CONJUNTOS Y NÚMEROS. Curso 2011-2012. **HOJA 4.**

1) Demuestra que hay infinitos enteros primos de la forma $4n-1$ y de la forma $6n-1$.

2) 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 $\alpha_i,\beta_i\in\mathbb{N}$. i) Expresa el $\mathrm{mcd}(a,b)$ y el $\mathrm{mcm}(a,b)$ en función de estas factorizaciones. ii) Demuestra que $ab=\mathrm{mcd}(a,b)\cdot\mathrm{mcm}(a,b)$. iii) Halla el máximo común divisor de 1547 y 3059 usando dos procedimientos: el descrito en i) y el algoritmo de Euclides.

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

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

5) Sea $S\subset\mathbb{Z}$ un subconjunto no vacío que cumple las 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) Sea $p\in\mathbb{Z}$, $(p\neq 0,-1,1)$. Suponer que p verifica la siguiente condición:

$$\forall a,b\in\mathbb{Z},\ p\mid ab \implies p\mid a \quad\vee\quad p\mid b.$$

Demuestra que p es primo.

7) Sean a,b,m números naturales con a y b coprimos entre sí. Demuestra que si $a\mid m$ y $b\mid m$ entonces $ab\mid m$. Encuentra un contraejemplo que muestre que si a y b no son coprimos entre sí el resultado no es cierto en general.

8) Demuestra que para todo $n\in\mathbb{N}$, $\sqrt{n}\in\mathbb{Q}\iff\sqrt{n}\in\mathbb{N}$.

9) Halla el conjunto de soluciones de las siguientes ecuaciones diofánticas:

a) $111x+36y=15$, b) $10x+26y=1224$, c) $6x+10y=20$.

10) 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.

11) 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.

12) (i) Teniendo en cuenta que $10\equiv 1\ \mathrm{mod}(9)$, prueba que $n\equiv s\ \mathrm{mod}(9)$ 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 $10\equiv -1\ \mathrm{mod}(11)$, 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: $2 \equiv -1 \bmod(3)$ 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.

13) Es habitual y más cómodo utilizar la notación $\mathbb{Z}_n$ para referirse a $\mathbb{Z}/n\mathbb{Z}$. Demuestra que

$$G : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \quad , \qquad G(\overline{k}, \overline{m}) = \overline{k+m}$$

y

$$H : \mathbb{Z}_n \times \mathbb{Z}_n \longrightarrow \mathbb{Z}_n \quad , \qquad H(\overline{k}, \overline{m}) = \overline{km}$$

están bien definidas como funciones. En otras palabras, que la imagen del par $(\overline{k}, \overline{m})$ es independiente de los representantes k y m elegidos. Probar también que G y H definen en $\mathbb{Z}_n$ una estructura de anillo.

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

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

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

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

16) 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 $\overline{a}^p + \overline{b}^p = (\overline{a} + \overline{b})^p$.

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

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

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

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

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

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

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

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

25) 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 $2 \cdot 3 \cdots (p-3)(p-2) \equiv 1 \pmod{p}$.