Formas Cuadráticas - Práctica 1

2do. Cuatrimestre 2008

Cuerpos cuadráticos imaginarios y formas binarias

1. Usando la recíprocidad cuadrática para el símbolo de Kronecker, probar la fórmula de reciprocidad de Jacobi. Esto es si $m \in \mathbb{N}$ es impar, entonces:
   - $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}$.
   - $\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}}$.
   - Si $m, n \in \mathbb{N}$ son impares, entonces
   $$\left(\frac{n}{m}\right) = \left(\frac{m}{n}\right)(-1)^{\frac{n-1}{2}\frac{m-1}{2}}.$$

2. Sea $D \equiv 0 \pmod 4$ y negativo, digamos $D = -4n$. En este ejercicio probaremos que $h(D) > 1$ si $n \neq 1, 2, 3, 4, 7$. Para esto consideramos los casos:
   - Si $n = pq$, con $p \neq 1 \neq q$ y $\gcd(p, q) = 1$, construir una forma reducida que no sea principal. Luego, si $h(-4n) = 1$, $n = p^r$.
   - Si $n = 2^s$, con $s \geq 4$, construir una forma reducida no principal (sugerencia: tomar $a = 4$). Calcular $h(-4), h(-8), h(-16)$ y $h(-32)$ y comprobar que los tres primeros son 1 y el último es 2.
   - Si $n = p^r$ con $p \neq 2$, y $n + 1$ no es una potencia de un primo (como en el primer ítem) entonces hay una forma reducida no principal.
   - Deducir del ítem anterior que si $h(-4n) = 1$ y $n \neq 2^r$, $n = p^r$ y $n + 1 = 2^s$. Si $s \geq 6$, construir una forma (con $a = 8$) reducida no principal.
   - Estudiar los finitos casos restantes para concluir el resultado.

3. En este ejercicio miraremos órdenes en cuerpos cuadráticos que no son el orden maximal. Sea $K = \mathbb{Q}[\sqrt{D}]$ un cuerpo cuadrático imaginario.
   - Probar que si $\mathcal{O}$ es un órden en K (o sea un $\mathbb{Z}$-módulo de rango 2 que es un anillo), entonces existe $f \in \mathbb{N}$ (llamado el *conductor*) tal que $\mathcal{O} = \mathbb{Z} + f\mathcal{O}_K$, donde $\mathcal{O}_K$ denota el anillo de enteros de K.
   - Si $D \equiv 0, 1 \pmod 4$, $D < 0$, miremos $\mathcal{O}_D = \mathbb{Z} + \mathbb{Z}\frac{D+\sqrt{D}}{2}$. Si $\mathfrak{a} \subset \mathcal{O}_D$, es un $\mathbb{Z}$-módulo de rango 2, probar que existe una base de la forma
   $$\mathfrak{a} = \left\langle a, \frac{b + c\sqrt{D}}{2} \right\rangle, \quad \text{con } a, b, c \in \mathbb{Z}.$$

- Si $\mathfrak{a} \subset \mathcal{O}_D$ es un ideal para $\mathcal{O}_D$, probar que $c \mid a$ y $c \mid b$ (sugerencia: usar lo visto en clase que si τ es un elemento del semiplano superior de discriminante d, o sea el minimal de τ en $\mathbb{Z}[x]$ tiene discriminante d, entonces $\langle 1, \tau \rangle$ es un $\mathcal{O}_d$-ideal). Luego, si $c = \pm 1$ decimos que el ideal es primitivo (y se corresponde con una forma primitiva) y si $c \neq \pm 1$, el ideal es un múltiplo de un ideal primitivo.

4. Continuamos con el estudio de ideales para $\mathcal{O}_D$ como en el ejercicio anterior:

   - Un ideal (fraccionario) para $\mathcal{O}$ es un conjunto $\mathfrak{a} \subset K$ tal que

     $$\mathcal{O} = \{\alpha \in K \ : \ \alpha\mathfrak{a} \subset \mathfrak{a}\}.$$

     Probar que si $\mathfrak{a} \subset \mathcal{O}_D$ es un ideal para $\mathcal{O}_D$, entonces es inversible (sugerencia: usando el ítem anterior, ¿quién es el inverso?). Deducir que los ideales fraccionarios para $\mathcal{O}_D$ formas un grupo.
   - Probar que si $\mathfrak{a}, \mathfrak{b}$ son ideales para $\mathcal{O}$, el producto $\mathfrak{ab}$ también es un ideal para $\mathcal{O}$. Luego el conjunto de ideales fraccionarios para $\mathcal{O}$ es un grupo.
   - Verificar (usando el ejercicio 6 de la entrega final de Teoría de Números) que el conjunto de ideales de norma coprima con f (el conductor del ítem anterior) tiene factorización única.

5. Veamos que si $p \mid f$ entonces el ideal $p\mathcal{O}_D$ no tiene factorización en primos. Comencemos con el caso p impar.

   - Probar que un ideal de norma p tiene base $\left\langle p, \frac{b+\sqrt{D}}{2} \right\rangle$ para algún b divisible por p.
   - Probar que un tal $\mathbb{Z}$-módulo de rango 2 no es un ideal para $\mathcal{O}_D$. Luego no hay ideales de norma p.
   - Probar que el ideal $p\mathcal{O}_D$ no es primo. (Sugerencia: hallar un par de elementos tales que su producto esté en $p\mathcal{O}_D$ pero ninguno de ellos lo esté).

6. Veamos el caso $p = 2$.

   - Probar que los discriminantes fundamentales (i.e. que corresponden al anillo de enteros de un cuerpo) son $D < 0$ tales que:
     - D es libre de cuadrados y $D \equiv 1 \pmod 4$.
     - $4 \mid D$, $D/4$ es libre de cuadrados y $D/4 \equiv 3 \pmod 4$.
     - $4 \mid D$, $D/4$ es libre de cuadrados y $D \equiv 8 \pmod 1)6$.
   - De manera similar al ejercicio anterior, probar que si D no es fundamental, no hay un ideal primo de norma 2.
   - Probar que $2\mathcal{O}_D$ no es un ideal primo para $\mathcal{O}_D$ si D es par.

- Deducir que 2 no se escribe como producto de primos.

7. Veamos una aplicación de los últimos dos ejercicios a formas cadráticas binarias: probar que si D es un discriminante fundamental, entonces todos los primos $p \mid D$ se representan de forma propia por alguna forma cuadrática binaria de discriminante D. Más aún, probar que si $m \in \mathbb{N}$ es coprimo con D, entonces m se representa si y sólo si pm se representa. ¿Qué pasa si D no es fundamental?