra un ejemplo que muestre que esto puede no ser cierto si a y b no son coprimos.

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

6) i) Probar la identidad $x^{2k+1} + 1 = (x+1)\sum_{j=0}^{2k}(-1)^j x^{2k-j}$. Utilizar esta identidad para probar 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*.

ii) Probar la identidad $x^n - 1 = (x-1)\sum_{j=0}^{n-1} x^j$. Utilizar esta identidad para probar que si $2^n - 1$ es primo entonces n es primo. Se denominan *primos de Mersenne* los de la forma $2^n - 1$.

7) 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.

8) (i) Teniendo en cuenta que $10 \equiv 1 \mod(9)$, prueba que $n \equiv s \mod(9)$ 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?

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

(iii) Si en vez de dígitos tuviésemos los *bits* del desarrollo de n en base 2, usa: $2 \equiv -1 \mod(3)$ 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.

(iii) Prueba que, para n, m dados, y si s_n, s_m son las respectivas sumas de sus dígitos, se cumple:

al es el inverso multiplicativo de cada uno de sus elementos. Haz lo mismo con $\mathcal{U}(\mathbb{Z}_8)$.

11) i) 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?

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

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

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

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

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

16) Escribe una sola congruencia que sea equivalente al sistema de congruencias: $x \equiv 1 \pmod{4}$, $x \equiv 2 \pmod{3}$ y $x \equiv 3 \pmod{7}$.

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

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

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

20) Demuestra los apartados a), b) y c) siguientes para concluir el teorema de Wilson:

Si p es primo, $(p-1)! \equiv -1 \pmod{p}$.

a) Demuestra que si p es primo, $(a,p) = 1$, existe una sola solución $\pmod{p}$ de la congruencia $ax \equiv 1 \pmod{p}$.

b) Demuestra que si $a \neq 1, p-1$, el x correspondiente en el apartado anterior es distinto de a.

c) Utilizando los apartados a) y b), demuestra que $2 \cdot 3 \cdots (p-3)(p-2) \equiv 1 \pmod{p}$.