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 $\chi : U\big(4a\big) \to \{\pm 1\}$ 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 $\chi(p) = \chi(p')$.