TEORÍA DE NÚMEROS – TAREA 3

PARA ENTREGAR EL JUEVES 14 DE FEBRERO

1. *a*) Encuentra una raíz primitiva módulo p para $p = 5, 7, 11, 29$.
   b) Sea g una raíz primitiva módulo p, p primo. Muestra que g^a es una raíz primitiva módulo p si y sólo si $\text{mcd}(a, p-1) = 1$.
   c) ¿Cuántas raíces primitivas módulo p hay?
2. Prueba el teorema de Wilson: Si p es primo, entonces $(p-1)! \equiv -1 \pmod{p}$. (**Sugerencia:** Usa una raíz primitiva.)
3. Sea $p > 3$ primo. Sea R (resp. N) un conjunto completo de residuos cuadráticos (resp. no-residuos) módulo p.
   a) Muestra que
   $$\prod_{r \in R} r \equiv -\prod_{n \in N} n \equiv (-1)^{(p+1)/2} \pmod{p}.$$
   b) Muestra que
   $$\sum_{r \in R} r \equiv \sum_{n \in N} n \equiv 0 \pmod{p}.$$
   (**Sugerencia:** Usa una raíz primitiva.)
4. *a*) Muestra que la sucesión $n^5 - n + 3$ no contiene ningún cuadrado. (**Sugerencia:** reduce módulo 5).
   b) Sea $p \equiv 3, 5 \pmod{8}$. Muestra que la sucesión $n! + n^p - n + 2$ contiene a lo más una cantidad finita de cuadrados.
5. Decide si 219 es un residuo cuadrático módulo 383 y 143. (Ten cuidado).
6. Di para qué primos p se tiene que 5 es un residuo cuadrático. Lo mismo para 3.
7. Supón que p, q son primos tales que $p = 2q + 1$.
   a) Muestra que si $q \equiv 1 \pmod{4}$, entonces 2 es una raíz primitiva módulo p.
   b) ¿Bajo qué condiciones en q se tiene que 5 es una raíz primitiva módulo p?
8. Demuestra que $y^2 = x^3 + 7$ no tiene soluciones enteras. (**Sugerencia:** Suma uno a cada lado de la ecuación.)