Introducción a la Teoría de Números
Lista de ejercicios final, 2006

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 6 problemas, cada uno inspirado en la lista de ejercicios correspondiente. Hay que entregar *exactamente* 4 problemas. Se sugiere entregar 2 problemas de 20 puntos y 2 problemas de 30, pero se aceptarán otras combinaciones (tener en cuenta que en algunas combinaciones no es posible llegar al máximo puntaje).

Calificación. El puntaje máximo es 100 puntos. Obteniendo un mínimo de 50 puntos se exonera el examen práctico por dos períodos (diciembre y febrero), y el puntaje obtenido se considerará como nota de práctico.

Entrega. La fecha límite para la entrega es el miércoles 6 de diciembre a las 10:30 en mi oficina (piso 14) *sin excepciones.*

Página del curso. `http://www.cmat.edu.uy/~tornaria/2006/TN/`

1. (20 puntos) La sucesión de Fibonacci F_n se define de la siguiente manera: $F_0 = 0$, $F_1 = 1$, y para $n \geq 2$, $F_n = F_{n-1} + F_{n-2}$. Probar que para todo $n \geq 0$ el máximo común divisor entre F_n y F_{n+1} es 1.

2. (30 puntos) Si p es un primo impar, entonces existe una raíz primitiva módulo p^n:

   (a) Mostrar que existe una raíz primitiva g módulo p tal que $g^{p-1} \not\equiv 1 \pmod{p^2}$. (Asumir la existencia de una raíz primitiva módulo p.)

   (b) Probar que $(1 + ap)^{p^{n-2}} \equiv 1 + ap^{n-1} \pmod{p^n}$ si $n \geq 2$.

   (c) Si $p \nmid a$, entonces $1 + ap$ tiene orden p^{n-1} módulo p^n.

   (d) Concluir que g como en la parte (a) es una raíz primitiva módulo p^n.

3. (20 puntos) Factorizar $n = 6979530194492209$ usando el método de Fermat.

4. (30 puntos) Sea p un primo impar. En este ejercicio se trata de probar que $\left(\frac{2}{p}\right) = 1$ si y solo si $p \equiv \pm 1 \pmod 8$:

   (a) Mostrar que
   $$x = \frac{1 - t^2}{1 + t^2}, \quad y = \frac{2t}{1 + t^2}$$
   es una parametrización del conjunto de soluciones de $x^2 + y^2 \equiv 1 \pmod p$. Es decir que las soluciones $(x, y) \in \mathbb{Z}/p \times \mathbb{Z}/p$ están en biyección con los $t \in \mathbb{Z}/p \cup \{\infty\}$ tales que $1 + t^2 \not\equiv 0 \pmod p$. Aquí $t = \infty$ corresponde a la solución $(-1, 0)$. (Sugerencia: si (x_1, y_1) es una solución, considerar la recta $y = t(x + 1)$ que pasa por (x_1, y_1) y por $(-1, 0)$, y calcular x_1, y_1 en función de t.)

(b) Probar que el número de soluciones de $x^2 + y^2 \equiv 1 \pmod p$ es $p+1$ si $p \equiv 3 \pmod 4$ y $p-1$ si $p \equiv 1 \pmod 4$.

(c) Sea S el conjunto de pares $(a,b) \in \mathbb{Z}/p \times \mathbb{Z}/p$ tales que $a+b=1$ y $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. Mostrar que $\#S = \frac{p+1-4}{4}$ si $p \equiv 3 \pmod 4$ y $\#S = \frac{p-1-4}{4}$ si $p \equiv 1 \pmod 4$. Concluir que $\#S$ es impar si y solo si $p \equiv \pm 1 \pmod 8$.

(d) El mapa $\sigma(a,b) = (b,a)$ que intercambia coordenadas es una biyección del conjunto S en si mismo. Mostrar que son equivalentes

i. σ tiene exactamente un punto fijo,

ii. existe $a \in \mathbb{Z}$ tal que $2a \equiv 1 \pmod p$ y $\left(\frac{a}{p}\right) = 1$,

iii. $\left(\frac{2}{p}\right) = 1$.

(e) Concluir mostrando que σ tiene exactamente un punto fijo si y solo si $\#S$ es impar.

5. (20 puntos) Usando fracciones continuas, encontrar un número racional $x \approx 25.352941...$.

6. (30 puntos) 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 (o lo que es lo mismo, porque el anillo $\mathbb{Z}[\sqrt{-2}]$ tiene factorización única). 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.