TEORÍA ALGEBRAICA DE NÚMEROS (16-10-2019)	•	Grado en Matemáticas Curso 2019–20	Hoja 3

Residuos cuadráticos.

1. Calcular:

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

2. Demostrar que 5 no es un residuo cuadrático para los primos de la forma $p = 6^n + 1$.

3. Calcular $\left(\frac{5}{p}\right)$.

4. Demostrar que si $n > 1$ es un entero, entonces $N = \sum_{k=1}^{n} k!$ no es un cuadrado.

5. Demostrar que el primo 9239 divide a $2^{4619} - 1$.

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

$$x^2 + y^2 \equiv 1 \pmod{p},$$

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

7. Determinar las condiciones que debe de satisfacer un primo impar p para que -7 sea residuo cuadrático módulo p.

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

9. Sea q un primo tal que $p = 2q + 1$ es un primo de la forma $8k + 3$. Calcular $\left(\frac{q}{p}\right)$.

10. Sea $M_p > 3$ un primo de Mersenne. Calcular $\left(\frac{3}{M_p}\right)$.

11. Sea p un primo impar. Demostrar

$$\sum_{k=1}^{p-2} \left(\frac{k(k+1)}{p}\right) = -1.$$

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

13. Sea p un primo de la forma $13 + 20k$ o $17 + 20k$. Demostrar que las siguiente ecuaciones no tienen solución:

a) $x^4 \equiv 25 \pmod{p}$.

b) $x^4 + p\,y^4 = 25\,z^4$.

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

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

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

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

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

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

16. 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

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

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