# 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 $\chi$) 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 Géneros

Dado $D \equiv 0, 1 \,(\mathsf{mod}\, 4)$, $D \neq 0$, un entero $m$ (impar, coprimo con $D$) está representado (primitivamente) por alguna forma cuadrática de discriminante $D$, si y sólo $D$ es un residuo cuadrático módulo $4m$. Si $m = p > 0$ es primo, entonces esto equivale también a que $\chi_D(p) = (D/p) = 1$.

**Observación 2.1.** Si $p$ es un primo positivo impar que no divide a $D$ y $p$ es representable por alguna forma cuadrática primitiva de discriminante $D$, entonces todo primo positivo impar $q \equiv p \,(\mathsf{mod}\, D)$ también es representable por alguna forma primitiva de discriminante $D$.

**Teorema 2.2** (Dirichlet)**.** *Dados números enteros coprimos $m$ y $D$, la sucesión*

$$m \;, \quad m + D \;, \quad m + 2D \;, \quad \ldots$$

*contiene infinitos números primos.*

En particular, el Teorema 2.2 implica que toda clase de congruencia $c \in U(D)$ contiene, al menos, un primo positivo impar. Esto tiene la siguiente consecuencia.

**Corolario 2.3.** *Si $c \in U(D)$ es tal que $\chi_D(c) = 1$, entonces $c$ es representable por alguna forma cuadrática (primitiva) de discriminante $D$.*

Teniendo en cuenta el Corolario 2.3 y la Observación 2.1, asociamos, a una forma $f$ de discriminante $D$, el subconjunto de clase de congruencia módulo $D$, coprimas con $D$,[1] representadas por $f$:

$$\mathsf{S}^*(f) \;=\; \big\{ c \in U(D) \;:\; c \text{ está representada por } f \big\} \;.$$

¿Es cierto que, si $c \in U(D)$ está representada por alguna forma (primitiva) de discriminante $D$, *entonces* $\chi_D(c) = 1$? La respuesta es que sí. En particular, dada una forma primitiva $f$ de discriminante $D$, el subconjunto $\mathsf{S}^*(f)$, en verdad, está contenido en

$$\mathsf{ker}(\chi_D) \;=\; \big\{ c \in U(D) \;:\; \chi_D(c) = 1 \big\} \;.$$

Fijado un discriminante $D$, para cada $m \in \mathbb{Z}$, podemos preguntarnos qué formas cuadráticas primitivas de discriminante $D$ lo representan. A cada entero le corresponderá un subconjunto de formas y, en realidad, un subconjunto de clases de formas. Este subconjunto podría ser vacío. De la misma manera, fijado $D$, a cada clase de congruencia $c \in U(D)$, le asociamos el subconjunto de aquellas clases de formas que la representan. Este subconjunto de formas constituye un *género de formas cuadráticas.*

**Teorema 2.4.** *Sea $D \equiv 0, 1 \,(\mathsf{mod}\, 4)$, $D \neq 0$ y sea $c \in U(D)$. Si dos formas primitivas $f$ y $g$ de discriminante $D$ representan $c$, entonces $\mathsf{S}^*(f) = \mathsf{S}^*(g)$.*

Es decir, los subconjuntos $\mathsf{S}^*(f)$ y $\mathsf{S}^*(g)$ son iguales o disjuntos.

[1] Si $m \equiv n \,(\mathsf{mod}\, D)$, entonces $(m, D) = (n, d)$. En particular, la noción de que una clase de congruencia módulo $D$ sea coprima con $D$ está bien definida.

## 3 Composición de formas cuadráticas

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

**Teorema 3.1.** *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 3.1 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:

$$\begin{tikzcd} & \mathsf{ker}(\chi_D) \arrow[r] \arrow[d] & U(D) \arrow[r, "\chi_D"] & \{\pm 1\} \\ C(D) \arrow[r] & \{\text{géneros}\} & & \end{tikzcd} .$$

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 $D$.