Introducción a la Teoría de Números
Lista de ejercicios final, 2008

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* 4 problemas de los 5 planteados.

Calificación. El puntaje máximo es 80 puntos (20 puntos por problema). Obteniendo un mínimo de 50 puntos se exonera el examen práctico y el puntaje obtenido se considerará como nota de práctico. Dicha exoneración tendrá validez sólo por los períodos de diciembre 2008 y de febrero-marzo 2009, y podrá ser utilizada solamente una vez para rendir examen.

Entrega. La fecha límite para la entrega es el miércoles 26 de noviembre a las 10:00, al comienzo de la clase, *sin excepciones*.

Página del curso. `http://www.cmat.edu.uy/~tornaria/2008/TN/`

1. Sea p un primo, y sea $f(x)$ un polinomio mónico de grado $d < p$. En este problema se trata de probar que la congruencia $f(x) \not\equiv 0 \pmod{p}$ tiene solución. Denotamos

$$\Delta f(x) := f(x+1) - f(x).$$

   (a) Para $k \geq 1$, mostrar que $\Delta^k f(x)$ es una combinación lineal con coeficientes enteros de $f(x), f(x+1), \ldots, f(x+k)$.
   (b) Mostrar que $\Delta^d f(x) = d!$.
   (c) Concluir que en cualquier conjunto de $d+1$ enteros consecutivos, al menos uno de ellos es solución de $f(x) \not\equiv 0 \pmod{p}$.
   (d) Dar un ejemplo de un polinomio mónico $f(x)$ de grado p con coeficientes enteros, tal que $f(x) \equiv 0 \pmod{p}$ para todo $x \in \mathbb{Z}$.

2. 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.

3. Supongamos que $x^4 + y^4 = w^2$ tiene solución en enteros positivos, y sea x, y, w una tal solución con w el mínimo posible.

   (a) Asumiendo que x es impar, usar $(2d)$ para mostrar que
   $$x^2 = m^2 - n^2, \qquad y^2 = 2mn, \qquad w = m^2 + n^2,$$
   con m y n enteros positivos relativamente primos de distinta paridad.

   (b) Mostrar que
   $$x = r^2 - s^2, \qquad n = 2rs, \qquad m = r^2 + s^2,$$
   con r y s enteros positivos relativamente primos de distinta paridad.

   (c) Usar $(2c)$ para probar que r, s, m son todos cuadrados perfectos, digamos a^2, b^2, c^2.

   (d) Mostrar que $a^4 + b^4 = c^2$, y que esto contradice la minimalidad de w.

   Concluir que $x^4 + y^4 = z^4$ no tiene solución en enteros positivos.

4. Sea $D > 0$ un discriminante positivo, no cuadrado perfecto.

   (a) Mostrar que cualquier forma cuadrática de discriminante D es equivalente a una forma (a, b, c) con
   $$|b| \leq |a| \leq |c|.$$
   Sugerencia: entre todas las formas equivalentes a la dada, considerar una con $|b|$ mínimo. Los coeficientes a y c son no nulos pues D no es un cuadrado perfecto.

   (b) Si (a, b, c) satisface las desigualdades de la parte anterior, mostrar que
   $$|a| \leq \frac{\sqrt{D}}{2}.$$

   (c) Concluir que $h(D)$, el número de clases de equivalencia de formas cuadráticas de discriminante D, es finito.

   (d) Mostrar que $h(8) \leq 2$. [De hecho, $h(8) = 1$.]

5. El propósito de este problema es mostrar que $\left(\frac{-2}{p}\right) = 1$ cuando $p \equiv 1, 3 \pmod 8$.

   (a) Cuando $p \equiv 1 \pmod 8$, escribir $p = 8k + 1$ y usar la identidad
   $$x^{8k} - 1 = ((x^{2k} - 1)^2 + 2x^{2k})(x^{4k} - 1)$$
   para mostrar que $\left(\frac{-2}{p}\right) = 1$.

   (b) Cuando $p \equiv 3 \pmod 8$, asumir que $\left(\frac{-2}{p}\right) = -1$. Concluir que $\left(\frac{8}{p}\right) = 1$ y por lo tanto p es representado por una forma de discriminante 8.

   (c) Mostrar que toda forma de discriminante 8 es equivalente a $\pm(x^2 - 2y^2)$. Sugerencia: ver (4d).

   (d) Mostrar que un primo impar $p = \pm(x^2 - 2y^2)$ debe ser congruente con $\pm 1 \bmod 8$.

   Concluir que si $p \equiv 1, 3 \pmod 8$ entonces $\left(\frac{-2}{p}\right) = 1$.