TEORÍA ALGEBRAICA DE NÚMEROS (7-10-2019 → 21-10-2019)	•	**Grado en Matemáticas** **Curso 2019–20**	**Hoja 1**

Ecuaciones diofánticas. Congruencias.

1. Demostrar $\boxed{\text{Lema}}$: Sea D un dominio de factorización única (DFU) y $a, b \in D$ primos entre si tales que existe $c \in D$ y $n \in \mathbb{N}$ cumpliéndose $ab = c^n$. Entonces existen $a_1, b_1 \in D$ y $u, v \in \mathcal{U}(D)$ (i.e. unidades de D) tales que $a = ua_1^n$ y $b = vb_1^n$.

2. Calcular todas las soluciones enteras de la ecuación de Pell: $C_d : x^2 - dy^2 = 1$ para $d < 0$.

3. Calcular las soluciones enteras y racionales de las siguiente cónicas:

$$C_1 : 2x^2 + 7y^2 = 11 \qquad \text{y} \qquad C_2 : 2x^2 + 8y^2 = 9.$$

4. Calcular las soluciones racionales de la cónica $C : 2x^2 - 7y^2 = 11$.

5. Encontrar condiciones para que un entero k no pueda ser la suma de tres cubos enteros.

6. Sea $c \in \mathbb{Z}$ tal que existen $a, b \in \mathbb{Q}$ cumpliendo $b^2 - a^3 = c$.

a) Demostrar que entonces $(A, B) = \left(\dfrac{a^4 - 8ca}{4b^2}, \dfrac{-a^6 - 20ca^3 + 8c^2}{8b^3} \right)$ satisface $B^2 - A^3 = c$.

b) Demostrar que el punto (A, B) es el punto corte de la curva plana $y^2 = x^3 + c$ con la recta tangente a dicha curva en el punto $(x, y) = (a, b)$.

7. Calcular las soluciones enteras de $y^2 - y = x^3$.

8. Calcular las soluciones enteras de $y^2 = x^3 + 16$.

9. Fijado un entero $k \in \mathbb{Z}$ definimos la ecuación diofántica $C_k : x^3 + y^3 = k$. Calcular $C_k(\mathbb{Z})$ para $|k| \leq 100$.

10. Definimos la ecuación diofántica $C : x^3 + y^3 = 7$.

a) Calcular $C(\mathbb{Z})$.

b) Demostrar $\#C(\mathbb{Q}) > 11$.

11. Calcular las soluciones enteras de $y^2 = x^5 - 1$.

12. (**Teorema de la congruencia lineal**) Sean $a, b \in \mathbb{Z}$ y $m \in \mathbb{N}$. Demostrar que la ecuación $ax \equiv b \pmod{m}$ tiene solución si y sólo si (a, m) divide a b. Demostrar que en dicho caso se tiene que hay exactamente (a, m) soluciones. Además si x_0 es una solución, entonces el resto de soluciones son de la form

$$x_k = x_0 + k\frac{m}{(a.m)}\,, \qquad k = 1, \ldots, (a, m) - 1.$$

13. Resolver la congruencias lineales:

a) $5\,x \equiv 3 \pmod{24}$. **b)** $25\,x \equiv 15 \pmod{120}$.

14. Sea p un primo y $f(x) = c_0 + c_1\,x + \cdots + c_n\,x^n \in \mathbb{Z}[x]$. Demostrar los siguientes resultados:

a) Teorema (Lagrange): Si $p \nmid c_n$, entonces la congruencia polinómica $f(x) \equiv 0 \pmod{p}$ tiene como mucho n soluciones.

b) Si $f(x) \equiv 0 \pmod{p}$ tiene más de n soluciones, entonces $c_i \equiv 0 \pmod{p}$, $i = 0, \ldots, n$.

c) Demostrar que el Teorema de Lagrange no es cierto si p no es primo.