Rev.R.Acad.Cienc.Exact.Fis.Nat. (Esp)
Vol. 94, N.º 3, pp 357-376, 2000
Monográfico: Contribuciones al estudio algorítmico de problemas de moduli aritméticos

INMERSIONES DE ÓRDENES CUADRÁTICOS EN EL ORDEN GENERADO POR $\Gamma_0(N)$

(orden cuadrático/grupo de congruencia/inmersión/número de clases)

P. BAYER*, A. TRAVESA**

* Universitat de Barcelona, Facultat de Matemàtiques. Departament d'Àlgebra i Geometria. Gran Via de les Corts Catalanes, 585. E-08007 Barcelona (bayer@mat.ub.es)

** Universitat de Barcelona, Facultat de Matemàtiques. Departament d'Àlgebra i Geometria. Gran Via de les Corts Catalanes, 585. E-08007 Barcelona (travesa@mat.ub.es)

RESUMEN

El objetivo de este artículo es el estudio de las inmersiones $K \to \mathbf{M}(2, \mathbb{Q})$, de un cuerpo cuadrático en el álgebra de matrices, que son enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, en donde $\mathcal{O}_\Delta$ es un orden de K de discriminante Δ, y $\mathcal{O}_0(N)$ es un orden del álgebra de matrices asociado al grupo de congruencia $\Gamma_0(N)$. Consideramos distintos tipos de inmersiones: optimales, primitivas, y biprimitivas, que clasificamos bajo la acción del grupo $\Gamma_0(N)$. En cada caso, el conjunto cociente obtenido es finito. Determinamos los números de clases correspondientes por medio del control de invariantes numéricos adecuados. En particular, el cómputo del número de clases de inmersiones biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ recupera el número de puntos de Heegner de tipo (N, Δ) obtenido en el artículo **[Ar-Ba 00-1]**.

ABSTRACT

The aim of this paper is the study of the embeddings $K \to \mathbf{M}(2, \mathbb{Q})$, of a quadratic field in the matrix algebra, which are integral for the pair $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, where $\mathcal{O}_\Delta$ denotes an order of K of discriminent Δ, and $\mathcal{O}_0(N)$ is an order of the matrix algebra attached to the congruence group $\Gamma_0(N)$. Special types of embeddings are considered: optimal, primitive, and biprimitive, which we classify under the action of the group $\Gamma_0(N)$. Each quotient set is finite. The corresponding class numbers are determined by pursuing the control of suitable numerical invariants. In particular, the calculation of the class number of biprimitive embeddings for the pair $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ recovers the number of Heegner points of type (N, Δ) obtained in **[Ar-Ba 00-1]**.

[1] Con soporte parcial de DGES, PB96-0166.

INTRODUCCIÓN

Sean $K := \mathbb{Q}(\sqrt{\Delta_0})$ el cuerpo cuadrático asociado a un discriminante fundamental Δ_0, $\mathcal{O}_\Delta$ el orden de K de discriminante $\Delta := \Delta_0 r^2$, $r \geq 1$, y $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ un orden cualquiera del álgebra de matrices 2×2 de coeficientes racionales. En **[Ba-Tr 00-2]**, se han caracterizado las inmersiones enteras y las inmersiones optimales para la pareja $(\mathcal{O}, \mathcal{O}_\Delta)$ en función de la forma cuadrática ternaria nórmica asociada al orden $\mathbb{Z} + 2\mathcal{O}$; y se ha establecido una clasificación de estas inmersiones para ciertos subgrupos de $\mathbf{GL}(2, \mathbb{Q})$.

En este artículo, se trata de precisar la clasificación, por el grupo de congruencia $\Gamma_0(N)$, de las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ que son enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. En la sección primera, se recuerdan las definiciones y las primeras propiedades y se establece explícitamente la acción del grupo $\Gamma_0(N)$ en los conjuntos de inmersiones.

La sección segunda se dedica al estudio de ciertas clases especiales de inmersiones; más concretamente, las inmersiones primitivas y las inmersiones biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. En particular, se estudia en qué casos existen inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras, optimales, primitivas o biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$; se da una caracterización de la existencia de tales inmersiones en función de las leyes de descomposición del cuerpo cuadrático K.

El objetivo de la sección tercera es establecer diversos invariantes para las clases de $\Gamma_0(N)$-equivalencia de inmersiones y determinar sus valores.

En la sección cuarta, se halla el resultado principal para la clasificación de las inmersiones. A partir de un teorema de comparación, ésta se remite a la clasificación clásica de las formas cuadráticas binarias enteras primitivas de discriminante dado respecto del grupo $\mathbf{SL}(2,\mathbb{Z})$.

La sección quinta se dedica al estudio de los números de clases de $\Gamma_0(N)$-equivalencia de inmersiones; en particular, se obtienen fórmulas para los números de clases de diversos tipos de inmersiones y, por lo tanto, para los números de $\Gamma_0(N)$-clases de equivalencia de las formas cuadráticas binarias enteras que las definen.

La sección sexta se dedica al estudio de las inmersiones enteras y optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$, en el caso en que $\mathcal{O}(1, N, D)$ es el orden de $\mathbf{M}(2, \mathbb{Q})$ generado por $\Gamma_0(N)$, que, en general, no es el orden $\mathcal{O}_0(N)$. En particular, se reduce la clasificación de estas inmersiones al de inmersiones enteras y optimales en el orden $\mathcal{O}_0(N)$, y se obtiene su clasificación.

Finalmente, en la sección séptima se proporcionan ejemplos numéricos.

3. ACCIÓN DE $\Gamma_0(N)$ EN EL CONJUNTO DE INMERSIONES

Sean $\Delta_0 \in \mathbb{Z}$ un discriminante fundamental y $K := \mathbb{Q}(\sqrt{\Delta_0})$ el cuerpo cuadrático asociado. Para cada número entero $r \geq 1$, sea $\Delta := \Delta_0 r^2$ el discriminante asociado al orden $\mathcal{O}_\Delta \subseteq K$, de índice r en el anillo de enteros $\mathcal{O}_{\Delta_0}$ de K.

Sea $N \geq 1$ un número entero, y consideremos el orden

$$\mathcal{O}_0(N) := \left\{ \begin{bmatrix} x & y \\ zN & t \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\} \subseteq \mathbf{M}(2, \mathbb{Q}).$$

El grupo

$$\Gamma_0(N) := \left\{ \begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \det = 1 \right\} \subseteq \mathbf{SL}(2, \mathbb{Z})$$

es el grupo de las unidades de norma 1 de $\mathcal{O}_0(N)$. Para las notaciones y las propiedades de los órdenes del álgebra de matrices $\mathbf{M}(2, \mathbb{Q})$ y sus grupos de unidades de norma 1, cf. **[Ba-Tr 00-1]**.

Definición 1.1. *Se dice que una inmersión $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ es entera (resp. optimal) para la pareja $(\mathcal{O}, \mathcal{O}_\Delta)$, donde $\mathcal{O} \subseteq \mathbf{M}(2, \mathbb{Q})$ es un orden cualquiera, si $\lambda(\mathcal{O}_\Delta) \subseteq \mathcal{O}$ (resp. $\lambda^{-1}(\mathcal{O}) = \mathcal{O}_\Delta$).*

Las inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ se corresponden biyectivamente con las representaciones

$$-b^2 + 4Nac = -\Delta$$

de $-\Delta$ por la forma ternaria entera nórmica $n_{0,2}(X, Y, Z) = -Y^2 + 4NXZ$ asociada al submódulo formado por las matrices de traza nula del orden $\mathbb{Z} + 2\mathcal{O}_0(N)$. En efecto, las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ se corresponden con las matrices

$$\lambda(\sqrt{\Delta}) := \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix},$$

con $a, b, c \in \mathbb{Z}$ y tales que $-b^2 + 4Nac = -\Delta$. Y las inmersiones optimales, con las matrices $\lambda(\sqrt{\Delta})$ tales que $\mathrm{mcd}(a, b, c) = 1$ (cf. **[Ba-Tr 00-2]**).

Aunque las matrices $\lambda(\sqrt{\Delta})$ pertenecen a un suborden estricto de $\mathcal{O}_0(N)$ y $\Gamma_0(N)$ no es un subgrupo del grupo de los elementos inversibles de este suborden, sabemos que $\Gamma_0(N)$ actúa por conjugación en el conjunto de las posibles matrices $\lambda(\sqrt{\Delta}) \in \mathbb{Z} + 2\mathcal{O}_0(N)$. Hacemos explícita esta acción.

Dada una matriz cualquiera $P := \begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} \in \Gamma_0(N)$, y dado un elemento $A := \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix} \in \mathbb{Z} + 2\mathcal{O}_0(N)$ tal que $-b^2 + 4Nac = -\Delta$, pongamos $A' := P^{-1}AP$; entonces, es $A' := \begin{bmatrix} -b' & -2c' \\ 2a'N & b' \end{bmatrix}$, donde

$$\begin{bmatrix} a' \\ b' \\ c' \end{bmatrix} = \mathcal{P} \begin{bmatrix} a \\ b \\ c \end{bmatrix},$$

con

$$\mathcal{P} := \begin{bmatrix} \alpha^2 & \alpha\gamma & \gamma^2 N \\ 2\alpha\beta N & \alpha\delta + \beta\gamma N & 2\gamma\delta N \\ \beta^2 N & \beta\delta & \delta^2 \end{bmatrix}, \quad \alpha\delta + \beta\gamma N = 1 + 2\beta\gamma N.$$

Por tanto, $A' \in \mathbb{Z} + 2\mathcal{O}_0(N)$ y también es un elemento de traza nula y norma $-\Delta$.

Proposición 1.2. *La asignación $P \mapsto \mathcal{P}$ define un antimorfismo inyectivo de grupos $\Gamma_0(N)/\{\pm 1\} \to \mathbf{O}^+(n_{0,2})$, donde $\mathbf{O}^+(n_{0,2})$ designa el grupo ortogonal especial asociado a la forma cuadrática ternaria entera $n_{0,2}(X, Y, Z) = -Y^2 + 4NXZ$.* □

Puesto que $\mathcal{P}$ es, en particular, un automorfismo del grupo abeliano $\mathbb{Z}^3$, se tiene el resultado siguiente.

Corolario 1.3. *Sean $P \in \Gamma_0(N)$ y $\mathcal{P}$ la matriz asociada. Dada $\begin{bmatrix} a \\ b \\ c \end{bmatrix}$ s $\mathbb{Z}^3$, sea $\begin{bmatrix} a' \\ b' \\ c' \end{bmatrix} \in \mathbb{Z}^3$ definida por $\begin{bmatrix} a' \\ b' \\ c' \end{bmatrix} := \mathcal{P} \begin{bmatrix} a \\ b \\ c \end{bmatrix}$. Entonces, se tiene que $\mathrm{mcd}(a, b, c) = \mathrm{mcd}(a', b', c')$.* □

2. INMERSIONES PRIMITIVAS Y BIPRIMITIVAS

Recordemos que la acción usual del grupo $\mathbf{PGL}(2, \mathbb{R})$ en el plano complejo $\mathbb{C} \cup \{\infty\}$ se define por la fórmula

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix}(z) := \frac{az + b}{cz + d},$$

para $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathbf{GL}(2, \mathbb{R})$ y $z \in \mathbb{C} \cup \{\infty\}$ arbitrarios, ya que las homotecias actúan trivialmente.

En particular, si $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ es una inmersión cualquiera, se tiene que $\det(\lambda(\sqrt{\Delta})) = -\Delta \neq 0$; por tanto, $\lambda(\sqrt{\Delta}) \in \mathbf{GL}(2, \mathbb{Q})$.

Por otra parte, si nos restringimos al subgrupo de las matrices de determinante positivo, la acción restringe, por un lado, al semiplano superior $\mathbb{H} := \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$, y, por otro, a $\mathbb{R} \cup \{\infty\}$.

Dado un polinomio cuadrático $aZ^2 + bZ + c$, con $a, b, c \in \mathbb{R}$, sea $\Delta := b^2 - 4ac$ su discriminante. Escribiremos las raíces del polinomio en la forma

$$z := \frac{-b + \sqrt{\Delta}}{2a}, \quad z' := \frac{-b - \sqrt{\Delta}}{2a},$$

donde elegimos $z \in \mathbb{H}$, si $\Delta < 0$.

Observación 2.1. *Sea $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ una inmersión cualquiera, dada por la asignación $\lambda(\sqrt{\Delta}) =: \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix}$, con $a, b, c \in \mathbb{Q}$.*

Para la acción de $\mathbf{GL}(2, \mathbb{R})$ en $\mathbb{C} \cup \{\infty\}$, existen exactamente dos puntos $z, z' \in \mathbb{C} \cup \{\infty\}$ fijos por todas las matrices de $\lambda(K)$; es decir, las matrices $x + y\lambda(\sqrt{\Delta})$, con $x, y \in \mathbb{Q}$. Estos dos números complejos son las raíces

$$z := \frac{-b + \sqrt{\Delta}}{2Na}, \quad z' := \frac{-b - \sqrt{\Delta}}{2Na},$$

del polinomio $NaZ^2 + bZ + c$. En particular, los dos puntos sólo dependen de $\lambda(K)$, pero no de la imagen de ningún elemento concreto de K, de manera que están asociados unívocamente a la inmersión λ.

El grupo $\mathbf{GL}(2, \mathbb{Q})$ y, en consecuencia, cualquiera de sus subgrupos, actúa en el conjunto de todas las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$, en el sentido que dadas una matriz $P \in \mathbf{GL}(2, \mathbb{Q})$, y una inmersión λ_1, la conjugación $\sqrt{\Delta} \mapsto \lambda_2(\sqrt{\Delta}) := P^{-1}\lambda_1(\sqrt{\Delta})P$ define otra inmersión de K en $\mathbf{M}(2, \mathbb{Q})$; escribiremos σ_P para designar la conjugación $A \mapsto P^{-1}AP$.

Si dos inmersiones cualesquiera $\lambda_1, \lambda_2 : K \to \mathbf{M}(2, \mathbb{Q})$ son $\Gamma_0(N)$-equivalentes, de manera que para una matriz $P \in \Gamma_0(N)$ se tiene que $\sigma_P \circ \lambda_1 = \lambda_2$, entonces los puntos fijos respectivos, z_1, z_2, son equivalentes por la acción de la matriz P^{-1}; es decir, se tiene que $P^{-1}z_1 = z_2$, y que $P^{-1}z_1' = z_2'$. Por tanto, hemos establecido el resultado siguiente.

Corolario 2.2. *A cada clase de $\Gamma_0(N)$-equivalencia de inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ le corresponde una clase de $\Gamma_0(N)$-equivalencia de puntos de $\mathbb{H} \cup \mathbb{R} \cup \{\infty\}$ para la acción de $\Gamma_0(N)$ en $\mathbb{C} \cup \{\infty\}$ como subgrupo de $\mathbf{GL}(2, \mathbb{R})$.* □

Por otra parte, si dos puntos $z_1, z_2 \in \mathbb{C}$ son $\Gamma_0(N)$-equivalentes, entonces los puntos Nz_1, Nz_2 son $\mathbf{SL}(2,\mathbb{Z})$-equivalentes. En efecto, si una matriz $P := \begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} \in \Gamma_0(N)$ es tal que $Pz_1 = z_2$, entonces es $Q(Nz_1) = Nz_2$, donde $Q := \begin{bmatrix} \alpha & \beta N \\ \gamma & \delta \end{bmatrix} \in \mathbf{SL}(2, \mathbb{Z})$. Finalmente, observemos que si z_1 satisface la ecuación $NaZ^2 + bZ + c = 0$, entonces para Nz_1 se satisface que $a(Nz_1)^2 + b(Nz_1) + Nc = 0$; es decir, Nz_1 satisface la ecuación $aZ^2 + bZ + Nc = 0$. La observación de estos resultados nos lleva a la definición siguiente.

Definición 2.3. *Diremos que una inmersión $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ entera para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, y dada por la asignación*

$$\lambda(\sqrt{\Delta}) = \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix}, \quad a, b, c \in \mathbb{Z},$$

es primitiva si, y sólo si, $\mathrm{mcd}(Na, b, c) = 1$. *Diremos que es biprimitiva si, y sólo si, es* $\mathrm{mcd}(Na, b, c) = \mathrm{mcd}(a, b, Nc) = 1$.

En particular, toda inmersión biprimitiva es primitiva y toda inmersión primitiva es optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. El objetivo principal de esta sección es estudiar los dos problemas siguientes.

Problema 1. *Dada una inmersión $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$, ¿para qué parejas $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ es λ entera, optimal, primitiva o biprimitiva?*

Problema 2. *Dada una pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, ¿existen inmersiones λ enteras, optimales, primitivas o biprimitivas para esta pareja?*

En relación con el primer problema, tenemos el teorema siguiente.

Teorema 2.4. *Sea $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ una inmersión del cuerpo cuadrático $K := \mathbb{Q}(\sqrt{\Delta_0})$, asociado al discriminante fundamental Δ_0, en $\mathbf{M}(2, \mathbb{Q})$. Existen números enteros $N, r \geq 1$ tales que λ es biprimitiva para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, donde $\Delta := \Delta_0 r^2$.*

Para demostrar el teorema, caracterizaremos los valores de N y de r (o sea, de Δ) para los cuales λ es entera, optimal, primitiva y biprimitiva, respectivamente, para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Definición 2.5. *Para una inmersión* $\lambda : \mathbb{Q}(\sqrt{\Delta_0}) \to \mathbf{M}(2, \mathbb{Q})$ *cualquiera, pondremos* $\mathrm{Ent}(\lambda)$ *para designar el conjunto de los pares de números enteros* (N, Δ), $N \geq 1$, $\Delta = \Delta_0 r^2$ *con* $r \geq 1$, *tales que* λ *es entera para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. *Análogamente,* $\mathrm{Opt}(\lambda)$, $\mathrm{Prim}(\lambda)$ *y* $\mathrm{Biprim}(\lambda)$ *designarán los conjuntos de pares* (N, Δ) *tales que* λ *es optimal, primitiva y biprimitiva, respectivamente, para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Con estas notaciones, el enunciado del teorema anterior se puede precisar en la forma siguiente, que proporciona la solución del primer problema.

Teorema 2.6. *Sea* $\lambda : \mathbb{Q}(\sqrt{\Delta_0}) \to \mathbf{M}(2, \mathbb{Q})$ *una inmersión cualquiera y sean* $A, B, C \in \mathbb{Q}$ *tales que* $\lambda(\sqrt{\Delta_0}) = \begin{bmatrix} -B & -2C \\ 2A & B \end{bmatrix}$. *Sea* $r_1 \geq 1$ *el mínimo común denominador de los números racionales* A, B, C, *y pongamos* $N_1 := r_1|A|$, $b_1 := r_1 B$, $c_1 := r_1 C$, *y* $\Delta_1 := \Delta_0 r_1^2$. *Entonces,* N_1, b_1, $c_1 \in \mathbb{Z}$, $N_1 \geq 1$, Δ_1 *es un discriminante asociado al discriminante fundamental* Δ_0, *y, además, los valores de* N *y* Δ *para los cuales* λ *es entera, optimal, primitiva o biprimitiva para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ *son los dados por:*

(a) $\mathrm{Ent}(\lambda) = \{(N, \Delta_1 r^2) : r \geq 1,\ N | r N_1\}$.

(b) $\mathrm{Opt}(\lambda) = \{(Nr, \Delta_1 r^2) : r \geq 1,\ N | N_1,\ \mathrm{mcd}(r, N_1/N) = 1\}$.

(c) $\mathrm{Prim}(\lambda) = \{(N, \Delta_1) : N | N_1\}$.

(d) $\mathrm{Biprim}(\lambda) = \{(N, \Delta_1) : N | N_1,\ \mathrm{mcd}(N_1/N, b_1, N) = 1\}$.

Demostración. Si λ es entera para una pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, donde Δ es un discriminante asociado al discriminante fundamental Δ_0, ha de ser $\Delta = \Delta_0 r^2$, para algún número entero $r \geq 1$, y es necesario que $\lambda(\sqrt{\Delta}) = \lambda(r\sqrt{\Delta_0}) \in \in \mathbb{Z} + 2\mathcal{O}_0(N) \subseteq \mathbb{Z} + 2\mathbf{M}(2, \mathbb{Z})$; por tanto, debe ser rA, rB, $rC \in \mathbb{Z}$; esto obliga a que r sea múltiplo de r_1 o, equivalentemente, a que Δ sea de la forma $\Delta = \Delta_1 r^2$, con $\Delta_1 := \Delta_0 r_1^2$, y $r \geq 1$ un número entero cualquiera. Y para cada uno de estos valores de Δ, los valores de N para los cuales es $\lambda(\sqrt{\Delta}) \in \mathbb{Z} + 2\mathcal{O}_0(N)$ son exactamente los divisores del número entero rN_1; esto demuestra (a).

Notemos que el hecho que Δ_0 sea un discriminante fundamental implica, por un lado, que es $A \neq 0$ y, por otro, que es $\mathrm{mcd}(N_1, b_1, c_1) = 1$; es decir, que los numeradores de los números racionales A, B, C no pueden tener divisores comunes. Esta observación será útil para calcular, a continuación, los pares $(N, \Delta) \in \mathrm{Ent}(\lambda)$ para los cuales la inmersión λ es optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Sean, pues, $r \geq 1$ y N un divisor de rN_1; entonces, λ es entera para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. El cálculo de $\lambda(\sqrt{\Delta})$ proporciona

$$\lambda(\sqrt{\Delta}) = \begin{bmatrix} -rb_1 & -2rc_1 \\ 2\varepsilon r N_1 & rb_1 \end{bmatrix},$$

donde $\varepsilon := \mathrm{sig}(A)$; por tanto, λ es optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ si, y sólo si, es $\mathrm{mcd}(a, rb_1, rc_1) = 1$, con $a \in \mathbb{Z}$ el número entero tal que $\varepsilon r N_1 = aN$. Esto implica que a no es divisible por ninguno de los primos que dividen r; en particular, N es múltiplo de r y, si ponemos $N = rN'$, debe ser $\varepsilon r N_1 = aN = arN'$. Pero esto ya es suficiente, ya que $\mathrm{mcd}(N_1, b_1, c_1) = 1$, de manera que, puesto que a divide N_1, es $\mathrm{mcd}(a, b_1, c_1) = 1$ y, en consecuencia, $\mathrm{mcd}(a, rb_1, rc_1) = \mathrm{mcd}(a, r) = 1$. Esto demuestra (b).

Para los valores del caso anterior, es decir, los que hacen que λ sea optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, se tiene que

$$\lambda(\sqrt{\Delta}) = \begin{bmatrix} -rb_1 & -2rc_1 \\ 2aN & rb_1 \end{bmatrix},$$

de manera que $\mathrm{mcd}(Na, rb_1, rc_1) = r$; por tanto, λ es primitiva para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ si, y sólo si, es $r = 1$. Esto demuestra (c).

Finalmente, para la inmersión primitiva del caso anterior, es $\Delta = \Delta_0 r_1^2$ y $\lambda(\sqrt{\Delta}) = \begin{bmatrix} -b_1 & -2c_1 \\ 2aN & b_1 \end{bmatrix}$. Calculemos $d := \mathrm{mcd}(a, b_1, Nc_1)$. Puesto que $\mathrm{mcd}(N_1, b_1, c_1) = 1$ y $a = \pm\dfrac{N_1}{N}$ divide N_1, es $\mathrm{mcd}(a, b_1, c_1) = 1$, de manera que $d = \mathrm{mcd}(a, b_1, N) = \mathrm{mcd}(N_1/N, b_1, N)$. Por tanto, los valores posibles de N son aquellos para los cuales es $\mathrm{mcd}(N_1/N, b_1, N) = 1$. □

Observación 2.7. *Notemos que, en particular, para* $N = N_1$ *o bien para* $N = 1$, *es* $(N, \Delta_1) \in \mathrm{Biprim}(\lambda)$. *En particular, todos los conjuntos* $\mathrm{Ent}(\lambda)$, $\mathrm{Opt}(\lambda)$, $\mathrm{Prim}(\lambda)$, $\mathrm{Biprim}(\lambda)$ *son no vacíos.*

Por otra parte, en el caso particular en que $A, B, C \in \mathbb{Z}$, *es decir, en el caso en que* $r_1 = 1$, *el discriminante* Δ_1 *coincide con el discriminante fundamental* Δ_0, *de manera que, en este caso, la inmersión* λ *sólo es primitiva o biprimitiva para algún valor de* N *cuando* $\Delta = \Delta_0$.

Observación 2.8. *Sea* $\lambda : K = \mathbb{Q}(\sqrt{\Delta}) \to \mathbf{M}(2, \mathbb{Q})$ *una inmersión entera para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, *dada por* $\lambda(\sqrt{\Delta}) = \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix}$, *con* $a, b, c \in \mathbb{Z}$ *y* $-b^2 + 4Nac = -\Delta$. *Hemos definido el concepto de inmersión biprimitiva para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ *por las condiciones*

$\mathrm{mcd}(Na, b, c) = \mathrm{mcd}(a, b, Nc) = 1$. *Estas condiciones equivalen a las*

$$\mathrm{mcd}(a, b, c) = \mathrm{mcd}(N, b, c) = \mathrm{mcd}(a, b, N) = 1,$$

y también a las

$$\mathrm{mcd}(a, b, c) = \mathrm{mcd}(N, b, ac) = 1.$$

En particular, si se satisface que $\mathrm{mcd}(a, b, c) = 1$, *también se tiene que*

$$\mathrm{mcd}(N, b, ac) = \mathrm{mcd}(a, b, N)\mathrm{mcd}(N, b, c)$$

y que $\mathrm{mcd}(Na, b, c) = \mathrm{mcd}(N, b, c)$ *y* $\mathrm{mcd}(a, b, Nc) = \mathrm{mcd}(a, b, N)$. *Esta observación será útil más adelante.*

Corolario 2.9 (Descenso de nivel). *Sean* $\lambda : K \longrightarrow \mathbf{M}(2, \mathbb{Q})$ *una inmersión,* Δ *un discriminante, y* $N, N' \geq 1$ *números enteros tales que* N' *divide* N.

(a) Si λ *es entera para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, *entonces* λ *es entera para la pareja* $(\mathcal{O}_0(N'), \mathcal{O}_\Delta)$.

(b) Si λ *es primitiva para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, *entonces* λ *es primitiva para la pareja* $(\mathcal{O}_0(N'), \mathcal{O}_\Delta)$.

(c) La inmersión λ *puede ser optimal para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, *pero no ser optimal para la pareja* $(\mathcal{O}_0(N'), \mathcal{O}_\Delta)$.

(d) La inmersión λ *puede ser biprimitiva para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, *pero no ser biprimitiva para la pareja* $(\mathcal{O}_0(N'), \mathcal{O}_\Delta)$. □

La solución del segundo problema para las inmersiones enteras, optimales y primitivas viene dada por el resultado siguiente; para las inmersiones biprimitivas, cf. el teorema **3.11**.

Teorema 2.10. *Sean* $N, r \geq 1$ *números enteros y* $\Delta := \Delta_0 r^2$ *un discriminante asociado al discriminante fundamental* Δ_0. *Existe alguna inmersión* $\lambda : K \longrightarrow \mathbf{M}(2, \mathbb{Q})$ *entera para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ *si, y sólo si, la descomposición de N en factores primos es de la forma*

$$N = \prod_p p^{v_p},$$

con $v_p \leq 1 + 2v_p(r)$, *si p ramifica en el orden maximal del cuerpo cuadrático K;* $v_p \leq 2v_p(r)$, *si p es inerte en el orden maximal de K; y* v_p *cualquiera, si p descompone completamente en el orden maximal de K. Existen inmersiones primitivas para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ *si, y sólo si, existen inmersiones optimales para* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$; *si, y sólo si, existen inmersiones enteras para* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Demostración. La existencia de inmersiones $\lambda : K \longrightarrow \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ equivale a la existencia de soluciones enteras (a, b, c) de la ecuación diofántica

$$-b^2 + 4Nac = -\Delta;$$

la existencia de inmersiones optimales, a la existencia de soluciones enteras primitivas de esta ecuación; y la existencia de inmersiones primitivas, a la existencia de soluciones enteras primitivas y tales que $\mathrm{mcd}(Na, b, c) = 1$. Cualquiera de las tres condiciones equivale a la existencia de soluciones de la congruencia

$$b^2 \equiv \Delta \pmod{4N}$$

(puesto que podemos tomar $c = 1$); y, en virtud del teorema chino del resto, a la existencia de soluciones de cada una de las congruencias

$$b^2 \equiv \Delta = \Delta_0 r^2 \pmod{p^{v_p}}, \qquad p > 2,$$
$$b^2 \equiv \Delta = \Delta_0 r^2 \pmod{2^{2+v_2}}, \qquad p = 2,$$

donde escribimos N en la forma $N = \prod_p p^{v_p}$, y p designan números primos arbitrarios distintos.

Sea p un número primo, y pongamos $r = p^w r'$, con $w \geq 0$ i r' no divisible por p; es decir, $w = v_p(r)$.

Consideremos, en primer lugar, el caso en que $p \neq 2$ y que es $v_p > 2w + 1$. La congruencia

$$b^2 \equiv \Delta_0 p^{2w} r'^2 \pmod{p^{v_p}}$$

tiene solución b si, y sólo si, la congruencia

$$x^2 \equiv \Delta_0 \pmod{p^{v_p - 2w}}$$

tiene solución $x \equiv \dfrac{b}{r' p^w} \pmod{p^{v_p - 2w}}$. Puesto que $v_p - 2w \geq 2$ y Δ_0 no puede ser divisible por p^2, la condición anterior equivale a decir que Δ_0 no es divisible por p y que la congruencia

$$x^2 \equiv \Delta_0 \pmod{p}$$

tiene dos soluciones distintas (que se pueden elevar a soluciones módulo $p^{v_p - 2w}$ en virtud del lema de Hensel); es decir, que el polinomio $X^2 - \Delta_0$ tiene dos raíces distintas en $\mathbb{Z}/p\mathbb{Z}$; o sea, que p descompone completamente en el orden maximal del cuerpo cuadrático K.

Supongamos, ahora, que es $p \neq 2$ y $v_p = 2w + 1$. La congruencia

$$b^2 \equiv \Delta_0 p^{2w} r'^2 \pmod{p^{v_p}}$$

tiene solución si, y sólo si, la congruencia

$$x^2 \equiv \Delta_0 \pmod{p}$$

tiene solución; y esto equivale a decir que el polinomio $X^2 - \Delta_0$ tenga alguna raíz en $\mathbb{Z}/p\mathbb{Z}$; es decir, que p descomponga completamente o bien ramifique en el orden maximal de K.

Finalmente, supongamos que $p \neq 2$ y que $v_p \leq 2w$; entonces, la congruencia

$$b^2 \equiv \Delta_0 p^{2w} r'^2 \pmod{p^{v_p}}$$

se reduce a la congruencia

$$b^2 \equiv 0 \pmod{p^{v_p}},$$

que siempre tiene solución.

Resta considerar el caso $p = 2$; es decir, la congruencia

$$b^2 \equiv \Delta_0 2^{2w} r'^2 \pmod{2^{2+v_2}}.$$

Supongamos, pues, que es $v_2 > 2w + 1$. La congruencia

$$b^2 \equiv \Delta_0 2^{2w} r'^2 \pmod{2^{2+v_2}}$$

tiene solución b si, y sólo si, la congruencia

$$x^2 \equiv \Delta_0 \pmod{2^{2+v_2-2w}}$$

tiene solución $x \equiv \dfrac{b}{r'2^w} \pmod{2^{2+v_2-2w}}$. Puesto que $2 + v_2 - 2w \geq 4$, eso implica que la congruencia $x^2 \equiv \Delta_0 \pmod{2^4}$ tiene solución. Ahora, dado que Δ_0 es un discriminante fundamental, o bien es $\Delta_0 \equiv 1 \pmod 4$, o bien es $\Delta_0 = 4\delta_0$, con $\delta_0 \equiv 2,3 \pmod 4$. En el primer caso, $\Delta_0 \equiv 1 \pmod 4$, la congruencia $x^2 \equiv \Delta_0 \pmod 8$ tiene solución, de manera que debe ser $\Delta_0 \equiv 1 \pmod 8$; y recíprocamente, si $\Delta_0 \equiv 1 \pmod 8$, las cuatro soluciones distintas de $x^2 \equiv \Delta_0 \pmod 8$ se pueden elevar, en virtud del lema de Hensel, a soluciones de $x^2 \equiv \Delta_0 \pmod{2^{2+v_2-2w}}$.

En el otro caso, si la congruencia $x^2 \equiv \Delta_0 = 4\delta_0 \pmod{2^4}$ tuviese solución, debería ser $\dfrac{x^2}{4} \equiv \delta_0 \equiv 2,3 \pmod 4$, caso en que, evidentemente, no hay solución.

Por tanto, si $v_2 > 1 + 2w$, la congruencia

$$b^2 \equiv \Delta_0 2^{2w} r'^2 \pmod{2^{2+v_2}}$$

tiene solución si, y sólo si, es $\Delta_0 \equiv 1 \pmod 8$ o, lo que es equivalente, si, y sólo si, 2 descompone completamente en el orden maximal de K.

En el caso $p = 2$ y $v_2 = 2w + 1$, la congruencia

$$b^2 \equiv \Delta_0 2^{2w} r'^2 \pmod{2^{2+v_2}}$$

tiene solución b si, y sólo si, la congruencia

$$x^2 \equiv \Delta_0 \pmod{2^3}$$

tiene solución $x \equiv \dfrac{b}{r'2^w} \pmod{2^3}$; y esto equivale a decir que 2 o bien descompone completamente o bien ramifica en el orden maximal de K.

Finalmente, si $p = 2$ y $v_2 \leq 2w$, la congruencia

$$b^2 \equiv \Delta_0 2^{2w} r'^2 \pmod{2^{2+v_2}}$$

siempre tiene solución. En efecto; esto es claro si $v_2 \leq \leq 2w - 2$, ya que la congruencia se reduce a $b^2 \equiv 0 \pmod{2^{2+v_2}}$; también es claro si $v_2 = 2w$, ya que la congruencia

$$x^2 \equiv \Delta_0 r'^2 \pmod{2^2}$$

tiene solución, puesto que $\Delta_0 r'^2$ es un discriminante y, en consecuencia, es $\Delta_0 r'^2 \equiv 0,1 \pmod 4$; y también es claro si $v_2 = 2w - 1$, ya que la congruencia

$$x^2 \equiv \Delta_0 r'^2 \pmod 2$$

tiene solución evidente. □

Corolario 2.11. *Si $\Delta = \Delta_0$ es un discriminante fundamental, toda inmersión $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta_0})$ es automáticamente biprimitiva para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta_0})$. Más generalmente, si* mcd$(N, r) = 1$, *toda inmersión $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta_0 r^2})$ es automáticamente biprimitiva para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta_0 r^2})$.*

Demostración. Sea $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ una inmersión optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, dada por la asignación $\lambda(\sqrt{\Delta}) = \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix}$, con $\Delta := \Delta_0 r^2$, $r \geq 1$. De la igualdad $b^2 - 4Nac = \Delta_0 r^2$, y teniendo en cuenta que Δ_0 es un discriminante fundamental, se deduce que mcd(N, b, ac) divide r. En particular, si es mcd$(N, r) = 1$, debe ser mcd$(N, b, ac) = 1$, de donde λ es biprimitiva para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta_0 r^2})$, puesto que mcd$(a, b, c) = 1$, por hipótesis. □

Observación 2.12. *Puede ser que existan inmersiones primitivas y no existan inmersiones biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. Basta, por ejemplo, que exista un primo $p \neq 2$ que divida r y N, pero tal que p^2 no divida N (hecho acorde con las condiciones del teorema). Entonces, p debe dividir b y ac, de manera que p divide* mcd(N, b, ac) *y ninguna inmersión entera para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ es biprimitiva para dicha pareja.*

3. INVARIANTES DE LAS CLASES DE INMERSIONES

La clasificación de las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para las parejas $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ respecto del grupo $\Gamma_0(N)$ es equivalente a la clasificación de las formas cuadráticas binarias enteras del tipo $[Na, b, c] := NaX^2 + + bXY + cY^2$ por este grupo. En efecto, la relación

$P^{-1}\lambda(\sqrt{\Delta})P = \lambda'(\sqrt{\Delta})$, para $P \in \Gamma_0(N)$, equivale a la relación $P^tBP = B'$, donde $B := \begin{bmatrix} 2aN & b \\ b & 2c \end{bmatrix}$ y $B' := \begin{bmatrix} 2a'N & b' \\ b' & 2c' \end{bmatrix}$ son las matrices asociadas a las formas cuadráticas $[Na,b,c]$ y $[Na',b',c']$. A continuación, enunciaremos y demostraremos los resultados para la clasificación en términos de inmersiones.

En primer lugar, conviene observar que $\Gamma_0(N)$ no sólo actúa en los conjuntos de inmersiones enteras y optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, sino que también actúa en los conjuntos de inmersiones primitivas y biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

En efecto, supongamos que $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ es una inmersión entera para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, dada por la asignación $\lambda(\sqrt{\Delta}) = \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix} \in \mathbb{Z} + 2\mathcal{O}_0(N)$, y que $P := \begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} \in \Gamma_0(N)$ es una matriz cualquiera. Sea $\lambda'(\sqrt{\Delta}) := P^{-1}\lambda(\sqrt{\Delta})P$, de manera que $\lambda'(\sqrt{\Delta}) = \begin{bmatrix} -b' & -2c' \\ 2a'N & b' \end{bmatrix} \in \mathbb{Z} + 2\mathcal{O}_0(N)$, con

$$\begin{bmatrix} a' \\ b' \\ c' \end{bmatrix} = \mathcal{P} \begin{bmatrix} a \\ b \\ c \end{bmatrix},$$

para la matriz $\mathcal{P}$ definida como en la sección primera.

Este sistema de ecuaciones se puede escribir equivalentemente en la forma

$$\begin{aligned} Na' &:= \alpha^2 Na + \alpha\gamma Nb + \gamma^2 N^2 c \\ b' &:= 2\alpha\beta Na + (1 + 2\beta\gamma N)b + 2\gamma\delta Nc \\ c' &:= \beta^2 Na + \beta\delta b + \delta^2 c, \end{aligned}$$

de manera que $\mathrm{mcd}(Na, b, c)$ divide $\mathrm{mcd}(Na', b', c')$; y recíprocamente, al tener en cuenta la matriz inversa P^{-1} de P. Por tanto, $\mathrm{mcd}(Na, b, c) = \mathrm{mcd}(Na', b', c')$.

Análogamente, si escribimos el sistema en la forma

$$\begin{aligned} a' &:= \alpha^2 a + \alpha\gamma b + \gamma^2 Nc \\ b' &:= 2\alpha\beta Na + (1 + 2\beta\gamma N)b + 2\gamma\delta Nc \\ Nc' &:= \beta^2 N^2 a + \beta\delta Nb + \delta^2 Nc, \end{aligned}$$

obtenemos que $\mathrm{mcd}(a, b, Nc) = \mathrm{mcd}(a', b', Nc')$.

Por tanto, hemos demostrado que se satisfacen los resultados siguientes.

Corolario 3.1. *Los números enteros* $\mathrm{mcd}(Na, b, c)$ *y* $\mathrm{mcd}(a, b, Nc)$ *son invariantes de las clases de* $\Gamma_0(N)$*-equivalencia de inmersiones enteras (resp. optimales) para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. □

Corolario 3.2. *El grupo* $\Gamma_0(N)$ *actúa en el conjunto de las inmersiones primitivas (resp. biprimitivas) para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. □

Observación 3.3. *Análogamente, a partir del sistema anterior se obtiene que* $\mathrm{mcd}(N, b, ac)$ *es un invariante para las clases de* $\Gamma_0(N)$*-equivalencia de inmersiones enteras (resp. optimales, primitivas, biprimitivas) para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Interesa definir otro invariante de las clases de $\Gamma_0(N)$-equivalencia de inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. Para ello, tenemos el resultado siguiente.

Proposición 3.4. *La clase de b módulo* $2N$ *es un invariante para las clases de* $\Gamma_0(N)$*-equivalencia de inmersiones enteras (resp. optimales, primitivas, biprimitivas) para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Demostración. Basta escribir la ecuación

$$b' = 2\alpha\beta Na + (1 + 2\beta\gamma N)b + 2\gamma\delta Nc$$

en la forma equivalente

$$b' = b + 2N(\alpha\beta a + \beta\gamma b + \gamma\delta c),$$

y reducir módulo $2N$. □

Una última observación antes de emprender la clasificación. El conjunto de las inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ está en correspondencia biyectiva con el conjunto de los elementos de $\mathbb{Z} + 2\mathcal{O}_0(N)$ de traza nula y determinante $-\Delta$; es decir, con el conjunto de las matrices de la forma

$$[Na, b, c] := \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix}, \quad -b^2 + 4Nac = -\Delta;$$

y el conjunto de las inmersiones optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, con el de las matrices como la anterior tales que, además, se satisface que $\mathrm{mcd}(a, b, c) = 1$. Análogamente, al añadir la condición $\mathrm{mcd}(Na, b, c) = 1$ se obtiene una biyección con el conjunto de las inmersiones primitivas, y al añadir las condiciones $\mathrm{mcd}(Na, b, c) = \mathrm{mcd}(a, b, Nc) = 1$, una biyección con el conjunto de las inmersiones biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. Por tanto, la clasificación de las inmersiones es equivalente a la clasificación de estos conjuntos.

Definición 3.5. *Pondremos $\mathcal{H}(N, \Delta)$ para designar el conjunto de las matrices*

$$[Na, b, c] := \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix}, \quad a, b, c \in \mathbb{Z},$$

de determinante $-b^2 + 4Nac = -\Delta$. Notemos que $\mathcal{H}(N, \Delta) \subseteq \mathcal{H}(N', \Delta)$, para todo divisor N' de N; en particular, para $N' = 1$, tenemos que $\mathcal{H}(N, \Delta) \subseteq \mathcal{H}(1, \Delta)$.

Corolario 3.6. *El grupo $\Gamma_0(N)$ actúa de manera natural en los conjuntos $\mathcal{H}(N', \Delta)$, para N' divisor de N.*

Demostración. Basta observar que $\Gamma_0(N')$ actúa de manera natural en $\mathcal{H}(N', \Delta)$ y que $\Gamma_0(N) \subseteq \Gamma_0(N')$ es un subgrupo. □

Corolario 3.7. *La clase de b módulo $2N$ es un invariante de las clases de $\Gamma_0(N)$-equivalencia de $\mathcal{H}(N, \Delta)$.* □

En general, para una matriz cualquiera $[Na, b, c] \in \in \mathcal{H}(N, \Delta)$, pondremos $m_1 := \text{mcd}(Na, b, c)$, $m_2 := \text{mcd}(a, b, Nc)$. En el caso en que $\text{mcd}(a, b, c) = 1$, se tiene que (cf. la observación **2.8**)

$$m_1 = \text{mcd}(Na, b, c) = \text{mcd}(N, b, c),$$
$$m_2 = \text{mcd}(a, b, Nc) = \text{mcd}(a, b, N),$$
$$\text{mcd}(m_1, m_2) = 1,$$
$$m := m_1 m_2 = \text{mcd}(N, b, ac).$$

Hemos obtenido, pues, diferentes invariantes asociados a las clases de $\Gamma_0(N)$-equivalencia de inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$; a saber, $d := \text{mcd}(a, b, c)$, $m_1 := \text{mcd}(Na, b, c)$, $m_2 := \text{mcd}(a, b, Nc)$, y B, la clase de b módulo $2N$.

Definición 3.8. *Dados números enteros $N, d, m_1, m_2 \geq 1$, y $\Delta, B \in \mathbb{Z}$, pondremos*

$$\mathcal{H}(N, \Delta; d, m_1, m_2, B)$$

para designar el conjunto de las matrices $[Na, b, c] \in \in \mathcal{H}(N, \Delta)$ tales que $\text{mcd}(a, b, c) = d$, $\text{mcd}(Na, b, c) = m_1$, $\text{mcd}(a, b, Nc) = m_2$, y $b \equiv B \pmod{2N}$. En el caso de no fijar alguno de los valores del invariante, escribiremos $*$ en el lugar correspondiente.

3.9. Ejemplos y propiedades

- Puesto que el invariante B está definido módulo $2N$, para números enteros $B, B' \in \mathbb{Z}$ tales que $B \equiv B' \pmod{2N}$, se tiene que

$$\mathcal{H}(N, \Delta; d, m_1, m_2, B) = \mathcal{H}(N, \Delta; d, m_1, m_2, B').$$

- En consecuencia, se tiene que

$$\mathcal{H}(N, \Delta; d, m_1, m_2, *) = \bigcup_{B \,(\text{mod } 2N)} \mathcal{H}(N, \Delta; d, m_1, m_2, B),$$

la reunión disjunta, donde $\mathcal{H}(N, \Delta; d, m_1, m_2, *)$ designa el conjunto de las matrices $[Na, b, c] \in \mathcal{H}(N, \Delta)$ tales que $\text{mcd}(a, b, c) = \text{d}$, $\text{mcd}(Na, b, c) = m_1$, $\text{mcd}(a, b, Nc) = m_2$, y b es cualquiera.

- En particular, $\mathcal{H}(N, \Delta; 1, *, *, *)$ es el subconjunto de $\mathcal{H}(N, \Delta)$ formado por las matrices $[Na, b, c]$ tales que $\text{mcd}(a, b, c) = 1$; es decir, de las matrices que se corresponden con las inmersiones optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

- Llamaremos $\Gamma_0(N)$-primitivas a las matrices que se corresponden con las inmersiones primitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$; es decir, a las matrices de $\mathcal{H}(N, \Delta; 1, 1, *, *)$.

- Llamaremos $\Gamma_0(N)$-biprimitivas a las matrices que se corresponden con las inmersiones biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$; es decir, a las matrices de $\mathcal{H}(N, \Delta; 1, 1, 1, *)$.

- Para cada divisor natural m_1 de N, tenemos que

$$\mathcal{H}(N, \Delta; 1, m_1, *, *) = \bigcup_{\substack{m_2 | N \\ \text{mcd}(m_1, m_2) = 1}} \mathcal{H}(N, \Delta; 1, m_1, \text{m}_2, *).$$

- Notemos que, en el caso $N = 1$, se tiene que $d = m_1 = = m_2$, y que, para toda matriz $[a, b, c] \in \mathcal{H}(1, \Delta)$ es $b \equiv \Delta \pmod 2$, de manera que basta únicamente con el invariante d. Escribiremos, pues, $\mathcal{H}(1, \Delta; d)$, o bien $\mathcal{H}(1, \Delta; *)$.

- En general, se tiene que $\mathcal{H}(N, \Delta; 1, *, *, *) \subsetneq \subsetneq \mathcal{H}(1, \Delta; 1)$, puesto que puede ser $\text{mcd}(a, b, c) = 1$ pero $\text{mcd}(Na, b, c) \neq 1$.

Por el uso que haremos del resultado siguiente, conviene destacarlo.

Corolario 3.10. *Para todo par de divisores naturales (m_1, m_2) primos entre sí de N, el grupo $\Gamma_0(N)$ actúa en los conjuntos*

$$\mathcal{H}(N, \Delta; 1, m_1, m_2, *), \quad \mathcal{H}(N, \Delta; 1, m_1, *, *).$$

La clase de b módulo $2N$ es invariante de las clases de $\Gamma_0(N)$-equivalencia. □

El teorema siguiente permite caracterizar en qué casos los conjuntos $\mathcal{H}(N, \Delta; 1, m_1, m_2, B)$ son no vacíos; en particular, responde al problema **2** de la sección 2 para el caso de las inmersiones biprimitivas.

Teorema 3.11. *Sean N, Δ, B, m_1, $m_2 \in \mathbb{Z}$ números enteros tales que N, m_1, $m_2 \geq 1$, y Δ es un discriminante. El conjunto*

$$\mathcal{H}(N, \Delta; 1, m_1, m_2, B)$$

es no vacío si, y sólo si, se satisfacen las condiciones siguientes:

(a) $B^2 \equiv \Delta \pmod{4N}$.

(b) $\mathrm{mcd}(m_1, m_2) = 1$.

(c) $m_1 m_2 = \mathrm{mcd}\left(N, B, \dfrac{B^2 - \Delta}{4N}\right)$.

Además, si el conjunto $\mathcal{H}(N, \Delta; 1, m_1, m_2, B)$ es no vacío, también es no vacío el conjunto $\mathcal{H}(N', \Delta'; 1, 1, m_2, B')$, donde $N' := \dfrac{N}{m_1}$, $\Delta' := \dfrac{\Delta}{m_1^2}$, y $B' := \dfrac{B}{m_1} \in \mathbb{Z}$.

Demostración. Si existe alguna matriz

$$[Na, b, c] \in \mathcal{H}(N, \Delta; 1, m_1, m_2, B),$$

se satisface la igualdad $b^2 - 4Nac = \Delta$, de manera que se tiene que $B^2 - \Delta$ es divisible por $4N$. Esto demuestra la propiedad (a). La propiedad (b) se ha visto anteriormente. Además, se tiene que $\mathrm{mcd}\left(N, B, \dfrac{B^2 - \Delta}{4N}\right) = \mathrm{mcd}\left(N, b, \dfrac{b^2 - \Delta}{4N}\right) = m_1 m_2$, lo que demuestra (c). Finalmente, para $a' := a$, $b' := \dfrac{b}{m_1}$, $c' := \dfrac{c}{m_1}$, se tiene que

$$[N'a', b', c'] \in \mathcal{H}(N', \Delta', 1, 1, m_2, B'),$$

hecho que demuestra la última propiedad.

Para demostrar el recíproco, observemos, en primer lugar, que la condición (a) es equivalente a decir que $\dfrac{B^2 - \Delta}{4N} \in \mathbb{Z}$, de manera que tiene sentido considerar $\mathrm{mcd}\left(N, B, \dfrac{B^2 - \Delta}{4N}\right)$. Puesto que, por la hipótesis (c), el producto $m_1 m_2$ divide el cociente $\dfrac{B^2 - \Delta}{4N}$, y teniendo en cuenta (b), podemos escribir $\dfrac{B^2 - \Delta}{4Nm_1m_2} = a'c'$, con $a', c' \in \mathbb{Z}$ tales que $\mathrm{mcd}(a', c') = 1$, $\mathrm{mcd}(a', m_1) = 1$, y $\mathrm{mcd}(c', m_2) = 1$. Para ello, es suficiente colocar en c' todos los factores primos comunes al cociente y a m_1, en a' todos los factores primos comunes al cociente y a m_2, y repartir el resto del cociente en factores primos entre sí. Una vez hecho esto, podemos definir $b := B$, $a := m_2 a'$ y $c := m_1 c'$, y se tiene que

$$[Na, b, c] \in \mathcal{H}(N, \Delta; 1, m_1, m_2, B),$$

de manera que este conjunto es no vacío, como queríamos demostrar. □

Corolario 3.12. *Dada una pareja cualquiera de números enteros (N, Δ), con $N \geq 1$ y Δ un discriminante, condición necesaria y suficiente para que exista alguna inmersión $\lambda : K \longrightarrow \mathbf{M}(2, \mathbb{Q})$ biprimitiva para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ es que exista un número entero B tal que $B^2 \equiv \Delta \pmod{4N}$ y $\mathrm{mcd}\left(N, B, \dfrac{B^2 - \Delta}{4N}\right) = 1$.* □

Observación 3.13. *En general, fijados m_1, m_2 en las condiciones del teorema, la clase de B módulo $2N$ no está determinada. En cambio, si fijamos B y m_1, entonces m_2 está determinado por la igualdad $m_1 m_2 = \mathrm{mcd}\left(N, B, \dfrac{B^2 - \Delta}{4N}\right)$.*

4. CLASIFICACIÓN DE LAS INMERSIONES

Para emprender el estudio de la clasificación de las inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ respecto del grupo $\Gamma_0(N)$, conviene destacar, en primer lugar, el resultado siguiente, que es un corolario inmediato de la definición **3.8**.

Proposición 4.1. *El grupo $\Gamma_0(N)$ actúa en cada uno de los conjuntos $\mathcal{H}(N, \Delta; *, *, *, B)$, $\mathcal{H}(N, \Delta; 1, *, *, B)$, $\mathcal{H}(N, \Delta; 1, m_1, *, B)$, y $\mathcal{H}(N, \Delta; 1, m_1, m_2, B)$.* □

Definición 4.2. *Para cada uno de los conjuntos*

$$\mathcal{H}(N, \Delta; d, m_1, m_2, B),$$

escribiremos

$$H(N, \Delta; d, m_1, m_2, B) := \mathcal{H}(N, \Delta; d, m_1, m_2, B)/\Gamma_0(N)$$

para designar el conjunto de $\Gamma_0(N)$-clases de equivalencia. Y análogamente en caso de no fijar el valor de alguno de los invariantes.

El resultado principal para la clasificación de las inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ es el siguiente teorema de comparación.

Teorema 4.3. *Sean dados un número entero $N \geq 1$, un discriminante $\Delta := \Delta_0 r^2$, $r \geq 1$, asociado al discriminante fundamental Δ_0, y un número entero $B \in \mathbb{Z}$ tal que $B^2 \equiv \Delta \pmod{4N}$. Para cada descomposición $m_1 m_2 = m := \mathrm{mcd}\left(\mathrm{N}, \mathrm{B}, \dfrac{\mathrm{B}^2 - \Delta}{4N}\right)$ tal que $\mathrm{mcd}(m_1, m_2) = 1$, existe una correspondencia biyectiva entre los conjuntos cociente*

$$H(N, \Delta; 1, m_1, m_2, B) \longrightarrow H(1, \Delta; 1).$$

La demostración del teorema sigue de manera esencial ideas esbozadas en **[Gr-Ko-Za 87]**. Comenzaremos por definir la aplicación, para lo cual utilizaremos el resultado siguiente.

Lema 4.4. *Mantengamos las notaciones y las hipótesis del enunciado del teorema.*

(a) Existe alguna descomposición $N = N_1N_2$ *tal que* $N_1, N_2 \geq 1$, *y*

$$\mathrm{mcd}(N_1, N_2) = \mathrm{mcd}(N_1, m_1) = \mathrm{mcd}(N_2, m_2) = 1.$$

(b) Sea $f := [Na, b, c] \in \mathcal{H}(N, \Delta; 1, m_1, m_2, B)$, *cualquiera; entonces, es* $\bar{f} := [N_1a, b, N_2c] \in \bar{\mathcal{H}}(1, \Delta; 1)$.

Demostración. Para la demostración de la propiedad (a), cf. la del teorema **3.11**. Para (b), basta ver que $\mathrm{mcd}(N_1a, b, N_2c) = 1$, hecho que dejamos a la atención del lector. □

Podemos fijar, pues, una descomposición como la del lema, y definir una aplicación

$$\mathcal{H}(N, \Delta; 1, m_1, m_2, B) \xrightarrow{\varphi} \bar{\mathcal{H}}(1, \Delta; 1)$$

por la asignación $f = [Na, b, c] \mapsto \bar{f} = [N_1a, b, N_2c]$. Observemos que, en el caso $m_1 = 1$, podemos tomar $N_1 := N$, $N_2 := 1$, de manera que la aplicación φ sea, sencillamente, la inclusión natural.

Lema 4.5. *La aplicación* φ *define, por paso al cociente, una aplicación*

$$H(N, \Delta; 1, m_1, m_2, B) \xrightarrow{\varphi} H(1, \Delta; 1)$$

entre los conjuntos cociente.

Demostración. Hay que demostrar que si

$$f, f' \in \mathcal{H}(N, \Delta; 1, m_1, m_2, B)$$

son equivalentes por una matriz $P = \begin{bmatrix} \alpha & \beta \\ \gamma N & \delta \end{bmatrix} \in \Gamma_0(N)$, entonces $\bar{f}$, $\bar{f}'$ son equivalentes por una matriz de $\mathbf{SL}(2,\mathbb{Z})$. Sean, pues, $f = [Na,b,c]$, $f' = [Na',b',c']$, y supongamos que se satisfacen las condiciones $\begin{bmatrix} a' \\ b' \\ c' \end{bmatrix} = \mathcal{P} \begin{bmatrix} a \\ b \\ c \end{bmatrix}$. Dicho de otra manera, se satisface el sistema de ecuaciones

$$\begin{aligned} a' &= \alpha^2 a + \alpha\gamma b + \gamma^2 Nc \\ b' &= 2\alpha\beta Na + (1 + 2\beta\gamma N)b + 2\gamma\delta Nc \\ c' &= \beta^2 Na + \beta\delta b + \delta^2 c. \end{aligned}$$

Si multiplicamos la primera ecuación por N_1 y la tercera por N_2, obtenemos el sistema equivalente

$$\begin{aligned} N_1a' &= \alpha^2 N_1 a + \alpha(\gamma N_1)b + (\gamma N_1)^2 N_2 c \\ b' &= 2\alpha(\beta N_2)N_1 a + \big(1 + 2(\beta N_2)(\gamma N_1)\big)b + 2(\gamma N_1)\delta N_2 c \\ N_2c' &= (\beta N_2)^2 N_1 a + (\beta N_2)\delta b + \delta^2 N_2 c, \end{aligned}$$

de manera que las matrices $\bar{f} = [N_1a, b, N_2c]$ y $\bar{f}' = [N_1a', b', N_2c']$ son $\mathbf{SL}(2, \mathbb{Z})$-equivalentes por la matriz

$$\begin{bmatrix} \alpha & \beta N_2 \\ \gamma N_1 & \delta \end{bmatrix},$$

como queríamos demostrar. □

Lema 4.6. *La aplicación*

$$\varphi : H(N, \Delta; 1, m_1, m_2, B) \longrightarrow H(1, \Delta; 1)$$

es inyectiva.

Demostración. Supongamos que $\bar{f}$ es $\mathbf{SL}(2,\mathbb{Z})$-equivalente con $\bar{f}'$; es decir, que para una matriz $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix} \in \mathbf{SL}(2, \mathbb{Z})$, se satisface el sistema

$$\begin{aligned} N_1a' &= \alpha^2 N_1 a + \alpha\gamma b + \gamma^2 N_2 c, \\ b' &= 2\alpha\beta N_1 a + (1 + 2\beta\gamma)b + 2\gamma\delta N_2 c, \\ N_2c' &= \beta^2 N_1 a + \beta\delta b + \delta^2 N_2 c. \end{aligned}$$

Teniendo en cuenta la demostración del lema anterior, basta ver que γ es divisible por N_1, y β, por N_2.

Ahora bien, la primera ecuación nos dice que N_1 divide el producto $\gamma(\alpha b + \gamma N_2 c)$; y, puesto que $2N_1$ divide $2N$ y $2N$ divide $b' - b$ (ya que $b' \equiv b \equiv B \pmod{2N}$), la segunda ecuación nos dice que N_1 divide el producto $\gamma(\beta b + \delta N_2 c)$. Teniendo en cuenta que $\alpha\delta - \beta\gamma = 1$, obtenemos que N_1 divide los productos γb y $\gamma N_2 c$; y, puesto que $\mathrm{mcd}(N_1, N_2) = 1$, tenemos que N_1 divide los productos $\gamma\, b$ y $\gamma\, c$; y, evidentemente, N_1 divide el producto $\gamma\, N_1 a$. Finalmente, puesto que $\mathrm{mcd}(N_1a, b, c) = 1$, obtenemos que N_1 debe dividir γ. La cuestión de divisibilidad de β por N_2 es completamente análoga, al tener en cuenta las dos últimas ecuaciones. □

Lema 4.7. *La aplicación*

$$\varphi : H(N, \Delta; 1, m_1, m_2, B) \longrightarrow H(1, \Delta; 1)$$

es exhaustiva.

Demostración. Consideremos una matriz cualquiera $\bar{f} := [\bar{a}, \bar{b}, \bar{c}] \in \bar{\mathcal{H}}(1, \Delta; 1)$ y veamos que existen α, β, γ,

$\delta \in \mathbb{Z}$ tales que $\alpha\delta - \beta\gamma = 1$ y que para los números enteros a, b, c definidos por

$$\begin{aligned} a &= \alpha^2\bar{a} + \alpha\gamma\bar{b} + \gamma^2\bar{c}, \\ b &= 2\alpha\beta\bar{a} + (1 + 2\beta\gamma)\bar{b} + 2\gamma\delta\bar{c}, \\ c &= \beta^2\bar{a} + \beta\delta\bar{b} + \delta^2\bar{c}, \end{aligned}$$

se satisfacen las propiedades que c es divisible por N_2, a lo es por N_1, y que la matriz $\left[N_2 a,\ b,\ \dfrac{c}{N_2}\right]$ pertenece a $\mathcal{H}(N, \Delta; 1, m_1, m_2, B)$.

Tengamos en cuenta, en primer lugar, que se tiene que $B^2 \equiv \Delta \pmod{4N}$, de manera que $B \equiv \Delta \pmod 2$, y que $\bar{b} \equiv \Delta \pmod 2$, puesto que $\bar{b}^2 - 4\bar{a}\,\bar{c} = \Delta$; por tanto, $\bar{b} \equiv B \pmod 2$. Así, podemos escribir las ecuaciones anteriores en la forma equivalente siguiente:

$$a = \alpha\left(\alpha\bar{a} + \gamma\,\frac{\bar{b}+B}{2}\right) + \gamma\left(\alpha\,\frac{\bar{b}-B}{2} + \gamma\,\bar{c}\right),$$

$$\begin{aligned} b &= B + 2\beta\left(\alpha\bar{a} + \gamma\,\frac{\bar{b}+B}{2}\right) + 2\delta\left(\alpha\,\frac{\bar{b}-B}{2} + \gamma\bar{c}\right) = \\ &= B + 2\alpha\left(\beta\bar{a} + \delta\,\frac{\bar{b}-B}{2}\right) + 2\gamma\left(\beta\,\frac{\bar{b}+B}{2} + \delta\bar{c}\right), \end{aligned}$$

$$c = \beta\left(\beta\bar{a} + \delta\,\frac{\bar{b}-B}{2}\right) + \delta\left(\beta\,\frac{\bar{b}+B}{2} + \delta\,\bar{c}\right);$$

y veamos que se pueden encontrar números enteros α, β, γ, δ, tales que

$$\begin{aligned} &\alpha\delta - \beta\gamma = 1, \\ &\alpha\bar{a} + \gamma\,\frac{\bar{b}+B}{2} \equiv 0 \pmod{N_1}, \\ (*)\qquad &\alpha\,\frac{\bar{b}-B}{2} + \gamma\bar{c} \equiv 0 \pmod{N_1}, \\ &\beta\bar{a} + \delta\,\frac{\bar{b}-B}{2} \equiv 0 \pmod{N_2}, \\ &\beta\,\frac{\bar{b}+B}{2} + \delta\,\bar{c} \equiv 0 \pmod{N_2}. \end{aligned}$$

Observemos que el determinante de las matrices

$$\begin{bmatrix} \bar{a} & \dfrac{\bar{b}+B}{2} \\ \dfrac{\bar{b}-B}{2} & \bar{c} \end{bmatrix}, \quad \begin{bmatrix} \bar{a} & \dfrac{\bar{b}-B}{2} \\ \dfrac{\bar{b}+B}{2} & \bar{c} \end{bmatrix},$$

es divisible por N; en particular, por N_1 y por N_2. Por otra parte, se tiene que $\operatorname{mcd}\left(\bar{a}, \dfrac{\bar{b}+B}{2}, \dfrac{\bar{b}-B}{2}, \bar{c}\right) = 1$, puesto que $\operatorname{mcd}(\bar{a}, \bar{b}, \bar{c}) = 1$.

Vamos a resolver el sistema de ecuaciones

$$\begin{bmatrix} \bar{a} & \dfrac{\bar{b}+B}{2} \\ \dfrac{\bar{b}-B}{2} & \bar{c} \end{bmatrix} \begin{bmatrix} \alpha \\ \gamma \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{N_1}$$

por aplicación del teorema chino del resto.

Sean $p \geq 1$ un número primo que divida N_1 y $v \geq 1$ la valoración p-ádica de N_1. Existen α_p, $\gamma_p \in \mathbb{Z}$ tales que p no divide α_p o bien p no divide γ_p, y tales que

$$\begin{bmatrix} \bar{a} & \dfrac{\bar{b}+B}{2} \\ \dfrac{\bar{b}-B}{2} & \bar{c} \end{bmatrix} \begin{bmatrix} \alpha_p \\ \gamma_p \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{p^v};$$

para ello, observemos que alguno de los cuatro coeficientes del sistema no es divisible por p, de manera que la ecuación correspondiente se puede resolver haciendo igual a 1 $(\operatorname{mod} p^v)$ la incógnita que corresponde al otro coeficiente. En particular, alguno de los α_p, γ_p es inversible módulo p^v, de manera que podemos elegir β_p, $\delta_p \in \mathbb{Z}$ tales que $\alpha_p\delta_p - \beta_p\gamma_p \equiv 1 \pmod{p^v}$. Ahora, podemos elegir α_1, β_1, γ_1, $\delta_1 \in \mathbb{Z}$ tales que $\alpha_1 \equiv \alpha_p \pmod{p^v}$, $\beta_1 \equiv \beta_p \pmod{p^v}$, $\gamma_1 \equiv \gamma_p \pmod{p^v}$, $\delta_1 \equiv \delta_p \pmod{p^v}$, para todos los primos que dividan N_1. En particular, se tiene que para α_1, β_1, γ_1, $\delta_1 \in \mathbb{Z}$ se satisface el sistema

$$\begin{bmatrix} \bar{a} & \dfrac{\bar{b}+B}{2} \\ \dfrac{\bar{b}-B}{2} & \bar{c} \end{bmatrix} \begin{bmatrix} \alpha_1 \\ \gamma_1 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{N_1},$$

junto con la ecuación $\alpha_1\delta_1 - \beta_1\gamma_1 \equiv 1 \pmod{N_1}$.

Análogamente, existen α_2, β_2, γ_2, $\delta_2 \in \mathbb{Z}$ tales que

$$\begin{bmatrix} \bar{a} & \dfrac{\bar{b}+B}{2} \\ \dfrac{\bar{b}-B}{2} & \bar{c} \end{bmatrix} \begin{bmatrix} \beta_2 \\ \delta_2 \end{bmatrix} \equiv \begin{bmatrix} 0 \\ 0 \end{bmatrix} \pmod{N_1}$$

y $\alpha_2\delta_2 - \beta_2\gamma_2 \equiv 1 \pmod{N_2}$.

Finalmente, podemos elegir α, β, γ, $\delta \in \mathbb{Z}$ tales que $\alpha \equiv \alpha_i \pmod{N_i}$, $\beta \equiv \beta_i \pmod{N_i}$, $\gamma \equiv \gamma_i \pmod{N_i}$, $\delta \equiv \delta_i \pmod{N_i}$, $i = 1, 2$. En particular, se tiene que $\alpha\delta - \beta\gamma \equiv 1 \pmod N$; y, por la exhaustividad del morfismo de reducción módulo N

$$\mathbf{SL}(2, \mathbb{Z}) \to \mathbf{SL}(2, \mathbb{Z}/N\mathbb{Z}),$$

podemos elegirlos de manera que sea $\alpha\delta - \beta\gamma = 1$.

Así, pues, hemos obtenido una solución del sistema $(*)$. Sólo queda por ver que $\left[N_2 a,\ b,\ \dfrac{c}{N_2}\right] \in \mathcal{H}(N, \Delta; 1, m_1,$

m_2, B). Para ello, observemos que c es divisible por N_2, y a es divisible por N_1, de manera que $\frac{a}{N_1}$, b, $\frac{c}{N_2} \in \mathbb{Z}$ y $N_2 a$ es divisible por N; además, puesto que la matriz $\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}$ pertenece a $\mathbf{SL}(2, \mathbb{Z})$, tenemos que $b^2 - 4N \frac{a}{N_1} \frac{c}{N_2} = b^2 - 4ac = \bar{b}^2 - 4\bar{a}\bar{c} = -\Delta$. Por otra parte, tenemos que $b \equiv B \pmod{2N}$, en virtud de la segunda de las ecuaciones. Finalmente, tenemos que $\operatorname{mcd}\left(\frac{a}{N_1}, b, \frac{c}{N_2}\right) = 1$, $\operatorname{mcd}\left(N\frac{a}{N_1}, b, \frac{c}{N_2}\right) = m_1$, y $\operatorname{mcd}\left(\frac{a}{N_1}, b, N\frac{c}{N_2}\right) = m_2$. En efecto; a partir del hecho que

$$\operatorname{mcd}(a, b, c) = \operatorname{mcd}(\bar{a}, \bar{b}, \bar{c}) = 1,$$

obtenemos que $\operatorname{mcd}\left(\frac{a}{N_1}, b, \frac{c}{N_2}\right) = 1$; y, también, que $\operatorname{mcd}\left(N_2 a, b, \frac{c}{N_2}\right)$ divide N_2 y, en particular, es primo con m_2; y que $\operatorname{mcd}\left(\frac{a}{N_1}, b, N_1 c\right)$ divide N_1 y, en particular, es primo con m_1; además, puesto que

$$\operatorname{mcd}\left(N, b, \frac{a}{N_1}\frac{c}{N_2}\right) = \operatorname{mcd}\left(N, b, \frac{ac}{N}\right) =$$

$$= \operatorname{mcd}\left(N, b, \frac{b^2 - \Delta}{4N}\right) = \operatorname{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right) = m_1 m_2,$$

se tienen las dos propiedades restantes.

Así, pues, tenemos que

$$f := \left[N\frac{a}{N_1}, b, \frac{c}{N_2}\right] \in \mathcal{H}(N, \Delta; 1, m_1, m_2, B)$$

y que $\varphi(f) = [a, b, c]$, que es $\mathbf{SL}(2, \mathbb{Z})$-equivalente a la matriz $\bar{f}$. Por tanto, la aplicación $\varphi : H(N, \Delta; 1, m_1, m_2, B) \to H(1, \Delta; 1)$ es exhaustiva. □

Con este lema, hemos acabado la demostración del teorema de clasificación de las inmersiones optimales. Ahora, obtenemos fácilmente la clasificación de las inmersiones enteras a partir del resultado siguiente.

Proposición 4.8. *Sea $d \geq 1$ un divisor de r, donde $\Delta = \Delta_0 r^2$. Existe una correspondencia biyectiva entre el conjunto $H(N, \Delta; d, *, *, *)$, de clases de $\Gamma_0(N)$-equivalencia de inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ tales que $\operatorname{mcd}(a, b, c) = d$, y el conjunto $H\left(N, \frac{\Delta}{d^2}; 1, *, *, *\right)$, de clases de $\Gamma_0(N)$-equivalencia de inmersiones optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta/d^2})$.*

Demostración. Notemos, en primer lugar, que $d := \operatorname{mcd}(a, b, c)$ es invariante para las clases de $\Gamma_0(N)$-equivalencia de inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, y que d es un divisor de r (donde $\Delta = \Delta_0 r^2$). Por otra parte, dada una inmersión $f = [Na, b, c] \in \mathcal{H}(N, \Delta; d, *, *, *)$, la inmersión $\frac{f}{d} = \left[N\frac{a}{d}, \frac{b}{d}, \frac{c}{d}\right]$ es optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta/d^2})$, es decir, pertenece a $\mathcal{H}\left(N, \frac{\Delta}{d^2}; 1, *, *, *\right)$. Y si f' es una inmersión $\Gamma_0(N)$-equivalente a f, entonces $\frac{f'}{d}$ es $\Gamma_0(N)$-equivalente a $\frac{f}{d}$, como inmersiones optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta/d^2})$. Por tanto, la asignación $f \mapsto \frac{f}{d}$ define, por paso al cociente, una aplicación

$$H(N, \Delta; d, *, *, *) \to H\left(N, \frac{\Delta}{d^2}; 1, *, *, *\right).$$

Además, si $f, f' \in \mathcal{H}(N, \Delta; d, *, *, *)$ son tales que $\frac{f'}{d}$ y $\frac{f}{d}$ son $\Gamma_0(N)$-equivalentes como inmersiones optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta/d^2})$, entonces f y f' son $\Gamma_0(N)$-equivalentes como inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. Por tanto, esta aplicación es inyectiva. Y, finalmente, dada una inmersión

$$g := [Na, b, c] \in \mathcal{H}\left(N, \frac{\Delta}{d^2}; 1, *, *, *\right),$$

la inmersión $dg = [Nad, bd, cd]$ pertenece a $\mathcal{H}(N, \Delta; d, *, *, *)$, de manera que la aplicación es exhaustiva. □

Finalmente, nos preocupamos del descenso de nivel para las inmersiones primitivas, que obtenemos como corolario del teorema de comparación **4.3**. Ya hemos visto, en el corolario **2.9**, que una inmersión primitiva para una pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ es automáticamente primitiva para la pareja $(\mathcal{O}_0(N'), \mathcal{O}_\Delta)$, para cualquier divisor $N' \geq 1$ de N; es decir, se tiene una inclusión

$$\mathcal{H}(N, \Delta; 1, 1, *, B) \to \mathcal{H}(N', \Delta; 1, 1, *, B')$$

para cada número entero $B' \equiv B \pmod{2N'}$.

Corolario 4.9. *Sea $N' \geq 1$ un divisor cualquiera de N. Para cada número entero B, sea $B' \in \mathbb{Z}$ tal que $B \equiv B' \pmod{2N'}$. La inclusión*

$$\mathcal{H}(N, \Delta; 1, 1, *, B) \to \mathcal{H}(N', \Delta; 1, 1, *, B')$$

define, por paso al cociente, una aplicación natural biyectiva

$$H(N, \Delta; 1, 1, *, B) \to H(N', \Delta; 1, 1, *, B').$$

Demostración. Puesto que estamos en el caso $m_1 = 1$, podemos elegir las descomposiciones $N = N_1N_2$, $N' = N_1'N_2'$ del lema **4.4** de manera que sea $N_2 = N_2' = 1$, $N_1 = N$, y $N_1' = N'$. De esta manera, las aplicaciones φ, φ' de la demostración del teorema son las inclusiones naturales

$$\mathcal{H}(N, \Delta; 1, 1, *, B) \to \mathcal{H}(1, \Delta; 1),$$
$$\mathcal{H}(N', \Delta; 1, 1, *, B') \to \mathcal{H}(1, \Delta; 1),$$

la primera de las cuales es la composición de la inclusión

$$\mathcal{H}(N, \Delta; 1, 1, *, B) \to \mathcal{H}(N', \Delta; 1, 1, *, B')$$

con la segunda. El teorema **4.3** nos asegura que, por paso al cociente, obtenemos biyecciones

$$H(N, \Delta; 1, 1, *, B) \to H(1, \Delta; 1),$$
$$H(N', \Delta; 1, 1, *, B') \to H(1, \Delta; 1);$$

puesto que la inclusión natural

$$\mathcal{H}(N, \Delta; 1, 1, *, B) \to \mathcal{H}(N', \Delta; 1, 1, *, B')$$

pasa al cociente, obtenemos que

$$H(N, \Delta; 1, 1, *, B) \to H(N', \Delta; 1, 1, *, B')$$

es biyectiva, como queríamos ver. □

5. NÚMEROS DE CLASES

En esta sección, procedemos a calcular los cardinales de los conjuntos de clases de equivalencia de inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras, optimales, primitivas y biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Dado un discriminante $\Delta = \Delta_0 r^2$, $r \geq 1$, asociado al discriminante fundamental Δ_0, escribiremos $h(\Delta)$ para designar el número de clases de equivalencia estricta (es decir, módulo la acción del grupo $\Gamma_0(1) = \mathbf{SL}(2,\mathbb{Z})$) de formas cuadráticas binarias, enteras, primitivas, y de discriminante Δ.

Observación 5.1. *Notemos que el número $h(\Delta)$ tiene en cuenta todas las formas cuadráticas binarias primitivas de discriminante Δ. En particular, cuando $\Delta < 0$, tiene en cuenta las formas definidas positivas y las formas definidas negativas.*

Teorema 5.2. *Sean N, Δ, B, d, m_1, $m_2 \in \mathbb{Z}$ números enteros tales que N, d, m_1, $m_2 \geq 1$, $\Delta = \Delta_0 r^2$, $r \geq 1$, es un discriminante asociado al discriminante fundamental Δ_0, $B^2 \equiv \Delta \pmod{4N}$, $\mathrm{mcd}(m_1, m_2) = 1$, y $\mathrm{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right) = m_1m_2$. Además, sean $S(N, \Delta, B) := 2^{s(N, \Delta, B)}$, donde $s(N, \Delta, B)$ denota el número de divisores primos positivos distintos de $\mathrm{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right)$;*

$$r^*(N, \Delta) := \#\{B \pmod{2N} : B^2 \equiv \Delta \pmod{4N}\};$$
$$s^*(N, \Delta) := \#\{B \pmod{2N} : B^2 \equiv \Delta \pmod{4N},$$
$$\mathrm{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right) = 1\}.$$

Los conjuntos de clases de $\Gamma_0(N)$-equivalencia de inmersiones enteras, optimales, primitivas y biprimitivas para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ son finitos. Además, para sus cardinales, se tienen las fórmulas siguientes:

(a) $\#H(N, \Delta; 1, m_1, m_2, B) = h(\Delta)$.

(b) $\#H(N, \Delta; 1, *, *, B) = h(\Delta)S(N, \Delta, B)$.

(c) (Biprimitivas) $\#H(N, \Delta; 1, 1, 1, *) = h(\Delta)s^*(N, \Delta)$.

(d) (Primitivas) $\#H(N, \Delta; 1, 1, *, *) = h(\Delta)r^*(N, \Delta)$.

(e) (Optimales) $\#H(N, \Delta; 1, *, *, *) = h(\Delta) \sum_{\substack{d \mid N \\ d \mid r \\ \square \nmid d}} r^*\left(\frac{N}{d}, \frac{\Delta}{d^2}\right)$.

(f) (Enteras) $\#H(N, \Delta) = \sum_{d \mid r} h(\Delta_0 d^2) \sum_{\substack{\delta \mid N \\ \delta \mid r \\ \square \nmid \delta}} r^*\left(\frac{N}{\delta}, \frac{\Delta_0 d^2}{\delta^2}\right)$.

Demostración. El teorema **3.11** nos dice que si no se satisfacen las condiciones requeridas en (a), el conjunto $H(N, \Delta; 1, m_1, m_2, B)$ es vacío; en consecuencia, el teorema **4.3** proporciona (a).

Para demostrar (b), observemos que, si $B^2 \not\equiv \Delta \pmod{4N}$, el conjunto $H(N, \Delta; 1, *, *, B)$ es vacío. En caso contrario, $H(N, \Delta; 1, *, *, B)$ es la reunión disjunta de los conjuntos $H(N, \Delta; 1, m_1, m_2, B)$, para todas las descomposiciones $\mathrm{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right) = m_1m_2$, tales que $m_1, m_2 \geq 1$ y $\mathrm{mcd}(m_1, m_2) = 1$. Aplicando (a), basta observar que $S(N, \Delta, B)$ es el número de divisores de $\mathrm{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right)$ libres de cuadrados o, equivalentemente, de descomposiciones como las que deseamos.

Veamos, ahora, (c) y (d). Para ello, observemos que el conjunto $H(N, \Delta; 1, 1, *, *)$ es la reunión disjunta de los $H(N, \Delta; 1, 1, *, B)$ para los valores de $B \pmod{2N}$ tales que $B^2 \equiv \Delta \pmod{4N}$. Además, puesto que $m_1 = 1$, el valor de m_2 debe coincidir con $\mathrm{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right)$; por tanto, para $m_2 := \mathrm{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right)$, se tiene que $H(N, \Delta; 1, 1, *, B) = H(N, \Delta; 1, 1, m_2, B) = h(\Delta)$. Para demostrar la igualdad enunciada en (d) basta observar, pues, la definición del factor $r^*(N, \Delta)$. Y, para (c), basta repetir el cálculo anterior para los valores de B tales que, además, es $m_2 = 1$, hecho que substituye el factor $r^*(N; \Delta)$ por $s^*(N; \Delta)$.

Demostremos (e). El conjunto $H(N, \Delta; 1, *, *, *)$ es la reunión disjunta de los conjuntos $H(N, \Delta; 1, *, *, B)$, para $B \pmod{2N}$ tal que $B^2 \equiv \Delta \pmod{4N}$. Por tanto, podemos escribir

$$\#H(N, \Delta; 1, *, *, *) = \sum_{\substack{B \pmod{2N} \\ B^2 \equiv \Delta \pmod{4N}}} \#H(N, \Delta; 1, *, *, B).$$

Ahora, aplicaremos (b), teniendo en cuenta que $S(N, \Delta, B)$ es el número de divisores libres de cuadrados de $\mathrm{mcd}\left(N, B, \frac{B^2-\Delta}{4N}\right)$ y, por tanto, la suma anterior es el cardinal del conjunto de pares (B, d) tales que $B \pmod{2N}$, $B^2 \equiv \Delta \pmod{4N}$, $d \mid N$, d libre de cuadrados, y d divide $\mathrm{mcd}\left(N, B, \frac{B^2-\Delta}{4N}\right)$. Esta última condición es equivalente, al tener en cuenta las demás, a la condición $d \mid r$ y $B^2 \equiv \Delta \pmod{4dN}$. En efecto; si d es libre de cuadrados y divide $\mathrm{mcd}\left(N, B, \frac{B^2-\Delta}{4N}\right)$, tenemos que d divide N y B, y que $B^2 \equiv \Delta \pmod{4dN}$; puesto que d^2 divide $4dN$ y B^2, tenemos que d^2 divide Δ, y la presencia del factor 4 en el módulo implica que d divide r. Recíprocamente, si d divide r y $B^2 \equiv \Delta \pmod{4dN}$, entonces d^2 divide Δ y B^2; puesto que d es libre de cuadrados, tenemos que d divide N y B, y la condición $B^2 \equiv \Delta \pmod{4dN}$ nos dice que d divide $\frac{B^2-\Delta}{4N}$; es decir, d divide $\mathrm{mcd}\left(N, B, \frac{B^2-\Delta}{4N}\right)$. Así, el valor de la suma anterior es

$$\#\{(B, d) : B \pmod{2N},\ B^2 \equiv \Delta \pmod{4dN},\ d \mid N,\ \square \nmid d,\ d \mid r\}.$$

Sumando para d, obtenemos que $\#H(N, \Delta; 1, *, *, *)$ es dado por la expresión

$$h(\Delta) \sum_{\substack{d \mid N \\ d \mid r \\ \square \nmid d}} \#\{B \pmod{2N} : B^2 \equiv \Delta \pmod{4dN}\}.$$

En consecuencia, si ponemos $B' := \frac{B}{d}$, $\Delta' := \frac{\Delta}{d^2}$, y $N' := \frac{N}{d}$, al dividir la congruencia por d^2, obtenemos que

$$\#\{B \pmod{2N} : B^2 \equiv \Delta \pmod{4dN}\}$$

coincide con

$$\#\{B' \pmod{2N'} : B'^2 \equiv \Delta' \pmod{4N'}\} = r^*\left(\frac{N}{d}, \frac{\Delta}{d^2}\right),$$

como queríamos demostrar.

Finalmente, para demostrar (f), observemos que la proposición **4.8** permite reducir el cálculo del número de clases de inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ al de las clases de inmersiones optimales para las parejas $(\mathcal{O}_0(N), \mathcal{O}_{\Delta/d^2})$, para todos los divisores d de r. En efecto; se tiene que

$$\mathcal{H}(N, \Delta) = \bigcup_{d \mid r} d\mathcal{H}\left(N, \frac{\Delta}{d^2}; 1, *, *, *\right),$$

con la reunión disjunta y $\Gamma_0(N)$-invariante; por tanto,

$$\#H(N, \Delta) = \sum_{d \mid r} \#H\left(N, \frac{\Delta}{d^2}; 1, *, *, *\right) =$$

$$= \sum_{d \mid r} \#H(N, \Delta_0 d^2; 1, *, *, *).$$

Basta, pues, aplicar (e). □

A continuación, procedemos al cálculo explícito de los números $r^*(N, \Delta)$ y $s^*(N, \Delta)$, lo que permite precisar las fórmulas para los números de clases.

Definición 5.3. *Dados números enteros $N \geq 1$, y Δ cualquiera, sean $R^*(N, \Delta)$ el número de raíces cuadradas de Δ módulo N, y $S^*(N, \Delta)$ el número de éstas, $B \pmod{N}$, tales que* $\mathrm{mcd}\left(N', B, \frac{B^2-\Delta}{N}\right) = 1$, *donde* $N' := \frac{N}{\mathrm{mcd}(4, N)}$.

Lema 5.4. *Sea $N = \prod_p p^{v_p}$ la descomposición en factores primos de un número entero cualquiera $N \geq 1$; es decir, para cada número primo $p \geq 2$, sea $v_p := v_p(N)$ la valoración p-ádica de N, y pongamos $v'_p := v_p(N')$, donde $N' := \frac{N}{\mathrm{mcd}(4, N)}$. Para todo número entero Δ, se satisface que*

$$R^*(N, \Delta) = \prod_{p \mid N} R^*(p^{v_p}, \Delta), \qquad S^*(N, \Delta) = \prod_{p \mid N} S^*(p^{v_p}, \Delta).$$

Demostración. El teorema chino del resto proporciona inmediatamente la igualdad para $R^*(N, \Delta)$. Para $S^*(N, \Delta)$, basta observar que la condición $\mathrm{mcd}\left(N', B, \frac{B^2-\Delta}{N}\right) = 1$ equivale a decir que, para todo primo p que divide N, p no divide $\mathrm{mcd}\left(p^{v'_p}, B, \frac{B^2-\Delta}{p^{v_p}}\right)$. □

Corolario 5.5. *Sean $N \geq 1$, y Δ un discriminante. Entonces,*

$$r^*(N, \Delta) = \frac{1}{2} R^*(4N, \Delta),$$

$$s^*(N, \Delta) = \frac{1}{2} S^*(4N, \Delta).$$

Demostración. La definición de $r^*(N, \Delta)$ como el cardinal del conjunto $\{B \pmod{2N} : B^2 \equiv \Delta \pmod{4N}\}$, la observación que, para un número entero B, la propiedad $B^2 \equiv \Delta \pmod{4N}$ es equivalente a la propiedad $(B + 2N)^2 \equiv \Delta \pmod{4N}$, y el hecho que $B \not\equiv B + 2N \pmod{4N}$, pero $B \equiv B + 2N \pmod{2N}$, proporcionan la primera fórmula. Obtenemos la segunda análogamente, puesto que, además, se satisface la igualdad

$$\operatorname{mcd}\left(N, B + 2N, \frac{(B + 2N)^2 - \Delta}{4N}\right) = \operatorname{mcd}\left(N, B, \frac{B^2 - \Delta}{4N}\right). \square$$

Hemos reducido, pues, el cálculo de los factores $r^*(N, \Delta)$ y $s^*(N, \Delta)$ al de los números $R^*(p^{v_p}, \Delta)$ y $S^*(p^{v_p}, \Delta)$, para todo número primo $p \neq 2$ y de $R^*(2^{2+v_2}, \Delta)$ y $S^*(2^{2+v_2}, \Delta)$, para $p = 2$, donde $v_p := v_p(N)$.

El valor de los factores $R^*(p^{v_p}, \Delta)$ es conocido. Pero, teniendo en cuenta que hay que calcular, también, los factores $S^*(p^{v_p}, \Delta)$, y que éste cálculo está basado en el anterior, los haremos ambos conjuntamente. Por comodidad de notación, escribiremos $w_p := \left[\frac{v_p}{2}\right]$, la parte entera de $\frac{v_p}{2}$. En particular, v_p es par si, y sólo si, $v_p = 2w_p$; y v_p es impar si, y sólo si, $v_p = 2w_p + 1$. Por otra parte, convendrá tener en cuenta la paridad de $t_p := v_p(\Delta)$. Escribiremos $r_p := \left[\frac{t_p}{2}\right]$, la parte entera de $\frac{t_p}{2}$, y $\Delta = p^{t_p}\Delta'_p$, de manera que p no divide Δ'_p.

Proposición 5.6. *Sean Δ un número entero cualquiera, $p \geq 2$ un número primo, y $v_p \geq 0$ un número entero. Entonces:*

(1) El valor de $R^*(p^{v_p}, \Delta)$ es el dado por:

- *Si $v_p = 0$, p cualquiera, $R^*(p^{v_p}, \Delta) = 1$.*
- *Si $1 \leq v_p \leq v_p(\Delta)$, p cualquiera, $R^*(p^{v_p}, \Delta) = p^{w_p}$.*
- *Si $v_p > v_p(\Delta) = 2r_p + 1$, p cualquiera, $R^*(p^{v_p}, \Delta) = 0$.*
- Si $p \neq 2$ y $v_p > v_p(\Delta) = 2r_p$,

$$R^*(p^{v_p}, \Delta) = \begin{cases} 0, & si \left(\frac{\Delta'_p}{p}\right) = -1, \\ 2p^{r_p}, & si \left(\frac{\Delta'_p}{p}\right) = 1. \end{cases}$$

- *Si $p = 2$ y $v_2 > v_2(\Delta) = 2r_2$,*

$$R^*(2^{v_2}, \Delta) = \begin{cases} 2^{r_2}, & \text{si } v_2 - 2r_2 = 1, \\ 0, & si\ v_2 - 2r_2 \geq 2,\ \Delta'_2 \equiv 3 \pmod 4, \\ 2^{1+r_2}, & si\ v_2 - 2r_2 = 2,\ \Delta'_2 \equiv 1 \pmod 4, \\ 0, & si\ v_2 - 2r_2 \geq 3,\ \Delta'_2 \equiv 5 \pmod 8, \\ 2^{2+r_2}, & si\ v_2 - 2r_2 \geq 3,\ \Delta'_2 \equiv 1 \pmod 8. \end{cases}$$

(2) Y el valor de $S^*(p^{v_p}, \Delta)$ es el dado por:

- *Si $v_p = 0$, p cualquiera, $S^*(p^{v_p}, \Delta) = 1$.*
- *Si $1 \leq v_p < v_p(\Delta)$, $p \neq 2$,*

$$S^*(p^{v_p}, \Delta) = \begin{cases} p^{w_p - 1}(p - 1), & si\ v_p = 2w_p, \\ 0, & si\ v_p = 2w_p + 1. \end{cases}$$

- *Si $p = 2$ y $1 \leq v_2 < v_2(\Delta)$,*

$$S^*(2^{v_2}, \Delta) = \begin{cases} 2^{w_2}, & si\ 1 \leq v_2 \leq 2, \\ 2^{w_2 - 1}, & si\ v_2 = 2w_2 > 3, \\ 0, & si\ v_2 = 2w_2 + 1 \geq 3. \end{cases}$$

- *Si $p \neq 2$ y $1 \leq v_p = v_p(\Delta)$,*

$$S^*(p^{v_p}, \Delta) = \begin{cases} p^{r_p}, & si\ v_p = 2w_p + 1, \\ p^{r_p}, & si\ v_p = 2w_p, \left(\frac{\Delta'_p}{p}\right) = -1, \\ p^{r_p - 1}(p - 2), & si\ v_p = 2w_p, \left(\frac{\Delta'_p}{p}\right) = 1. \end{cases}$$

- *Si $p = 2$ y $1 \leq v_2 = v_2(\Delta)$,*

$$S^*(2^{v_2}, \Delta) = \begin{cases} 2^{r_2}, & si\ v_2 = 2r_2 + 1, \\ 2, & si\ v_2 = 2, \\ 2^{r_2 - 1}, & si\ v_2 = 2r_2 > 3. \end{cases}$$

- *Si $v_p > v_p(\Delta) = 2r_p + 1$, p cualquiera, $S^*(p^{v_p}, \Delta) = 0$.*
- *Si $p \neq 2$ y $v_p > v_p(\Delta) = 2r_p$,*

$$S^*(p^{v_p}, \Delta) = \begin{cases} 0, & si \left(\frac{\Delta'_p}{p}\right) = -1, \\ 2, & si\ r_p = 0, \left(\frac{\Delta'_p}{p}\right) = 1, \\ 2p^{r_p - 1}(p - 1), & si\ r_p \neq 0, \left(\frac{\Delta'_p}{p}\right) = 1. \end{cases}$$

- *Si $p = 2$ y $v_2 > v_2(\Delta) = 0$,*

$$S^*(2^{v_2}, \Delta) = \begin{cases} 1, & si\ v_2 = 1, \\ 0, & si\ v_2 \geq 2, \Delta \equiv 3 \pmod 4, \\ 2, & si\ v_2 = 2, \Delta \equiv 1 \pmod 4, \\ 0, & si\ v_2 \geq 3, \Delta \equiv 5 \pmod 8, \\ 4, & si\ v_2 \geq 3, \Delta \equiv 1 \pmod 8. \end{cases}$$

• *Si* $p = 2$ *y* $v_2 > v_2(\Delta) = 2r_2 > 0$,

$$S^*(2^{v_2}, \Delta) = \begin{cases} 2^{r_2}, & si\ \Delta_2' \equiv 3 \pmod 4,\ v_2 - 2r_2 = 1, \\ 0, & si\ \Delta_2' \equiv 3 \pmod 4,\ v_2 - 2r_2 \geq 2, \\ 0, & si\ \Delta_2' \equiv 1 \pmod 4,\ v_2 - 2r_2 = 1, \\ 2^{1+r_2}, & si\ \Delta_2' \equiv 5 \pmod 8,\ v_2 - 2r_2 = 2, \\ 0, & si\ \Delta_2' \equiv 5 \pmod 8,\ v_2 - 2r_2 \geq 3, \\ 0, & si\ \Delta_2' \equiv 1 \pmod 8,\ v_2 - 2r_2 = 2, \\ 2^{1+r_2}, & si\ \Delta_2' \equiv 1 \pmod 8,\ v_2 - 2r_2 \geq 3. \end{cases}$$

Demostración. Para todo número primo p, hay que calcular el número de soluciones $B \pmod{p^{v_p}}$ de la congruencia $B^2 \equiv \Delta \pmod{p^{v_p}}$ y el número de soluciones $B \pmod{p^{v_p}}$ tales que $\mathrm{mcd}\left(p^{v_p'}, B, \dfrac{B^2-\Delta}{p^{v_p}}\right)$ no es divisible por p, donde $v_p' = v_p$, si $p \neq 2$, y $v_2' := \max(0, v_2 - 2)$.

Escribamos $\Delta = p^{t_p}\Delta_p'$, con $t_p := v_p(\Delta) \geq 0$, de manera que $\Delta_p' \in \mathbb{Z}$ no es divisible por p. Entonces, la congruencia $B^2 \equiv \Delta \pmod{p^{v_p}}$ se puede escribir en la forma equivalente $B^2 \equiv p^{t_p}\Delta_p' \pmod{p^{v_p}}$.

Haremos el cálculo por distinción de casos. Es inmediato que, en el caso $v_p = 0$, se tiene que $R^*(p^{v_p}, \Delta) = S^*(p^{v_p}, \Delta) = 1$. Por otra parte, en el caso en que es $p = 2$ y $v_2 \leq 2$, para todas las soluciones $B \pmod{2^{v_2}}$ de $B^2 \equiv \Delta \pmod{2^{v_2}}$ se tiene que 2 no divide $\mathrm{mcd}\left(2^{v_2'}, B, \dfrac{B^2-\Delta}{2^{v_2}}\right)$, puesto que $v_2' = 0$; por tanto, en este caso es $S^*(2^{v_2}, \Delta) = R^*(2^{v_2}, \Delta)$. En consecuencia, a partir de ahora, y para el cálculo de $S^*(2^{v_2}, \Delta)$, supondremos que es $v_2 \geq 3$ sin mención explícita.

• Caso $1 \leq v_p \leq t_p$.

La congruencia se convierte en $B^2 \equiv 0 \pmod{p^{v_p}}$. Si $v_p = 2w_p$, sus soluciones $B \pmod{p^{v_p}}$ son de la forma $B = p^{w_p}B'$, con $B' \pmod{p^{w_p}}$ cualquiera. Y si $v_p = 2w_p + 1$, sus soluciones $B \pmod{p^{v_p}}$ son de la forma $B = p^{w_p+1}B'$, con $B' \pmod{p^{w_p}}$ cualquiera. Por tanto, $R^*(p^{v_p}, \Delta) = p^{w_p}$, en cualquier caso.

Puesto que $v_p \geq 1$, todas las soluciones B son divisibles por p, de manera que la condición que p no divida $\mathrm{mcd}\left(p^{v_p'}, B, \dfrac{B^2-\Delta}{p^{v_p}}\right)$ equivale a decir que p^{v_p+1} no divida $B^2 - \Delta$. Para el cálculo de $S^*(p^{v_p}, \Delta)$, conviene distinguir los casos $v_p < t_p$ y $v_p = t_p$.

• Subcaso $v_p < t_p$.

Puesto que p^{v_p+1} divide Δ, las soluciones válidas son aquellas para las cuales p^{v_p+1} no divide B^2. Así, si $v_p = 2w_p$, de entre las soluciones $B = p^{w_p}B'$, $B' \pmod{p^{w_p}}$, son válidas aquellas para las cuales p no divide B'; es decir, $S^*(p^{v_p}, \Delta) = \varphi(p^{w_p}) = p^{w_p-1}(p-1)$. Y si $v_p = 2w_p + 1$, ninguna solución $B = p^{w_p+1}B'$, $B' \pmod{p^{w_p}}$, es válida; es decir, $S^*(p^{v_p}, \Delta) = 0$.

• Subcaso $v_p = t_p$.

Si $v_p = 2w_p + 1$, se tiene que $p^{v_p+1} = p^{2w_p+2}$ divide B^2 pero no divide Δ; por tanto, p^{v_p+1} no divide $B^2 - \Delta$ y todas las soluciones son válidas; es decir, $S^*(p^{v_p}, \Delta) = p^{w_p}$.

Si $v_p = 2w_p$, será más cómodo restar, del número total de soluciones, el número de soluciones para las cuales p^{v_p+1} divide $B^2 - \Delta$. En efecto, esta última condición equivale a escribir la congruencia $B^2 \equiv \Delta \pmod{p^{v_p+1}}$; poniendo $B = p^{w_p}B'$, con B' definido módulo p^{w_p}, las soluciones B para las cuales p^{v_p+1} divide $B^2 - \Delta$ son aquellas para las cuales se satisface la congruencia $B'^2 \equiv \Delta_p' \pmod{p^{1+v_p-2w_p} = p}$. Es decir, para calcular $S^*(p^{v_p}, \Delta)$, habrá que restar de p^{w_p} el número de elementos $B' \pmod{p^{w_p}}$ tales que $B'^2 \equiv \Delta_p' \pmod p$. Y, puesto que $w_p \geq 1$, cada clase residual módulo p es la reducción de exactamente p^{w_p-1} clases residuales módulo p^{w_p}, de manera que el número que hay que restar de p^{w_p} es el producto de p^{w_p-1} por el número de soluciones módulo p de la congruencia $B'^2 \equiv \Delta_p' \pmod p$. En el caso $p \neq 2$, esto es decir que $S^*(p^{v_p}, \Delta) = p^{w_p} - 2p^{w_p-1} = p^{w_p-1}(p-2)$, si $\left(\dfrac{\Delta_p'}{p}\right) = 1$, y $S^*(p^{v_p}, \Delta) = p^{w_p}$, si $\left(\dfrac{\Delta_p'}{p}\right) = -1$. Y en el caso $p = 2$, esto es decir que $S^*(2^{v_2}, \Delta) = 2^{w_2} - 2^{w_2-1} = 2^{w_2-1}$.

• Caso $v_p > t_p$.

Para que la congruencia $B^2 \equiv \Delta \pmod{p^{v_p}}$ tenga solución, es condición necesaria que t_p sea par. Luego, si t_p es impar, se tiene que $R^*(p^{v_p}, \Delta) = S^*(p^{v_p}, \Delta) = 0$. Podemos suponer, pues, que $t_p =: 2r_p$ es par. Las soluciones de la congruencia $B^2 \equiv \Delta \pmod{p^{v_p}}$ son los elementos $B = p^{r_p}B'$, con B' definido módulo $p^{v_p-r_p}$ y tal que $B'^2 \equiv \Delta_p' \pmod{p^{v_p-2r_p}}$. En particular, si Δ_p' no es un cuadrado módulo p (lo cual implica que es $p \neq 2$), no hay soluciones B' y, en consecuencia, $R^*(p^{v_p}, \Delta) = S^*(p^{v_p}, \Delta) = 0$.

Si $p \neq 2$ y $\left(\dfrac{\Delta_p'}{p}\right) = 1$, la congruencia $B'^2 \equiv \Delta_p' \pmod p$ tiene dos soluciones distintas; y, en virtud del lema de Hensel, la congruencia $B'^2 \equiv \Delta_p' \pmod{p^{v_p-2r_p}}$ tiene exactamente dos soluciones distintas. Cada una de estas dos soluciones es la reducción módulo $p^{v_p-2r_p}$ de exactamente p^{r_p} elementos de $\mathbb{Z}/p^{v_p-r_p}\mathbb{Z}$; por tanto, el número de soluciones $B' \pmod{p^{v_p-r_p}}$ de la congruencia $B'^2 \equiv \Delta_p' \pmod{p^{v_p-2r_p}}$ es exactamente $2p^{r_p}$; es decir, $R^*(p^{v_p}, \Delta) = 2p^{r_p}$. De estas soluciones, hay que ver cuántas satisfacen que p no divide $\mathrm{mcd}\left(p^{v_p}, B, \dfrac{B^2-\Delta}{p^{v_p}}\right)$. Si $r_p = 0$, p no divide B, de manera que las $2p^{r_p} = 2$ soluciones anteriores son válidas, y es $S^*(p^{v_p}, \Delta) = 2$. Supongamos, pues, que $r_p \geq 1$. Como antes, el lema de Hensel nos dice que el número de soluciones módulo $p^{1+v_p-2r_p}$ de la congruencia $B'^2 \equiv \Delta_p' \pmod{p^{1+v_p-2r_p}}$ también es dos, de manera que el número de soluciones B' módulo $p^{v_p-r_p}$ de la congruencia $B'^2 \equiv \Delta_p' \pmod{p^{v_p+1-2r_p}}$ es exactamente $2p^{r_p-1}$. Estas proporcio-

nan exactamente las soluciones $B \pmod{p^{v_p}}$ tales que p divide $\mathrm{mcd}\left(p^{v_p}, B, \dfrac{B^2-\Delta}{p^{v_p}}\right)$; es decir, obtenemos que $S^*(p^{v_p}, \Delta) = 2p^{r_p} - 2p^{r_p-1} = 2p^{r_p-1}(p-1)$.

Sólo resta estudiar el caso en que es $p = 2$ (y $v_2 > t_2 = v_2(\Delta) = 2r_2$). Hay que calcular el número de soluciones de la congruencia $B^2 \equiv 2^{2r_2}\Delta_2' \pmod{2^{v_2}}$, y el de las soluciones tales que $\mathrm{mcd}\left(B, \dfrac{B^2-\Delta}{2^{v_2}}\right)$ es impar. Las soluciones son los elementos $B = 2^{r_2}B'$, con B' definido módulo $2^{v_2-r_2}$ y tal que $B'^2 \equiv \Delta' \pmod{2^{v_2-2r_2}}$. Es decir, se tiene que $R^*(2^{v_2}, \Delta) = 2^{r_2}R^*(2^{v_2-2r_2}, \Delta_2')$. Y el número $R^*(2^{v_2-2r_2}, \Delta_2')$ sólo depende de la clase de congruencia de Δ_2' módulo 8, y del exponente $v_2 - 2r_2$. Si $v_2 - 2r_2 = 1$, es $R^*(2^{v_2-2r_2}, \Delta_2') = 1$; si $v_2 - 2r_2 \geq 2$, y $\Delta_2' \equiv 3 \pmod 4$, es $R^*(2^{v_2-2r_2}, \Delta_2') = 0$; si $v_2 - 2r_2 = 2$, y $\Delta_2' \equiv 1 \pmod 4$, es $R^*(2^{v_2-2r_2}, \Delta_2') = 2$; si $v_2 - 2r_2 \geq 3$, y $\Delta_2' \equiv 5 \pmod 8$, es $R^*(2^{v_2-2r_2}, \Delta_2') = 0$; finalmente, y en virtud del lema de Hensel, si $v_2 - 2r_2 \geq 3$, y $\Delta_2' \equiv 1 \pmod 8$, es $R^*(2^{v_2-2r_2}, \Delta_2') = 4$. Esto proporciona los valores de $R^*(2^{v_2}, \Delta)$ del enunciado.

Para calcular los valores de $S^*(2^{v_2}, \Delta)$, observemos que, si es $r_2 = 0$, entonces B es impar, de manera que para todas las soluciones se satisface la propiedad requerida; luego, en este caso, $S^*(2^{v_2}, \Delta) = R^*(2^{v_2}, \Delta)$. En el caso contrario, $r_2 \geq 1$, se tiene que B es par, y hay que ver cuántas soluciones $B' \pmod{2^{v_2-r_2}}$ de $B'^2 \equiv \Delta_2' \pmod{2^{v_2-2r_2}}$ no son soluciones de $B'^2 \equiv \Delta_2' \pmod{2^{1+v_2-2r_2}}$. En el caso $v_2 - 2r_2 = 1$, para la única solución $B' \equiv 1 \pmod{2^{v_2-2r_2}}$ de $B'^2 \equiv \Delta_2' \pmod{2^{v_2-2r_2}}$ es $B'^2 \equiv 1 \pmod{4 = 2^{1+v_2-2r_2}}$, de manera que las soluciones son válidas si, y sólo si, es $\Delta_2' \equiv 3 \pmod 4$; y si $\Delta_2' \equiv 1 \pmod 4$, ninguna solución es válida. En el caso $v_2 - 2r_2 = 2$, para toda solución $B' \pmod{2^{v_2-2r_2}}$ de $B'^2 \equiv \Delta_2' \pmod{2^{v_2-2r_2}}$ es $B'^2 \equiv 1 \pmod 8$, de manera que las soluciones son válidas si, y sólo si, es $\Delta_2' \equiv 5 \pmod 8$, puesto que si $\Delta_2' \equiv 3 \pmod 4$ no existen soluciones y si $\Delta_2' \equiv 1 \pmod 8$, todas las soluciones módulo $2^{v_2-2r_2}$ lo son módulo $2^{1+v_2-2r_2}$. Y, en el caso $v_2 - 2r_2 \geq 3$, para toda solución $B' \pmod{2^{v_2-2r_2}}$ de $B'^2 \equiv \Delta_2' \pmod{2^{v_2-2r_2}}$ es $B'^2 \equiv 1 \pmod 8$, de manera que es $\Delta_2' \equiv 1 \pmod 8$. En este caso, la mitad de las soluciones $B' \pmod{2^{v_2-r_2}}$ de $B'^2 \equiv \Delta_2' \pmod{2^{v_2-2r_2}}$ son soluciones de $B'^2 \equiv \Delta_2' \pmod{2^{1+v_2-2r_2}}$; por tanto, la otra mitad son válidas; es decir, $S^*(2^{v_2}, \Delta) = 2^{1+r_2}$. Esto acaba la demostración. □

Observación 5.7. *En el caso que nos interesa, Δ es un discriminante y los valores que queremos calcular son $\frac{1}{2}R^*(4N, \Delta)$ y $\frac{1}{2}S^*(4N, \Delta)$; en particular, siempre tendremos que es $v_2 \geq 2$, caso en que $R^*(2^{2+v_2}, \Delta)$ y $S^*(2^{2+v_2}, \Delta)$ son pares. Por otra parte, puesto que $\Delta = \Delta_0 r^2$, con Δ_0 un discriminante fundamental, para los primos que no dividen Δ_0, $v_p(\Delta)$ será par. Y si 2 no divide Δ_0, tendremos que $\Delta_2' \equiv 1 \pmod 4$. Estas consideraciones reducen el número de casos a tener en cuenta.*

6. INMERSIONES EN EL ORDEN GENERADO POR $\Gamma_0(N)$

El orden $\mathcal{O}_0(N)$ está generado por el grupo de congruencia $\Gamma_0(N)$ si, y sólo si, $\mathrm{mcd}(N, 6) = 1$. Con más precisión, en **[Ba-Tr 00-1]** se ha demostrado el resultado siguiente.

Proposición 6.1. *Sea $D := \mathrm{mcd}(N, 24)$. El subanillo de $\mathbf{M}(2, \mathbb{Q})$ generado por el grupo $\Gamma_0(N)$ es exactamente el orden*

$$\mathcal{O}(1, N, D) := \left\{ \begin{bmatrix} x & y \\ zN & x + tD \end{bmatrix} : x, y, z, t \in \mathbb{Z} \right\}. \quad \square$$

En el caso $D = 1$, el orden $\mathcal{O}(1, N, D)$ es exactamente el orden $\mathcal{O}_0(N)$; pero esto no es así si $D > 1$. Como consecuencia, en el caso en que $D > 1$, además de estudiar las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ conviene estudiar las inmersiones enteras para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$. Esto es lo que haremos a continuación.

Proposición 6.2. *Sea $D := \mathrm{mcd}(N, 24)$.*

(a) Existen inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ si, y sólo si, D^2 divide 6Δ.

(b) Si D^2 divide 6Δ, las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ son exactamente las inmersiones enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Demostración. Sea $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ una inmersión entera para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$; entonces, λ está dada por una asignación

$$\lambda(\sqrt{\Delta}) = \begin{bmatrix} -bD & -2c \\ 2aN & bD \end{bmatrix},$$

con $a, b, c \in \mathbb{Z}$ y $-D^2b^2 + 4Nac = -\Delta$ (cf. **[Ba-Tr 00-2]**). Si multiplicamos esta igualdad por 6, obtenemos que $-6D^2b^2 + 24Nac = -6\Delta$ y, puesto que D^2 divide $24N$, vemos que D^2 divide 6Δ. Además, puesto que $\mathcal{O}(1, N, D) \subseteq \mathcal{O}_0(N)$, la inmersión λ es entera para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$.

Recíprocamente, supongamos que D^2 divide 6Δ, y que $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ es una inmersión entera para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. Sea

$$\lambda(\sqrt{\Delta}) = \begin{bmatrix} -b & -2c \\ 2aN & b \end{bmatrix},$$

con $a, b, c \in \mathbb{Z}$ y $-b^2 + 4Nac = -\Delta$; entonces, $-6b^2 + 24Nac = -6\Delta$, de manera que D^2 divide $6b^2$; puesto que 6 es libre de cuadrados, obtenemos que D divide b y, por tanto, $\lambda(\sqrt{\Delta}) \in \mathcal{O}(2, 2N, 2D)$; es decir, λ es entera para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$. Esto acaba la demostración. □

Por otra parte, el grupo $\Gamma_0(N)$ coincide con el grupo

$$\Gamma(1, N, D) = \left\{ \begin{bmatrix} \alpha & \beta \\ \gamma N & \alpha + \delta D \end{bmatrix} : \alpha, \beta, \gamma, \delta \in \mathbb{Z}, \det = 1 \right\},$$

de los elementos de norma 1 de $\mathcal{O}(1, N, D)$. Por tanto, la clasificación de las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ para la acción del grupo de unidades de norma 1 de $\mathcal{O}(1, N, D)$ es exactamente la clasificación para el grupo $\Gamma_0(N)$. Por tanto, tenemos el resultado siguiente.

Corolario 6.3. *El conjunto de clases de $\Gamma_0(N)$-equivalencia de inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ es exactamente el conjunto de clases de $\Gamma_0(N)$-equivalencia de inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ enteras para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, para el caso en que D^2 divide 6Δ. En otro caso, no existen tales inmersiones.* □

El resultado análogo para las inmersiones optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ no es tan sencillo. En efecto; no es cierto en general, ni aún suponiendo que D^2 divide 6Δ, que las inmersiones optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ sean las inmersiones optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$. Se tiene el resultado siguiente.

Proposición 6.4. *Sea $\Delta := \Delta_0 r^2$, $r \geq 1$, un discriminante asociado al discriminante fundamental Δ_0, sea $D := \mathrm{mcd}(N, 24)$, y supongamos que D^2 divide 6Δ. El conjunto de las inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ es la reunión*

$$\bigcup_{d \mid \mathrm{mcd}(D, r)} \bigcup_{\substack{\mathrm{mcd}(b, d) = 1 \\ b \left(\mathrm{mod} \frac{2dN}{D}\right) \\ b^2 \equiv \frac{\Delta}{d^2} \left(\mathrm{mod} \frac{4dN}{D}\right)}} \mathcal{H}\left(N, \frac{\Delta}{d^2}; 1, *, *, \frac{bD}{d}\right).$$

Demostración. Sea $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ una inmersión entera para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$; entonces, $\lambda(\sqrt{\Delta})$ es de la forma

$$\lambda(\sqrt{\Delta}) = \begin{bmatrix} -bD & -2c \\ 2aN & bD \end{bmatrix},$$

con $a, b, c \in \mathbb{Z}$ y $-D^2b^2 + 4Nac = -\Delta$. Supongamos que λ es una inmersión optimal para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$, lo cual equivale a decir que es $\mathrm{mcd}(a, b, c) = 1$ (cf. **[Ba-Tr 00-2]**).

Decir que la inmersión λ es optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ equivale a decir que es $\mathrm{mcd}(a, bD, c) = 1$. Sin embargo, esto no tiene por qué suceder. En general, sea $d := \mathrm{mcd}(a, bD, c)$. Puesto que $\mathrm{mcd}(a, b, c) = 1$, tenemos que d divide D; entonces,

$$\lambda\left(\frac{\sqrt{\Delta}}{d}\right) = \begin{bmatrix} -\frac{bD}{d} & -2\frac{c}{d} \\ 2\frac{a}{d}N & \frac{bD}{d} \end{bmatrix},$$

de manera que λ es entera para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta/d^2})$; y, puesto que es $\mathrm{mcd}\left(\frac{a}{d}, \frac{bD}{d}, \frac{c}{d}\right) = 1$, la inmersión λ es optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{\Delta/d^2})$; así, λ pertenece a $\mathcal{H}\left(N, \frac{\Delta}{d^2}; 1, *, *, \frac{bD}{d}\right)$. Puesto que $\frac{\Delta}{d^2}$ es un discriminante, se satisface la condición $d \mid r$, de manera que $d \mid \mathrm{mcd}(D, r)$; y, además, es $\mathrm{mcd}(d, b) = 1$, puesto que $\mathrm{mcd}(d, b) = \mathrm{mcd}(a, bD, c, b) = \mathrm{mcd}(a, b, c) = 1$.

Recíprocamente; supongamos que $d \mid \mathrm{mcd}(D, r)$ es un divisor de D y de r, de manera que $\frac{\Delta}{d^2}$ es un discriminante, que $b \in \mathbb{Z}$ es tal que $\mathrm{mcd}(d, b) = 1$, y que $\lambda \in \mathcal{H}\left(N, \frac{\Delta}{d^2}; 1, *, *, \frac{bD}{d}\right)$. Entonces, tenemos que

$$\lambda\left(\frac{\sqrt{\Delta}}{d}\right) = \begin{bmatrix} -\frac{bD}{d} & -2\frac{c}{d} \\ 2\frac{a}{d}N & \frac{bD}{d} \end{bmatrix},$$

con $a, c \in \mathbb{Z}$ múltiplos de d, $-b^2D^2 + 4Nac = -\Delta$, y $\mathrm{mcd}\left(\frac{a}{d}, \frac{bD}{d}, \frac{c}{d}\right) = 1$; es decir,

$$\lambda(\sqrt{\Delta}) = \begin{bmatrix} -bD & -2c \\ 2aN & bD \end{bmatrix},$$

con $a, b, c \in \mathbb{Z}$; en consecuencia, la inmersión λ es entera para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$. Además, por ser $\mathrm{mcd}\left(\frac{a}{d}, \frac{bD}{d}, \frac{c}{d}\right) = 1$, se tiene que $\mathrm{mcd}(a, bD, c) = d$, de manera que se satisface la igualdad $\mathrm{mcd}(a, b, c) = \mathrm{mcd}(a, b, bD, c) = \mathrm{mcd}(d, b) = 1$; es decir, λ es optimal para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$, como queríamos demostrar. □

Análogamente al caso de las inmersiones enteras, obtenemos la clasificación de las inmersiones optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ respecto del grupo $\Gamma(1, N, D) = \Gamma_0(N)$.

Corolario 6.5. *Sea $\Delta := \Delta_0 r^2$, $r \geq 1$, un discriminante asociado al discriminante fundamental Δ_0, sea $D := \mathrm{mcd}(N, 24)$, y supongamos que D^2 divide 6Δ. Las clases de $\Gamma_0(N)$-equivalencia de inmersiones $\lambda : K \to \mathbf{M}(2, \mathbb{Q})$ optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_\Delta)$ son exacta-*

mente las clases de $\Gamma_0(N)$*-equivalencia de inmersiones optimales de los conjuntos*

$$H\left(N, \frac{\Delta}{d^2}; 1, *, *, \frac{bD}{d}\right),$$

para $d \mid \mathrm{mcd}(D, r)$ *y* $b \left(\mathrm{mod}\ \frac{2Nd}{D}\right)$ *tales que* $\frac{b^2D^2}{d^2} \equiv \frac{\Delta}{d^2} \pmod{4N}$ *y* $\mathrm{mcd}(b, d) = 1$. □

7. EJEMPLOS NUMÉRICOS

En esta sección, daremos ejemplos numéricos de los números de clases de $\Gamma_0(N)$-equivalencia de inmersiones λ: $\mathbb{Q}(\sqrt{-2}) \to \mathbf{M}(2, \mathbb{Q})$ enteras, optimales, primitivas, o biprimitivas, para algunas parejas $(\mathcal{O}, \mathcal{O}_\Delta)$. Concretamente, para $(\mathcal{O}_0(1), \mathcal{O}_\Delta)$, Δ cualquiera; para las parejas $(\mathcal{O}_0(N), \mathcal{O}_{-8})$ y $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$, con $N \geq 1$ cualquiera y $D := \mathrm{mcd}(N, 24)$; y para algunas parejas $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$, con N dependiente de Δ.

El caso más simple corresponde a tomar $N = 1$ y Δ cualquiera. En efecto; puesto que $N = 1$, todas las inmersiones optimales para la pareja $(\mathcal{O}_0(1), \mathcal{O}_\Delta)$ son automáticamente primitivas y biprimitivas. Y las inmersiones enteras para la pareja $(\mathcal{O}_0(1), \mathcal{O}_\Delta)$ son las inmersiones optimales para las parejas $(\mathcal{O}_0(1), \mathcal{O}_{\Delta/d^2})$, para $d \mid r$, donde $\Delta = \Delta_0 r^2$, con $r \geq 1$ y Δ_0 un discriminante fundamental. Teniendo en cuenta los resultados de la sección anterior, obtenemos el siguiente.

Corolario 7.1. *Sea* $\Delta = \Delta_0 r^2$, $r \geq 1$, *un discriminate cualquiera asociado al discriminante fundamental* Δ_0. *El número de* $\mathbf{SL}(2, \mathbb{Z})$*-clases de equivalencia de inmersiones* $\lambda : \mathbb{Q}(\sqrt{\Delta}) \to \mathbf{M}(2, \mathbb{Q})$ *optimales (o primitivas, o biprimitivas) para la pareja* $(\mathcal{O}_0(1), \mathcal{O}_\Delta)$ *es exactamente* $h(\Delta)$. *El número de* $\mathbf{SL}(2, \mathbb{Z})$*-clases de equivalencia de inmersiones enteras para la pareja* $(\mathcal{O}_0(1), \mathcal{O}_\Delta)$ *es exactamente* $\sum_{d \mid r} h(\Delta_0 d^2)$. □

A continuación, estudiamos los números de clases de inmersiones para las parejas $(\mathcal{O}_0(N), \mathcal{O}_{-8})$. Sean, pues, $\Delta := -8$, y $N = \prod_p p^{v_p}$ la descomposición de un número entero cualquiera $N \geq 1$ en factores primos.

Observemos, en primer lugar, que $\Delta = -8$ es un discriminante fundamental, de manera que toda inmersión $\lambda : \mathbb{Q}(\sqrt{-2}) \to \mathbf{M}(2, \mathbb{Q})$ optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{-8})$ es automáticamente primitiva y biprimitiva (cf. el corolario **2.11**). Y, en virtud del teorema **2.10**, existen inmersiones optimales (resp. enteras) para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{-8})$ si, y sólo si, $v_p \leq 1$ para todo primo ramificado en el orden maximal de $\mathbb{Q}(\sqrt{-8}) = \mathbb{Q}(\sqrt{-2})$, y $v_p = 0$ para todo primo inerte en el orden maximal de $\mathbb{Q}(\sqrt{-8})$; es decir, $v_2 \leq 1$ y $v_p = 0$ para todo primo $p \equiv 5,7 \pmod 8$. Puesto que $h(-8) = 2$, el cálculo del factor $r^*(N, -8)$ produce el resultado siguiente.

Corolario 7.2. *El número de clases de* $\Gamma_0(N)$*-equivalencia de inmersiones* $\lambda : \mathbb{Q}(\sqrt{-2}) \to \mathbf{M}(2, \mathbb{Q})$ *optimales (resp. primitivas, biprimitivas) para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_{-8})$ *es exactamente*

$$2^{\#\{p\,:\,p \mid 2N\}},$$

si para todo primo impar p *que divide* N *es* $p \equiv 1,3 \pmod 8$ *y* 4 *no divide* N. *Si* 4 *divide* N *o bien existe un primo* $p \equiv 5,7 \pmod 8$ *que divide* N, *entonces no hay inmersiones enteras para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_{-8})$. □

Estudiemos, ahora, el caso de las inmersiones optimales para las parejas $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$, con $D := \mathrm{mcd}(N, 24)$.

Hemos visto que para que existan tales inmersiones es necesario que existan inmersiones enteras (equivalentemente, que existan inmersiones optimales) para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{-8})$ y que D^2 divida $6\Delta = -48$. En particular, para $N = \prod_p p^{v_p}$ se deben satisfacer las restricciones $v_2 \leq 1$ y $v_p = 0$ para todo primo p tal que $p \equiv 5,7 \pmod 8$; y, además, puesto que D^2 debe dividir $-6\Delta = -48$, 3 tampoco puede dividir N; es decir, debe ser $v_3 = 0$.

Teniendo en cuenta estas restricciones, obtenemos que el valor de D puede ser

$$D = \begin{cases} 2, & \text{si } v_2 = 1, \\ 1, & \text{si } v_2 = 0. \end{cases}$$

Por otra parte, tenemos que $\mathrm{mcd}(D, r) = 1$, puesto que -8 es un discriminante fundamental y, por tanto, es $r = 1$. En consecuencia, las clases de $\Gamma_0(N)$-equivalencia de inmersiones optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$ son las clases de $\Gamma_0(N)$-equivalencia de los conjuntos

$$H(N, -8; 1, *, *, bD),$$

$$\text{para } b \left(\mathrm{mod}\ \frac{2N}{D}\right) \text{ tal que } b^2D^2 \equiv -8 \pmod{4N}.$$

Pero éstas son todas las inmersiones $\lambda : \mathbb{Q}(\sqrt{-2}) \to \mathbf{M}(2, \mathbb{Q})$ optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{-8})$. En efecto; puesto que Δ es par, para cualquier inmersión λ optimal para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{-8})$ el valor del invariante B debe ser par; luego, de la forma $B = 2b$. Por tanto, la condición que sea $B = bD$ no es restrictiva ni en el caso $D = 1$, ni en el caso $D = 2$. Es decir, se tiene que el conjunto de las clases de $\Gamma_0(N)$-equivalencia de inmersiones optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$ coincide con el conjunto de las clases de $\Gamma_0(N)$-equivalencia de inmersiones optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{-8})$.

Por tanto, hemos establecido el resultado siguiente.

Corolario 7.3. *Sea* $D := \mathrm{mcd}(N, 24)$. *El número de clases de* $\Gamma_0(N)$*-equivalencia de inmersiones* $\lambda : \mathbb{Q}(\sqrt{-2}) \to$

$\rightarrow \mathbf{M}(2, \mathbb{Q})$ *optimales para la pareja* $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$ *es exactamente*

$$2^{\#\{p\,:\,p\mid 2N\}},$$

si 4 *no divide N y para todo primo impar p que divide N es* $p \neq 3$ *y* $p \equiv 1,3 \pmod 8$. *Si* 4 *divide N, o bien* 3 *divide N, o bien existe un primo* $p \equiv 5,7 \pmod 8$ *que divide N, entonces no hay inmersiones enteras para la pareja* $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$. □

Notemos que, en este caso de discriminante −8, las inmersiones enteras (resp. optimales) para las parejas $(\mathcal{O}_0(N), \mathcal{O}_{-8})$ y $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$ coinciden, excepto en el caso en que 3 divide N; en este caso, aunque existan inmersiones enteras u optimales para la pareja $(\mathcal{O}_0(N), \mathcal{O}_{-8})$, no existen inmersiones enteras ni optimales para la pareja $(\mathcal{O}(1, N, D), \mathcal{O}_{-8})$.

Para terminar, estudiaremos los numeros de $\Gamma_0(N)$-clases de equivalencia de inmersiones λ: $\mathbb{Q}(\sqrt{\Delta}) \rightarrow \mathbf{M}(2, \mathbb{Q})$ primitivas para las parejas $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ en los casos en que Δ es cualquiera y $N := \Delta$, si 2 no divide Δ_0; y $N := \frac{\Delta}{4}$, si 2 divide Δ_0, o bien $N := \frac{\Delta}{2}$, si 4 divide Δ_0, pero 8 no divide Δ_0.

Proposición 7.4. *Sea* $\Delta = \Delta_0 r^2$, $r \geq 1$, *un discriminante asociado a un discriminante fundamental cualquiera* Δ_0. *Sea* $N := \Delta$, *si* $2 \nmid \Delta_0$; $N := \frac{\Delta}{4}$, si $2 \mid \Delta_0$; *o bien* $N := \frac{\Delta}{2}$, *si* $4 \mid \Delta_0$, *pero* $8 \nmid \Delta_0$. *El número de* $\Gamma_0(N)$*-clases de equivalencia de inmersiones* $\lambda : \mathbb{Q}(\sqrt{\Delta}) \rightarrow \mathbf{M}(2, \mathbb{Q})$ *primitivas para la pareja* $(\mathcal{O}_0(N), \mathcal{O}_\Delta)$ *es exactamente* $rh(\Delta)$. □

Demostración. En efecto; el cálculo de los factores $r^*(N, \Delta)$ proporciona, en estos casos, $r^*(N, \Delta) = r$. □

REFERENCIAS

1. **[Ar-Ba 00-1]** Arenas, A. & Bayer, P. (2000), Heegner points on modular curves, *Rev. R. Acad. Cienc. Exact. Fis. Nat., Esp.*, **94**, p.323-332.
2. **[Ba-Tr 00-1]** Bayer, P. & Travesa, A. (2000), Órdenes matriciales generados por grupos de congruencia, *Rev. R. Acad. Cienc. Exact. Fis. Nat., Esp.*, **94**, p.339-346.
3. **[Ba-Tr 00-2]** Bayer, P. & Travesa, A. (2000), Formas cuadráticas ternarias e inmersiones matriciales de órdenes cuadráticos, *Rev. R. Acad. Cienc. Exact. Fis. Nat., Esp.*, **94,** p. 347-355
4. **[Gr-Ko-Za 87]** Gross, B.; Kohnen, W. & Zagier, D. (1987), Heegner Points and Derivatives of *L*-Series. II, *Math. Ann.* **278**, p. 497-562.