TEORÍA ALGEBRAICA DE NÚMEROS (2-10-2018) • **Grado en Matemáticas** **Curso 2018–19** | **Hoja 2**

Congruencias. Residuos cuadráticos.

1. Resolver la congruencias lineales:
a) $5\,x \equiv 3 \,(\mathrm{mod}\, 24)$. **b)** $25\,x \equiv 15 \,(\mathrm{mod}\, 120)$.

2. Sea $f(x) \in \mathbb{Z}[x]$ y $n \in \mathbb{N}$, $n \geq 1$. Demostrar $\dfrac{f^{n)}(x)}{n!} \in \mathbb{Z}[x]$.

3. 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 $p \not| c_n$, entonces la congruencia polinómica $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ tiene como mucho n soluciones.
b) Si $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ tiene más de n soluciones, entonces $c_i \equiv 0 \,(\mathrm{mod}\, p)$, $i = 0, \ldots, n$.
c) Demostrar que el Teorema de Lagrange no es cierto si p no es primo.

4. Probar que $5\,n^3 + 7\,n^5 \equiv 0 \,(\mathrm{mod}\, 12)$, para todo entero n.

5. Encontrar todos los enteros positivos n para los que:
a) $n^{13} \equiv n \,(\mathrm{mod}\, 1365)$, **b)** $n^{17} \equiv n \,(\mathrm{mod}\, 4080)$.

6. Sea p un primo. El conjunto de los enteros p-ádicos se define como:

$$\mathbb{Z}_p = \{(a_1, a_2\,\ldots) \,:\, a_{n+1} \equiv a_n \pmod{p^n},\ n = 1, \ldots\}.$$

Demostrar:
a) $\mathbb{Z}_p$ es un anillos con las operaciones suma y producto termino a termino.
b) $\sqrt{2} \in \mathbb{Z}_7$.
c) $\frac{1}{2} \in \mathbb{Z}_p$, si $p \neq 2$.

7. Calcular:

$$\left(\frac{5}{3593}\right)\ ,\ \left(\frac{5}{3889}\right)\ ,\ \left(\frac{14}{137}\right)\ ,\ \left(\frac{55}{179}\right)\ ,\ \left(\frac{299}{397}\right)\ ,\ \left(\frac{37603}{48611}\right).$$

8. Demostrar que $\displaystyle\sum_{a=1}^{p-1}\left(\frac{a}{p}\right) = 0$ para cualquier primo impar p.

9. **a)** Sea q un primo impar tal que $q \equiv 1 \,(\mathrm{mod}\, 4)$, entonces q es un residuo cuadrático módulo p si y sólo si $p \equiv r \,(\mathrm{mod}\, q)$, donde r es un residuo cuadrático módulo q.
b) Calcular $\left(\frac{5}{p}\right)$.

10. Sea p un primo, demostrar que el número de soluciones de

$$x^2 + y^2 \equiv 1 \,(\mathrm{mod}\, p),$$

con $0 \leq x, y < p$, es par.

11. El Símbolo de Jacobi

Sea m un entero positivo impar. Podemos escribir $m = p_1 \dots p_s$ donde p_i son primos impares, no necesariamente distintos. Se define el símbolo de Jacobi como:

$$\left(\frac{a}{m}\right) = \prod_{i=1}^{s} \left(\frac{a}{p_i}\right).$$

Si m y m' son enteros positivos impares, demostrar:

a) $\left(\frac{a}{m\,m'}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$.

b) $\left(\frac{a\,a'}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right)$.

c) $\left(\frac{a}{m}\right) = \left(\frac{a'}{m}\right)$ si $a \equiv a' \pmod{m}$.

12. Si m es un entero positivo impar, demostrar:

a) $\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}$.

b) $\left(\frac{2}{m}\right) = (-1)^{(m^2-1)/8}$.

13. Ley de reciprocidad cuadrática para el símbolo de Jacobi

Sean m y n enteros positivos impares tales que $(m, n) = 1$. Demostrar

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}.$$

El símbolo de Jacobi se puede generalizar aún mas, y es lo que se llama el **Símbolo de Kronecker**. Sea $a = (-1)^n b$ y b, n enteros positivos, definimos

$$\left(\frac{a}{-1}\right) = (-1)^n = \text{signo}(a) \qquad \text{y} \qquad \left(\frac{a}{2}\right) = \begin{cases} 0 & \text{si } a \equiv 0 \pmod{2}, \\ \left(\frac{2}{a}\right) & \text{si } a \equiv 1 \pmod{2}. \end{cases}$$

Así para un entero cualquiera $n = (-1)^r 2^c\, m$ con $(2, m) = 1$ definimos

$$\left(\frac{a}{n}\right) = (-1)^r \left(\frac{a}{2}\right)^c \left(\frac{a}{m}\right)$$

donde $\left(\frac{a}{2}\right)$ se define como antes, y $\left(\frac{a}{m}\right)$ es el símbolo de Jacobi.

14. Si p es un primo impar, demostrar que el menor entero positivo que no es residuo cuadrático es menor que $\sqrt{p} + 1$.

15. Demostrar que $x^4 \equiv 25 \pmod{1013}$ no tiene solución.

16. Demostrar que $x^4 \equiv 25 \pmod{p}$ no tiene solución si p es un primo congruente a 13 ó 17 $\pmod{20}$.

17. Si p es un primo congruente a 13 ó 17 $\pmod{20}$, demostrar que $x^4 + p\,y^4 = 25\,z^4$ no tiene soluciones enteras no triviales.