Introducción a la Teoría de Números
Curso 2012

Lista 4. Reciprocidad cuadrática – entrega 12/10

1. Calcular a mano: $\left(\frac{3}{97}\right)$, $\left(\frac{3}{389}\right)$, $\left(\frac{22}{11}\right)$ y $\left(\frac{5!}{7}\right)$.
2. Encontrar $x \in \mathbb{N}$ tal que $x^2 \equiv 69 \pmod{389}$.
3. Encontrar el natural $x < 97$ tal que $x \equiv 4^{48} \pmod{97}$ (notar que 97 es primo).
4. ¿Cuántos números naturales $x < 2^{13}$ satisfacen la ecuación
$$x^2 \equiv 5 \pmod{2^{13}-1}?$$
Asumir que $2^{13}-1$ es primo.
5. Encontrar todas las soluciones a las siguientes ecuaciones cuadráticas
   (a) $19x^2 + 1783x + 29485 \equiv 0 \pmod{29527}$.
   (b) $x^2 + 2^{87} \equiv 0 \pmod{2^{89}-1}$.
   (c) $x^2 + 2^{47} \equiv 0 \pmod{2^{53}+5}$.
6. Usar la Ley de Reciprocidad Cuadrática para mostrar que, para todo primo $p \geq 5$,
$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1, 11 \pmod{12}, \\ -1 & \text{si } p \equiv 5, 7 \pmod{12}. \end{cases}$$
7. Usar que la existencia de raíces primitivas módulo un primo p para dar una demostración directa de que $\left(\frac{-3}{p}\right) = 1$ cuando $p \equiv 1 \pmod{3}$. (Sugerencia: mostrar que en tal caso hay un $c \in \mathbb{Z}$ de orden 3 módulo p, y ver que $(2c+1)^2 \equiv -3 \pmod{p}$.)
8. Mostrar que $\left(\frac{5}{p}\right) = 1$ cuando $p \equiv 1 \pmod{5}$ por el método del egercicio anterior. (Sugerencia: si c tiene orden 5 módulo p, entonces $(c+c^4)^2+(c+c^4)-1 \equiv 0 \pmod{5}$.)
9. Probar que para $n \in \mathbb{Z}$, el entero n^2+n+1 no tiene ningún divisor de la forma $6k-1$.
10. Usar la Ley de Reciprocidad Cuadrática para determinar los primos para los cuales 7 es un residuo cuadrático. Hacer lo mismo para 15.
11. Suponer que $p \equiv 3 \pmod{4}$ y que $q = 2p+1$ también es primo. Probar que $2^p - 1$ no es primo. (Sugerencia: usar el carácter cuadrático de 2 para mostrar que $q \mid 2^p - 1$.) Hay que asumir que $p > 3$.
12. Sea $\zeta = e^{2\pi i/8}$ una raiz octava primitiva de la unidad, y sea $\tau = \zeta + \zeta^{-1}$.
    (a) Mostrar que $\tau^2 = 2$ y concluir que, si p es un primo impar, $\tau^p \equiv \left(\frac{2}{p}\right)\tau \pmod{p}$.
    (b) Usar que $\zeta^8 = 1$ y que $\zeta^4 = -1$ para ver que
$$\zeta^p + \zeta^{-p} = \begin{cases} \tau, & \text{si } p \equiv \pm 1 \pmod{8}, \\ -\tau, & \text{si } p \equiv \pm 3 \pmod{8}. \end{cases}$$
    (c) Deducir la fórmula complementaria para $\left(\frac{2}{p}\right)$.