Introducción a la Teoría de Números
Lista de ejercicios final, 2010

Instrucciones. Justificar todas las respuestas. *No está permitido discutir los problemas con nadie.* Se puede usar material como libros, notas de curso, páginas web, dando referencias precisas a cualquier resultado que se use. Se puede usar una computadora, en cuyo caso tiene que quedar claro qué programa se usa y qué cuentas hace la computadora.

Hay que entregar *exactamente* 3 problemas de los 4 planteados.

Calificación. El puntaje máximo es 60 puntos (20 puntos por problema). Para aprobar el curso se requiere un mínimo de 30 puntos. Obteniendo 35 puntos o más se exonera la parte práctica del examen y el puntaje obtenido se considerará como nota de práctico. La exoneración tendrá validez sólo por los períodos de examen de diciembre 2010 y de febrero-marzo 2011, y podrá ser utilizada *solamente una vez* para rendir examen.

Entrega. La fecha límite para la entrega es el martes 30 de noviembre a las 17:00, *sin excepciones*.

1. En este problema se resuelve la ecuación $x^2 + y^2 = z^2$ con $x, y, z \in \mathbb{Z}$ relativamente primos dos a dos.
   (a) Mostrar que x, y no pueden ser ambos impares.
   (b) Suponer x par, y, z impares, y concluir que
   $$\left(\frac{x}{2}\right)^2 = \frac{(z+y)}{2} \cdot \frac{(z-y)}{2}.$$
   (c) Si $u, v \in \mathbb{Z}$ son tales que uv es un cuadrado perfecto y son relativamente primos, entonces u y v son cuadrados perfectos.
   (d) Concluir que $x = 2ab$, $y = b^2 - a^2$, $z = b^2 + a^2$, donde $a, b \in \mathbb{Z}$ son relativamente primos y tienen distinta paridad.
2. Sea n un entero impar positivo, factorizado como $n = \prod_{i=1}^{k} p_i^{e_i}$. Se define el *símbolo de Jacobi* $\left(\frac{a}{n}\right)$ de la siguiente forma:
   $$\left(\frac{a}{n}\right) = \prod_{i=1}^{k} \left(\frac{a}{p_i}\right)^{e_i}.$$
   (a) Dar un ejemplo que muestre que $\left(\frac{a}{n}\right) = 1$ no necesariamente implica que a es un cuadrado módulo n.
   (b) Si a y b son enteros, entonces
   $$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$
   (c) $\left(\frac{-1}{n}\right) = 1$ si y solo si $n \equiv 1 \pmod 4$.
   (d) $\left(\frac{2}{n}\right) = 1$ si y solo si $n \equiv \pm 1 \pmod 8$.
   (e) Si a es impar y positivo, entonces
   $$\left(\frac{a}{n}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}} \left(\frac{n}{a}\right).$$

3. Sea p un primo y $a \in \mathbb{Z}$.

   (a) Mostrar que el número de soluciones de la ecuación $x^2 - y^2 \equiv a \pmod{p}$ está dado por
   $$\sum_{y=0}^{p-1} \left(1 + \left(\frac{y^2 + a}{p}\right)\right).$$

   (b) Calcular directamente el número de soluciones de la ecuación $x^2 - y^2 \equiv a \pmod{p}$, mostrando que es $p - 1$ si $p \nmid a$ y $2p - 1$ si $p \mid a$.

   (c) Concluir que
   $$\sum_{y=0}^{p-1} \left(\frac{y^2 + a}{p}\right) = \begin{cases} -1 & \text{si } p \nmid a, \\ p - 1 & \text{si } p \mid a. \end{cases}$$

   (d) Evaluar la suma
   $$\sum_{n=1}^{p-1} \left(\frac{n(n+1)}{p}\right),$$
   donde p es un primo impar.

4. En este problema se busca mostrar el siguiente resultado de Fermat: los únicos puntos con coordenadas enteras en la curva elíptica $E : y^2 = x^3 - 2$ son $(3, \pm 5)$. Hay que usar el siguiente

   Lema. Si m es impar, entonces $m = x^2 + 2y^2$ y $m^3 = x^2 + 2y^2$ tienen el mismo número de representaciones propias (es decir con x e y coprimos);

   que vale porque la clase de $x^2 + 2y^2$ es la única clase discriminante -8. NO demostrar el Lema.

   (a) Verificar el Lema para $m = 3$ enumerando todas las representaciones de m y de m^3 y contando cuáles son propias.

   (b) Si $m = a^2 + 2b^2$ es una representación propia de m, entonces
   $$m^3 = (a^3 - 6ab^2)^2 + 2(3a^2b - 2b^3)^2$$
   es una representación propia de m^3.

   (c) Mostrar que el mapa que manda (a, b) en $(a^3 - 6ab^2, 3a^2b - 2b^3)$ es inyectivo. Sugerencia: notar que
   $$(a + b\sqrt{-2})^3 = (a^3 - 6ab^2) + (3a^2b - 2b^3)\sqrt{-2}.$$

   (d) Deducir, por el Lema, que las representaciones propias de $m^3 = x^2 + 2y^2$ son todas como en (b).

   (e) Mostrar que si (m, n) es un punto de coordenadas enteras en $E(\mathbb{Q})$ entonces m es impar y $m^3 = n^2 + 2 \cdot 1^2$ es una representación propia de m^3.

   (f) Concluir que $(3, \pm 5)$ es la única solución con coordenadas enteras.