Resumen de algunas relaciones

1 Reciprocidad cuadrática

El objetivo de esta parte será describir, dado un entero D, el conjunto de números primos que son representados por alguna forma cuadrática de discriminante D. El primer paso en esta dirección se resume de la siguiente manera.

Observación 1.1. Sea $D \in \mathbb{Z}$, $D \equiv 0, 1 \pmod{4}$ y sea p un primo (positivo) impar. Las afirmaciones siguientes son equivalentes:

(a) existe una forma cuadrática de discriminante D que representa p;

(b) la congruencia $x^2 \equiv D \pmod{p}$ admite una solución.

El siguiente resultado importante, es la Ley de Reciprocidad cuadrática.

Lema 1.2. *Sean p y q primos (positivos) impares, distintos. Entonces, la congruencia $x^2 \equiv q \pmod{p}$ tiene solución, si y sólo si la congruencia $x^2 \equiv p \pmod{q}$ tiene solución, salvo que $p \equiv q \equiv 3 \pmod{4}$, en cuyo caso, exactamente una de las dos congruencias tiene solución.*

En este contexto, podemos entender Reciprocidad como un lema técnico clave para probar el resultado definitivo.

Teorema 1.3. *Sea a un entero no cuadrado. Entonces, existe un morfismo sobreyectivo de grupos $\chi : U(4a) \to \{\pm 1\}$ con la siguiente propiedad: si p es un primo (positivo) impar que no divide a a, entonces la congruencia $x^2 \equiv a \pmod{p}$ tiene solución, si y sólo si $\chi(p) = 1$.*

Una de las características más importantes del Teorema 1.3 (o, mejor dicho, de la existencia de χ) es que la condición sobre el primo p de que $x^2 \equiv a \pmod{p}$ admita una solución se puede expresar como una condición sobre la clase de congruencia de p módulo $4a$. Es decir, dados p y p' primos positivos impares que no dividen a a, si $p \equiv p' \pmod{4a}$, entonces $x^2 \equiv a \pmod{p}$ tiene solución, si y sólo si $x^2 \equiv a \pmod{p'}$ tiene solución. Esto es así, porque, si $p \equiv p'$, entonces $\chi(p) = \chi(p')$.

2 Composición de formas cuadráticas

En esta parte, veremos que el conjunto de clases de formas cuadráticas posee estructura adicional.

Teorema 2.1. *Sea* $D \equiv 0, 1 \, (\mathsf{mod}\, 4)$*,* $D \neq 0$*. El conjunto* $C(D)$ *de clases de equivalencia propia de formas cuadráticas binarias primitivas de discriminante* D *admite una estructura de grupo abeliano (finito) con la siguiente propiedad: si* $m_1, m_2 \in \mathbb{Z}$ *son representados por clases* $C_1, C_2 \in C(D)$*, respectivamente, entonces el producto* $m_1 m_2$ *es representado por el producto de las clases,* $C_1 C_2$*.*

Por otro lado, si $D \equiv 0, 1 \, (\mathsf{mod}\, D)$, $D \neq 0$, el subconjunto de $U(D)$ conformado por aquellas clases de congruencia módulo D que están representadas por formas de discriminante D constituye un subgrupo. Precisamente, dicho subgrupo es $\mathsf{ker}(\chi_D) < U(D)$. El Teorema 2.1 sugiere que existe una relación entre el ahora *grupo de clases* $C(D)$ y el subgrupo $\mathsf{ker}(\chi_D)$.

Por *otro* lado, dos formas primitivas de discriminante D pertenecen al mismo género, si representan enteros en una misma clase de congruencia módulo D. Dicho de otra manera, si f y g son formas primitivas que *no pertenecen* al mismo género, entonces, ningún entero representado por f es congruente módulo D con un entero representado por g. Esta observación nos permite asignarle inequívocamente, a cada clase de congruencia módulo D repersentable, el género de formas (primitivas) que la representan.

El siguiente diagrama sintetiza el estado de situación:

$$\begin{array}{ccccc} & & \mathsf{ker}(\chi_D) & \longrightarrow & U(D) \xrightarrow{\chi_D} \{\pm 1\} \\ & & \downarrow & & \\ C(D) & \longrightarrow & \{\text{géneros}\} & & \end{array} .$$

En particular, si cada género de formas primitivas de discriminante D está compuesto por una única clase propia, entonces podemos decidir, dado un primo (impar, que no divide a D), si es representable por formas primitivas de discriminante D y, en tal caso, exactamente qué formas lo representan, mirando solamente su clase de congruencia módulo D.