Representación por formas cuadráticas binarias

Índice de contenidos

1 Preliminares

1.1 Residuos cuadráticos

Definición 1.1. Sean $m, n \in \mathbb{Z}$, $m > 0$ y $(m : n) = 1$. Si la ecuación

$$x^2 \equiv n \pmod{m} \tag{1}$$

tiene solución, decimos que n es un *residuo cuadrático módulo* m.

Definición 1.2 (El símbolo de Legendre)**.** Si $p > 2$ es un primo impar y $p \nmid n$, el *símbolo de Legendre* (n/p) denota el valor:

$$\left(\frac{n}{p}\right) = \begin{cases} 1 & \text{si } n \text{ es un residuo cuadrático módulo } p\ , \\ -1 & \text{si no.} \end{cases}$$

Teorema 1.3. *Si* $n \equiv n' \pmod{p}$ *(y* $p \nmid n$*), entonces*

$$\left(\frac{n}{p}\right) = \left(\frac{n'}{p}\right)\ .$$

Teorema 1.4. *Sea* $p > 2$ *un primo impar. En cada sistema de representantes de las clases de equivalencia módulo* p*, hay exactamente* $\frac{p-1}{2}$ *resduos cuadráticos; éstos están representados por:*

$$1^2,\ 2^2,\ \ldots,\ \left(\frac{p-1}{2}\right)^2\ . \tag{2}$$

En particular, la cantidad de *no residuos* es $\frac{p-1}{2}$.

Demostración. Será suficiente demostrar que los restos módulo p de los cuadrados (2) son todos distintos. Ahora, la ecuación $x^2 \equiv n \pmod{p}$ tiene, para cada n, como mucho, dos soluciones diferentes; si $p \nmid n$, 0 no es una solución y, por otra parte, si la ecuación tiene solución, existe una solución x en el intervalo $0 \leq x \leq p-1$. Dado que

$$(p-x)^2 \equiv x^2 \pmod{p}\ ,$$

si $(n/p) = 1$, existe una solución x en el intervalo $0 \leq x \leq \frac{p-1}{2}$ $(x \mapsto p - x)$. En particular, para n coprimo con p, existe una solución $1 \leq x \leq \frac{p-1}{2}$, o no existe ninguna. De esto, se deduce que los cuadrados (2) son incongruentes módulo p. □

Teorema 1.5 (El criterio de Euler)**.** *Si* $p > 2$ *es un primo impar y* $p \nmid n$*, entonces*

$$\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}\ .$$

Demostración. La congruencia $n^{p-1} \equiv 1$ implica que $n^{\frac{p-1}{2}} \equiv \pm 1$. Si $(n/p) = 1$, existe x tal que $x^2 \equiv n$ y, en consecuencia, $n^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 = \left(\frac{n}{p}\right)$. En particular, por el Teorema 1.4, los residuos cuadráticos proporcionan $\frac{p-1}{2}$ soluciones distintas a la ecuación

$$x^{\frac{p-1}{2}} \equiv 1 \pmod{p} . \tag{3}$$

Pero (3) tiene, a lo sumo, $\frac{p-1}{2}$ soluciones distintas, módulo p. En particular, la cantidad de soluciones es exactamente $\frac{p-1}{2}$ y las soluciones están representadas por los residuos cuadráticos. Si $(n/p) = -1$, entonces n *no puede ser* una solución de (3). Por lo tanto, n debe verificar $n^{\frac{p-1}{2}} \equiv -1 = (n/p)$. □

Teorema 1.6. *Si $p > 2$ es un primo impar y $p \nmid nn'$, entonces*

$$\left(\frac{nn'}{p}\right) = \left(\frac{n}{p}\right)\left(\frac{n'}{p}\right) .$$

Demostración. Por el Teorema 1.5, ambos lados de la igualdad son congruentes módulo p. Pero $p > 2$ y los símbolos toman únicamente los valores ± 1. Entonces, deben ser iguales. □

Teorema 1.7. *Si $p > 2$ es un primo impar, -1 es un residuo cuadrático módulo p precisamente cuando $p \equiv 1 \pmod{4}$:*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } p \equiv 1 \pmod{4} \\ -1 & \text{si } p \equiv 3 \pmod{4} \end{cases} .$$

Teorema 1.8 (El lema de Gauss)**.** *Sea $p > 2$ un primo impar y $p \nmid n$. Los restos de los $\frac{p-1}{2}$ enteros*

$$n,\, 2n,\, \ldots,\, \left(\frac{p-1}{2}\right) n \tag{4}$$

son todos distintos y, si m denota la cantidad de aquellos que son mayores que $p/2$, entonces

$$\left(\frac{n}{p}\right) = (-1)^m .$$

Demostración. Veamos, primero, que los restos de los enteros (4) son distintos. Ordenamos los restos en dos secuencias: sean $a_1, \ldots, a_l$ los restos menores que $p/2$ y sean $b_1, \ldots, b_m$ los restos mayores que $p/2$ ($m + l = \frac{p-1}{2}$). Si $1 \leq x, y \leq \frac{p-1}{2}$, entonces $xn \equiv yn$ implica $x \equiv y$ y $x = y$. Pero veamos que tampoco pueden ser opuestos: si $xn \equiv -yn$, entonces $x + y \equiv 0$, que no es compatible con $2 \leq x + y \leq p - 1$. Esto último tiene como consecuencia:

$$\{a_1, \ldots, a_l\} \sqcup \{p - b_1, \ldots, p - b_m\} = \{1, 2, \ldots, \tfrac{p-1}{2}\} . \tag{5}$$

Veamos, ahora, que $\frac{n}{p} = (-1)^m$. Por un lado, por definición,

$$\prod_i a_i \prod_j b_j \equiv \left(\frac{p-1}{2}\right)! \, n^{\frac{p-1}{2}} \pmod{p} .$$

Por otro lado, por (5),

$$\prod_i a_i \prod_j (p - b_j) \equiv \left(\frac{p-1}{2}\right)! .$$

De estas dos congruencias, se deduce que $n^{\frac{p-1}{2}} \equiv (-1)^m$. Por el Teorema 1.5, el hecho de que (n/p) toma valores ± 1 y que $p > 2$, se deduce la igualdad $(n/p) = (-1)^m$. □

Teorema 1.9. *Si $p > 2$ es un primo impar, entonces 2 es un residuo cuadrático módulo p precisamente cuando $p \equiv \pm 1 \pmod 8$:*

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \text{si } p \equiv 1, 7 \pmod 8 \\ -1 & \text{si } p \equiv 3, 5 \pmod 8 \end{cases} .$$

A lo largo de la demostración del Teorema 1.10, se demostrará nuevamente el Teorema 1.9.

Demostración. Por el Teorema 1.8, será suficiente mostrar que

$$m = \left| \left\{ \mathsf{r}_p(h\,2) \,:\, 1 \le h \le \tfrac{p-1}{2} \right\} \right| ,$$

donde r_p denota la función tomar resto módulo p. Pero, como $p > 2$, se cumple $p > h\,2 > 0$, si $1 \le h \le \frac{p-1}{2}$. Entonces,

$$m = \left| \left\{ 1 \le h \le \tfrac{p-1}{2} \,:\, p/2 < h\,2 < p \right\} \right| = \left\lfloor \frac{p}{2} \right\rfloor - \left\lfloor \frac{p}{4} \right\rfloor .$$

Separar en casos de acuerdo con el resto $\mathsf{r}_8(p)$. Módulo 2,

$$m \equiv \begin{cases} 0 & \text{si } \mathsf{r}_8(p) = 1 \\ 1 & \text{si } \mathsf{r}_8(p) = 3 \\ 1 & \text{si } \mathsf{r}_8(p) = 5 \\ 0 & \text{si } \mathsf{r}_8(p) = 7 \end{cases} \equiv \frac{p^2-1}{8} \pmod 2 .$$

□

Teorema 1.10 (La Ley de reciprocidad cuadrática)**.** *Si $p \neq q$ son dos primos impares distintos, entonces*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} .$$

Demostración. Nuevamente, consideramos el conjunto $\left\{k\,q\,:\,1\le k\le \frac{p-1}{2}\right\}$, separando sus restos en dos secuencias $a_1,\,\ldots,\,a_l<p/2$ y $b_1,\,\ldots,\,b_m>p/2$, $l+m=\frac{p-1}{2}$. Estas secuencias verifican (5). Definimos:

$$a\,:=\,\sum_i a_i\quad,\quad b\,:=\,\sum_j b_j\quad\text{y}\quad k\,q\,=\,q_k\,p+r_k\;,$$

donde $1\le r_k\le p-1$, es el resto de dividir $k\,q$ por p. Se deduce que:

$$\sum_{k=1}^{\frac{p-1}{2}} r_k\,=\,a+b\quad\text{y}\quad \sum_{k=1}^{\frac{p-1}{2}} k\,=\,\begin{cases}\frac{\frac{p-1}{2}\,\frac{p+1}{2}}{2} & =\,\frac{p^2-1}{8}\quad(!)\\ \sum_i a_i+\sum_j\,(p-b_j) & =\,a+mp-b\end{cases}\;.$$

De estas igualdades, se deduce:

$$(a+mp-b)\,q\,=\,\frac{p^2-1}{8}\,q\,=\,\sum_k k\,q\,=\,\sum_k\,(r_k+q_k\,p)\,=\,a+b+\Big(\sum_k q_k\Big)\,p$$

y, entonces,

$$\frac{p^2-1}{8}\,(q-1)\,=\,\Big(\sum_k q_k\Big)\,p\,+\,2b\,-\,mp\,\equiv\,\Big(\sum_k q_k\Big)\,+\,m\pmod 2\;.$$

Pero $q_k=\lfloor kq/p\rfloor$.[1] Entonces, $\sum_k\lfloor kq/p\rfloor\equiv m\,(\mathsf{mod}\,2)$, de lo que se deduce la expresión:

$$\left(\frac{q}{p}\right)\,=\,(-1)^{\sum_{k=1}^{\frac{p-1}{2}}\,\lfloor kq/p\rfloor}\;.\tag{6}$$

De manera análoga, o por simetría,

$$\left(\frac{p}{q}\right)\,=\,(-1)^{\sum_{l=1}^{\frac{q-1}{2}}\,\lfloor lp/q\rfloor}\;.\tag{7}$$

□

Lema 1.11. *Si $p,q>2$, $(p:q)=1$ son enteros positivos impares coprimos, entonces*

$$\sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor\,+\,\sum_{l=1}^{\frac{q-1}{2}}\left\lfloor\frac{lp}{q}\right\rfloor\,=\,\frac{p-1}{2}\,\frac{q-1}{2}\;.$$

Demostración. La expresión $f(k,l)=-kq+lp$ define una función

$$f\,:\,[\![1,\tfrac{p-1}{2}]\!]\,\times\,[\![1,\tfrac{q-1}{2}]\!]\,\to\,\mathbb{Z}\;,$$

[1] Si $q=2$, $\frac{p^2-1}{8}\equiv m\,(\mathsf{mod}\,2)$, pues $\lfloor k\,2/p\rfloor=0$, de donde se deduce –nuevamente– la fórmula para $(2/p)$.

que, como $(p:q)=1$, nunca se anula, pues, por ejemplo, $f(k,l)$ no es divisible por p; tampoco es divisible por q.[2] Podemos partir el dominio de acuerdo al signo de f:

$$[\![1,\tfrac{p-1}{2}]\!]\times[\![1,\tfrac{q-1}{2}]\!]=\big\{f>0\big\}\sqcup\big\{f<0\big\}\ .$$

Pero, para cada l en el rango $1\leq l\leq\frac{q-1}{2}$,

$$-kq+lp\ >\ 0\quad\Leftrightarrow\quad k\ <\ lp/q\ .$$

En tal caso, se debe cumplir que $k<p/2$. Así, para $l\in[\![1,\frac{q-1}{2}]\!]$,

$$1\ \leq\ k\ <\ lp/q\quad\Leftrightarrow\quad k\in[\![1,\tfrac{p-1}{2}]\!]\text{ y }f(k,l)\ >\ 0\ .$$

En particular,

$$\big|\{f>0\}\big|\ =\ \sum_{l=1}^{\frac{q-1}{2}}\left\lfloor\frac{lp}{q}\right\rfloor\ .$$

Análogamente,

$$\big|\{f<0\}\big|\ =\ \sum_{k=1}^{\frac{p-1}{2}}\left\lfloor\frac{kq}{p}\right\rfloor\ .$$

□

Teorema 1.12. *Sean $l>0$ y $p\nmid n$ un primo. La cantidad de soluciones de*

$$x^2\ \equiv\ n\,(\mathsf{mod}\,p^l)\tag{8}$$

está dada por la siguiente tabla:

$p=2$	$l=1$		1
	$l=2$	$n\equiv 1\,(\mathsf{mod}\,4)$	2
		$n\equiv 3\,(\mathsf{mod}\,4)$	0
	$l>2$	$n\equiv 1\,(\mathsf{mod}\,8)$	4
		$n\not\equiv 1\,(\mathsf{mod}\,8)$	0
$p>2$			$1+\left(\frac{n}{p}\right)$

Tabla 1: Cantidad de soluciones a (8)

Demostración. Si $p=2$, $x^2\equiv 1\,(\mathsf{mod}\,2)$ tiene como única solución módulo 2 a $x\equiv 1$; la ecuación $x^2\equiv 1\,(\mathsf{mod}\,4)$ tiene dos soluciones; $x^2\equiv 3\,(\mathsf{mod}\,4)$ no tiene soluciones; $x^2\equiv 1\,(\mathsf{mod}\,8)$ tiene cuatro soluciones; $x^2\equiv n\,(\mathsf{mod}\,8)$ no tiene soluciones, si $n\not\equiv 1\,(\mathsf{mod}\,8)$. En particular, si $l>2$ y $n\not\equiv 1\,(\mathsf{mod}\,8)$, entonces $x^2\equiv n\,(\mathsf{mod}\,2^l)$ no tiene soluciones.

[2] De hecho, también es cierto que $f(k,l)\not\equiv\pm f(k_1,l_1)$, si $(k,l)\neq(k_1,l_1)$, tanto módulo p como módulo q,

x	$x^2 \pmod 2$	$x^2 \pmod 4$	$x^2 \pmod 8$	$x^2 \pmod{16}$	$x^2 \pmod{32}$
1	1	1	1	1	1
3		1	1	9	9
5			1	9	25
7			1	1	17
9				1	17
11				9	25
13				9	9
15				1	1
17					1
19					9
21					25
23					17
25					17
27					25
29					9
31					1

Tabla 2: Cuadrados módulo potencias de $p = 2$

Si $0 \leq x \leq 2^l - 1$ y m representa la clase de x^2 módulo 2^l, entonces $m \equiv 1 \pmod 8$; la pregunta es si todo tal m aparece de esta manera, es decir, es un cuadrado. Hay exactamente 2^{l-3} valores de m en el rango $0 \leq m \leq 2^l - 1$ que cumplen $m \equiv 1 \pmod 8$. O bien $x^2 \equiv m$ no tiene solución, o bien existe x_0 tal que $x_0^2 \equiv m$. En este último caso, cualquier otro valor de x tal que $x^2 \equiv m$ cumple:

$$x^2 \equiv x_0^2 \pmod{2^l} \qquad \text{y} \qquad 2^{l-2} \quad \text{divide a} \quad \frac{x - x_0}{2} \frac{x + x_0}{2} \, .$$

Pero 2 no divide a ambos, $\frac{x-x_0}{2}$ y $\frac{x+x_0}{2}$, pues la suma es $\frac{x-x_0}{2} + \frac{x+x_0}{2} = x$, que es impar. Dicho de otra manera,

$$x \equiv x_0 \pmod{2^{l-1}} \qquad \text{o bien} \qquad x \equiv -x_0 \pmod{2^{l-1}} \, ,$$

pero no ambas. En total, hay, a lo sumo, cuatro soluciones en el rango $0 \leq x \leq 2^l - 1$, para cada m que admite alguna solución. Cada clase $m \equiv 1 \pmod 8$ contiene a lo sumo cuatro clases módulo 2^l, entonces los 2^{l-1} valores impares se subdividen en 2^{l-3} clases conteniendo a lo sumo cuatro elementos cada una. En definitiva, cada clase debe contener exactamente cuatro elementos. O sea, para $m \equiv 1 \pmod 8$, la ecuación $x^2 \equiv m \pmod{2^l}$ tiene solución y la cantidad de soluciones es exactamente cuatro.

Sea $p > 2$. Si $(n/p) = -1$, la ecuación $x^2 \equiv n \pmod p$ no tiene solución y, en particular, $x^2 \equiv n \pmod{p^l}$ no tiene solución; también vale $1 + (n/p) = 0$. Si $0 \leq x \leq p^l - 1$, $p \nmid x$, y m representa la clase de x^2 módulo p^l, entonces $(m/p) = 1$; hay, inductivamente, exactamente $\frac{p-1}{2} p^{l-1}$ valores de m en el rango $0 \leq m \leq p^l - 1$ tales que

$(m/p) = 1$. Para cada uno de ellos, o bien $x^2 \equiv m$ no tiene solución, o bien existe x_0 tal que $x_0^2 \equiv m$. En este último caso, cualquier otro valor de x tal que $x^2 \equiv m$ cumple:

$$x^2 \equiv x_0^2 \,(\mathsf{mod}\, p^l) \qquad \text{y} \qquad p^l \quad \text{divide a} \quad (x - x_0)\,(x + x_0)\ .$$

Pero p no divide a ambos, $(x - x_0)$ y $(x + x_0)$, pues la suma es $(x - x_0) + (x + x_0) = 2x$, que no es divisible por p. Dicho de otra manera,

$$x \equiv x_0 \,(\mathsf{mod}\, p^l) \qquad \text{o bien} \qquad x \equiv -x_0 \,(\mathsf{mod}\, p^l)\ ,$$

pero no ambas. En total hay, a lo sumo, dos soluciones en el rango $0 \le x \le p^l - 1$ para cada m que admite alguna solución. Los $(p-1)\,p^{l-1}$ elementos en el rango, no divisibles por p se separan en $\frac{p-1}{2}\,p^{l-1}$ clases, cada una con, a lo sumo, dos elementos. En definitiva, cada clase debe contener exactamente dos elementos. O sea, para m tal que $(m/p) = 1$, la ecuación $x^2 \equiv m \,(\mathsf{mod}\, p^l)$ tiene solución y la cantidad de soluciones es exactamente dos. En este caso, también vale $1 + (n/p) = 2$. □

Corolario 1.13. *Sean $m > 0$ y n un entero tal que $(n : m) = 1$. La cantidad de soluciones a (1) es*

- *0, si $4 \mid m$, $8 \nmid m$ y $n \equiv 3 \,(\mathsf{mod}\, 4)$,*
- *0, si $8 \mid m$ y $n \not\equiv 1 \,(\mathsf{mod}\, 8)$,*
- *0, si m es divisible por algún primo impar p tal que $(n/p) = -1$;*

en otro caso, si $s = \#\{p > 2 : \ \text{primo, } p|m\}$, la cantidad de soluciones es:

- *2^s, si $4 \nmid m$,*
- *2^{s+1}, si $4 \mid m$, pero $8 \nmid m$,*
- *2^{s+2}, si $8 \mid m$.*

1.2 El símbolo de Jacobi y el símbolo de Kronecker

Definición 1.14. Sea $m > 0$ un entero impar y sea $m = \prod_p p^{v_p(m)}$ la factorización de m como producto de primos a potencias. Si $(n : m) = 1$, entonces definimos el *símbolo de Jacobi de m en n*[3] como

$$\left(\frac{n}{m}\right) := \prod_p \left(\frac{n}{p}\right)^{v_p(m)}\ .$$

Teorema 1.15. [4] *Si $n \equiv n' \,(\mathsf{mod}\, m)$, entonces*

$$\left(\frac{n}{m}\right) = \left(\frac{n'}{m}\right)\ .$$

[3] ¿o de n en m?

[4] C.f. Teorema 1.3

Teorema 1.16. *Si* $(n : m) = (n : m') = 1$, $m, m' > 0$ *enteros impares, entonces*

$$\left(\frac{n}{m}\right)\left(\frac{n}{m'}\right) = \left(\frac{n}{mm'}\right) .$$

Demostración. La definición es completamente multiplicativa en m. □

Teorema 1.17. [5] *Si* $m > 0$ *es impar y* $(n : m) = (n' : m) = 1$, *entonces*

$$\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right) = \left(\frac{nn'}{m}\right) .$$

Teorema 1.18. [6] *Si* $m > 0$ *es impar, entonces*

$$\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}} .$$

Esto no quiere decir que -1 es un residuo cuadrático módulo m si y sólo si el símbolo de Jacobi es $(-1/m) = 1$: los residuos cuadráticos módulo 9 son 1, 4 y 7, pero $(-1/9) = \big((-1/3)\big)^2 = 1$, independientemente del valor de $(-1/3)$.

Demostración. Si $u_1, \ldots, u_r$ son impares, entonces

$$\Big(\prod_{i=1}^{r} u_i\Big) - 1 \equiv \sum_{i=1}^{r} (u_i - 1) \,(\mathsf{mod}\, 4) .$$

□

Teorema 1.19. [7] *Si* $m > 0$ *es impar, entonces*

$$\left(\frac{2}{m}\right) = (-1)^{\frac{m^2-1}{8}} .$$

Demostración. Si $u_1, \ldots, u_r$ son impares, entonces

$$\Big(\prod_{i=1}^{r} u_i^2\Big) - 1 \equiv \sum_{i=1}^{r} (u_i^2 - 1) \,(\mathsf{mod}\, 64) .$$

En particular, la congruencia vale módulo 16. □

Teorema 1.20. [8] *Si* $m, n > 0$ *son enteros imapres y coprimos, entonces*

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\,\frac{n-1}{2}} .$$

[5] C.f. Teorema 1.6
[6] C.f. Teorema 1.7
[7] C.f. Teorema 1.9
[8] C.f. Teorema 1.10

Teorema 1.21 (El primo arquimedeano)**.** *Sean $m, n \in \mathbb{Z}$ enteros impares (no necesariamente positivos), tales que $(m : n) = 1$. Entonces,*

$$\left(\frac{m}{|n|}\right)\left(\frac{n}{|m|}\right) = \begin{cases} -(-1)^{\frac{m-1}{2}\,\frac{n-1}{2}} & , \quad si\ m < 0\ y\ n < 0\ , \\ (-1)^{\frac{m-1}{2}\,\frac{n-1}{2}} & , \quad si\ m > 0\ o\ n > 0\ . \end{cases}$$

Definición 1.22. Sea $d \in \mathbb{Z}$ un entero que satisface:

- $d \equiv 0 \,(\mathsf{mod}\, 4)$ o bien $d \equiv 1 \,(\mathsf{mod}\, 4)$ y
- d no es un cuadrado perfecto

y sea $m > 0$ un entero. Definimos el *símbolo de Kronecker* (d/m) de la siguiente manera:

- si $m = 1$,
$$\left(\frac{d}{1}\right) = 1\ ;$$
- si $m = p$ es primo (incluyendo $p = 2$) y $p \mid d$, entonces
$$\left(\frac{d}{p}\right) = 0\ ;$$
- si $m = p$ es un primo *impar* (y no divide a d),
$$\left(\frac{d}{p}\right) = \left(\frac{d}{p}\right)$$
el símbolo de Legendre;
- si $m = 2$ (y no divide a d),
$$\left(\frac{d}{2}\right) = \left(\frac{2}{|d|}\right) = \begin{cases} 1 & , \quad \text{si } d \equiv 1 \,(\mathsf{mod}\, 8)\ , \\ -1 & , \quad \text{si } d \equiv 5 \,(\mathsf{mod}\, 8)\ ; \end{cases}$$
- si $m = \prod_p p^{v_p(m)}$ es la factorización de m como producto de primos (incluyendo 2) a potencias,
$$\left(\frac{d}{m}\right) = \prod_p \left(\frac{d}{p}\right)^{v_p(m)}\ .$$

Observación 1.23. (a) El símbolo de Kronecker $\left(\frac{d}{m}\right)$ se define sólo para ciertos valores de d ¿Por qué no se define para todo entero? (b) El símbolo de Kronecker $\left(\frac{d}{m}\right)$ se define para valores primos de m y luego se extiende de manera totalmente multiplicativa.

Teorema 1.24. *Si $d \in \mathbb{Z}$ está en las condiciones de la Definición 1.22 y $m_1, m_2 > 0$ son enteros, entonces*

$$\left(\frac{d}{m_1 m_2}\right) = \left(\frac{d}{m_1}\right)\left(\frac{d}{m_2}\right) .$$

Teorema 1.25. *Sean $k, d \in \mathbb{Z}$ tales que d está en las condiciones de la Definición 1.22 y $k > 0$, $(k : d) = 1$. Entonces, la cantidad de soluciones a la ecuación*

$$x^2 \equiv d \,(\mathsf{mod}\, 4k) \tag{9}$$

es igual a

$$2 \sum_{f|k}{}' \left(\frac{d}{f}\right) , \tag{10}$$

donde la suma se realiza sobre los divisores positivos y libres de cuadrados *de k (incluyendo $f = 1$).*[9]

Demostración. La cantidad de soluciones de (9) es igual al producto de la cantidad de soluciones de $x^2 \equiv d \,(\mathsf{mod}\, p^l)$ sobre las potencias de primos p^l que dividen exactamente a $4k$, es decir, $l = v_p(4k)$.

Si p es un primo impar, entonces $v_p(4k) = v_p(k)$ y, como $(k : d) = 1$, si $v_p(k) > 0$, entonces $p \nmid d$. En tal caso, la cantidad de soluciones a la ecuación

$$x^2 \equiv d \,(\mathsf{mod}\, p^l) ,$$

donde $l = v_p(4k)$ es igual a:

$$1 + \left(\frac{d}{p}\right) ,$$

donde (d/p) se puede interpretar como el símbolo de Legendre o bien como el símbolo de Kronecker.

Si $p = 2$, entonces $l = v_2(4k) = 2 + v_2(k)$ y el exponente l es $l \geq 2$ en general y es $l \geq 3$, si y sólo si $2 \mid k$. Separamos en casos. Si d es impar, entonces $d \equiv 1 \,(\mathsf{mod}\, 4)$ y $(4k : d) = 1$. Si $2 \nmid k$, entonces la ecuación admite exactamente dos soluciones módulo $2^l = 4$; si $2 \mid k$, entonces, o bien la ecuación módulo 2^l $(l \geq 3)$ admite soluciones y la cantidad de soluciones es 4, o bien no admite soluciones –el primer caso ocurre cuando $d \equiv 1 \,(\mathsf{mod}\, 8)$ y el segundo si $d \equiv 5 \,(\mathsf{mod}\, 8)$. En definitiva, la cantidad de soluciones para

$$x^2 \equiv d \,(\mathsf{mod}\, 2^l) ,$$

donde $l = v_2(4k)$ es igual, cuando d es impar, a:

$$\begin{cases} 2 \quad , & \text{si } 2 \nmid k \quad \text{o} \\ 2\left(1 + \left(\dfrac{d}{2}\right)\right) \quad , & \text{si } 2 \mid k \ . \end{cases}$$

[9] Podemos expresar la cantidad de soluciones usando la función de Möbius como $2 \sum_{f|k} |\mu(f)| \, (d/f)$.

Si d es par, entonces $d \equiv 0 \,(\mathsf{mod}\, 4)$ y la condición $(k : d) = 1$ implica que $2 \nmid k$. En este caso, $l = v_2(4k) = 2$ y la cantidad de soluciones módulo $4 = 2^l$ es 2: la ecuación

$$x^2 \equiv 0 \,(\mathsf{mod}\, 4)$$

tiene las soluciones $x \equiv 0$ y $x \equiv 2$.

En conclusión, independientemente de la paridad de d, la cantidad de soluciones para (9) es igual a:

$$2 \prod_{p|k} \left(1 + \left(\frac{d}{p}\right)\right)$$

(incluyendo $p = 2$, si $2 \mid k$), que es igual a la expresión (10). Notamos que el divisor $f = 1$ debe ser incluido. □

Observación 1.26. Si x_0 verifica (9), también $x_0 + 2k$ es una solución. En consecuencia, la suma $\sum'_{f|k} (d/f)$ (sin el factor 2) es igual a la cantidad de soluciones a (9) en el intervalo $0 \leq x < 2k$.

Dado d en las condiciones de la Definición 1.22, sea

$$a := |d| \ .$$

A continuación enunciamos algunas propiedades del símbolo de Kronecker que lo relacionan con el símbolo de Jacobi.

Proposición 1.27. *Sea $d \in \mathbb{Z}$ en las condiciones de la Definición 1.22 y sea $m > 0$ un entero coprimo con d. Entonces,*

- *si d es impar,*
$$\left(\frac{d}{m}\right) = \left(\frac{m}{a}\right) \ ;$$
- *si d es par, $d = 2^b u$, $2 \nmid u$ y $v = |u|$,*
$$\left(\frac{d}{m}\right) = \left(\frac{2}{m}\right)^b (-1)^{\frac{u-1}{2}\,\frac{m-1}{2}} \left(\frac{m}{v}\right) \ .$$

En el lado izquierdo, aparece el símbolo de Kronecker y, en el lado derecho, el símbolo de Jacobi.

Demostración. Si $m = 1$, $(d/1) = 1 = (1/a)$. Si $m = 2$, $(d/2) = (2/|d|) = (2/a)$. Si $m = p$, primo impar, $(d/p) = (d/p) = (d/p)$ (Kronecker, Jacobi, Legendre). Si, más aun, d es impar, $d \equiv 1 \,(\mathsf{mod}\, 4)$ y $(p : d) = 1$, entonces: si $d > 0$,

$$\left(\frac{d}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{d-1}{2}} \left(\frac{p}{d}\right) = \left(\frac{p}{d}\right) ;$$

si $d<0$, $a=|d|\equiv 3\,(\mathsf{mod}\,4)$ y

$$\left(\frac{d}{p}\right) \;=\; \left(\frac{a}{p}\right)(-1)^{\frac{p-1}{2}} \;=\; (-1)^{\frac{a+1}{2}\,\frac{p-1}{2}}\left(\frac{p}{a}\right) \;=\; \left(\frac{p}{a}\right)\,.$$

Queda ver el caso d par y $m=p$ primo impar; el caso general se deduce de que $(m:d)=1$ y la completa multiplicatividad de los símbolos de Jacobi y de Kronecker. Pero, si $d=2^b\,u$, $2\nmid u$ y $v=|u|$, entonces

$$\left(\frac{d}{p}\right) \;=\; \left(\frac{2}{p}\right)^b\left(\frac{u}{p}\right)\,,$$

con lo cual basta aplicar la reciprocidad a (v/p):

$$\left(\frac{u}{p}\right) \;=\; \begin{cases} \left(\dfrac{p}{u}\right)(-1)^{\frac{u-1}{2}\,\frac{p-1}{2}} \quad , & \text{si } u>0 \quad \text{y} \\ \left(\dfrac{v}{p}\right)(-1)^{\frac{p-1}{2}} \;=\; \left(\dfrac{p}{v}\right)(-1)^{\frac{v+1}{2}\,\frac{p-1}{2}} \quad , & \text{si } u<0\,. \end{cases}$$

Si $u>0$, entonces $v=u$ y $(p/u)=(p/v)$; si $u<0$, entonces $v=-u$ y $\frac{v+1}{2}\equiv\frac{u-1}{2}\,(\mathsf{mod}\,4)$. □

Teorema 1.28. *Si $d\in\mathbb{Z}$ está en las condiciones de la Definición 1.22, entonces,*

1. *si $(m:d)>1$, $(d/m)=0$;*
2. *$(d/1)=1\neq 0$;*
3. *$(d/m_1)\,(d/m_2)=(d/m_1m_2)$;*
4. *si $m_1\equiv m_2\,(\mathsf{mod}\,a)$, $(d/m_1)=(d/m_2)$;*
5. *existe m tal que $(d/m)=-1$.*

Demostración. Las propiedades (1) y (2) son parte de la definición del símbolo, esencialmente. La propiedad (3) fue enunciada en el Teorema 1.24.

Veamos (4). Si $(m_1:a)>1$, entonces $(m_2:a)>1$, también y $(d/m_1)=0=(d/m_2)$. En caso contrario, ambos, m_1 y m_2 son coprimos con a. Aplicamos, entonces, la Proposición 1.27: si d es impar,

$$\left(\frac{d}{m_1}\right) \;=\; \left(\frac{m_1}{a}\right) \;=\; \left(\frac{m_2}{a}\right) \;=\; \left(\frac{d}{m_2}\right)\,,$$

usando la periodicidad (Teorema 1.15) del símbolo de Jacobi; si, en cambio, d es par, debemos comparar

$$\begin{aligned} \left(\frac{d}{m_1}\right) \;&=\; \left(\frac{2}{m_1}\right)^b(-1)^{\frac{u-1}{2}\,\frac{m_1-1}{2}}\left(\frac{m_1}{v}\right) \qquad \text{con} \\ \left(\frac{d}{m_2}\right) \;&=\; \left(\frac{2}{m_2}\right)^b(-1)^{\frac{u-1}{2}\,\frac{m_2-1}{2}}\left(\frac{m_2}{v}\right)\,. \end{aligned}$$

Pero $m_1 \equiv m_2 \pmod{a}$ implica $m_1 \equiv m_2 \pmod{v}$ (pues $v \mid a$) e implica $m_1 \equiv m_2 \pmod{4}$ (pues $4 \mid a$). Entonces,

$$\left(\frac{m_1}{v}\right) = \left(\frac{m_2}{v}\right) \qquad \text{y} \qquad (-1)^{\frac{u-1}{2}\,\frac{m_1-1}{2}} = (-1)^{\frac{u-1}{2}\,\frac{m_2-1}{2}} .$$

Resta comparar los símbolos en 2. Notemos que $b \geq 2$. Como el símbolo de Kronecker toma valores ± 1 (o bien 0), podemos asumir que $b > 2$ (o, más aun, impar). Pero, en tal caso, como $8 \mid a$, se cumple $m_1 \equiv m_2 \pmod{8}$ y

$$\left(\frac{2}{m_1}\right) = (-1)^{\frac{m_1^2-1}{8}} = (-1)^{\frac{m_2^2-1}{8}} = \left(\frac{2}{m_2}\right) .$$

Para probar (5), alcanza aplicar la Proposición 1.27 con un valor adecuado de m. □

Teorema 1.29. *Si $d \in \mathbb{Z}$ está en las condiciones de la Definición 1.22 y $a = |d|$, entonces*

$$\left(\frac{d}{a-1}\right) = \begin{cases} 1 \quad , & \text{si } d > 0 \quad \text{y} \\ -1 \quad , & \text{si } d < 0 \ . \end{cases}$$

Teorema 1.30. *Si $n, m > 0$ cumplen $n \equiv -m \pmod{a}$, entonces*

$$\left(\frac{d}{n}\right) = \begin{cases} \left(\dfrac{d}{m}\right) \quad , & \text{si } d > 0 \quad \text{y} \\ -\left(\dfrac{d}{m}\right) \quad , & \text{si } d < 0 \ . \end{cases}$$

En particular, podemos extender el símbolo de Kronecker (d/n) de manera que admita valores negativos de n, de la siguiente manera:

$$\left(\frac{d}{-1}\right) = \begin{cases} 1 \quad , & \text{si } d > 0 \quad \text{y} \\ -1 \quad , & \text{si } d < 0 \ . \end{cases} \tag{11}$$

1.3 La ecuación de Pell

El objetivo de esta sección es resolver la ecuación

$$x^2 - d\,y^2 = 1 \ , \tag{12}$$

para un entero $d \in \mathbb{Z}$ fijo y valores enteros de las variables x, y. Los pares $(x, y) = (\pm 1, 0)$ son soluciones para cualquier valor de d.

Observación 1.31. Si $d = -1$, entonces la ecuación (12) tiene como únicas soluciones los pares $(\pm 1, 0)$ y $(0, \pm 1)$. Si $d < -1$, entonces, o bien $y = 0$ y $x \in \{\pm 1\}$, o bien $|y| \geq 1$ y $-d\,y^2 > 1$, lo que no da lugar a nuevas soluciones.

Si $d = a^2 > 0$ con $a \in \mathbb{Z}$, entonces la ecuación (12) es igual a:

$$1 = x^2 - d\,y^2 = (x - a\,y)\,(x + a\,y)$$

con lo que, una condición necesaria para que $(x, y) \in \mathbb{Z}^2$ sea solución es que $x - a\,y = x + a\,y \in \{\pm 1\}$. En tal caso, como $x = \frac{(x-a\,y)+(x+a\,y)}{2}$, se debe cumplir $x \in \{\pm 1\}$. Los pares $(x, y) = (\pm 1, 0)$ son las únicas soluciones.

Si $d = 0$, la ecuación es $x^2 = 1$, que tiene como únicas soluciones los pares $(\pm 1, y)$, con $y \in \mathbb{Z}$ arbitrario.

Observación 1.32. En general, los pares $(x, y) = (\pm 1, 0)$ son las únicas soluciones con $y = 0$. Si $(0, y)$ es solución, entonces $-d\,y^2 = 1$, con lo que $d = -1$ e $y \in \{\pm 1\}$. El único caso en donde $(0, y)$ es una solución es cuando $d = -1$ y, en ese caso, $y \in \{\pm 1\}$ da lugar a las únicas dos soluciones de esa forma.

De ahora en adelante, asumimos $d > 0$ y no cuadrado. Dado que cada par (x, y), $xy \neq 0$, que sea solución de (12) da lugar a las cuatro soluciones (x, y), $(-x, y)$, $(x, -y)$ y $(-x, -y)$, será suficiente conocer las soluciones con $x > 0$ e $y > 0$.

Teorema 1.33. *Sea $\alpha \in \mathbb{R}$ un número real y sea $m > 0$ un entero. Existen valores enteros de x e y tales que*

$$|x - \alpha\,y| < \frac{1}{m} \qquad y \qquad 0 < y \leq m\ .$$

Demostración. Si $u, v \in \mathbb{Z}$ y cumplen $0 \leq v \leq m$ y $u := \lfloor \alpha\,v \rfloor + 1$, entonces

$$0 < u - \alpha\,v \leq 1\ .$$

Dividiendo el intervalo $(\ 0, 1\ ]$ en los subintervalos

$$\Big(\ \frac{h}{m}, \frac{h+1}{m}\ \Big] \qquad (\ 0 \leq h \leq m-1\ ),$$

cada uno de ellos debe contener, al menos, dos de las expresiones $u - \alpha\,v$.[10] Así, existen $0 \leq v_1 < v_2 \leq m$ tales que

$$|(u_2 - \alpha\,v_2) - (u_1 - \alpha\,v_1)| < \frac{1}{m}\ .$$

Si $x = u_2 - u_1$ e $y = v_2 - v_1$, entonces $0 < y \leq m$ y $|x - \alpha\,y| < 1/m$. □

Teorema 1.34. *La desigualdad*

$$|x - \sqrt{d}\,y| < \frac{1}{y} \tag{13}$$

tiene infinitas soluciones con $x, y \in \mathbb{Z}$.

[10] O bien $u_1 - \alpha\,v_1 = u_2 - \alpha\,v_2$ para dos valores distintos $v_1 \neq v_2$, o bien la expresión $u - \alpha\,v$ toma $m + 1$ valores distintos en $(\ 0, 1\ ]$ que caen en m subintervalos. En el primer caso, $\alpha \in \mathbb{Q}$.

Demostración. Si $\alpha = \sqrt{d}$ (irracional) y $m = 1$, existen, por el Teorema 1.33, x_0, y_0 tales que $|x_0 - \sqrt{d}\, y_0| < 1$. De hecho, $x_0 = \left\lfloor \sqrt{d} \right\rfloor$ e $y_0 = 1$ sirven.

Dada una solución (x', y') con $y' > 0$ de la desigualdad (13), existen x e $y > 0$ tales que

$$|x - \sqrt{d}\, y| \ < \ |x' - \sqrt{d}\, y'| \ .$$

Para ver esto, elegir $m \geq 1$ tal que $1/m < |x' - \sqrt{d}\, y'|$, lo cual tiene sentido, porque $|x' - \sqrt{d}\, y'| \neq 0$ ($\sqrt{d}$ es irracional, $y' \neq 0$ y $x' \in \mathbb{Z}$). Por el Teorema 1.33, existen $x, y \in \mathbb{Z}$ tales que $0 < y \leq m$ y

$$|x - \sqrt{d}\, y| \ < \ \frac{1}{m} \begin{cases} < \ |x' - \sqrt{d}\, y'| & \text{y} \\ \leq \ \frac{1}{y} & . \end{cases}$$

□

En la demostración, no usamos que x', y' satisfacen $|x' - \sqrt{d}\, y'| < 1/y'$ para definir la nueva solución x, y; solamente usamos que $|x' - \sqrt{d}\, y'| \neq 0$.

Teorema 1.35. *Existe un valor entero $k = k(d) \neq 0$ para el cual la igualdad*

$$x^2 \ - \ d\, y^2 \ = \ k \tag{14}$$

tiene infinitas soluciones con $x, y \in \mathbb{Z}$ y ambos *positivos.*

Demostración. Sabemos, por el Teorema 1.34, que existen infinitos valores de $x, y \in \mathbb{Z}$ ($y > 0$) que verifican $|x - \sqrt{d}\, y| < 1/y$. Dado un par (x, y) que verifica esta desigualdad, podemos ver que

$$|x + \sqrt{d}\, y| \ \leq \ |x - \sqrt{d}\, y| + 2\sqrt{d}\, y \ < \ \frac{1}{y} + 2\sqrt{d}\, y \ \leq \ (1 + 2\sqrt{d})\, y \ .$$

En consecuencia,

$$0 \ < \ |x^2 - d\, y^2| \ < \ 1 + 2\sqrt{d} \ . \tag{15}$$

Existen finitos valores de $k \in \mathbb{Z}$ tales que $0 < |k| < 1 + 2\sqrt{d}$ (y hay al menos cuatro). Pero la cantidad de pares (x, y) que verifican (13) (y, por lo tanto, (15)) es infinita. Entonces, se debe cumplir (14) para infinitos pares (x, y) que cumplen (13), para *algún* valor de k. Además, como $|x - \sqrt{d}\, y| < 1/y$ e $y > 0$ implican $x > 0$, sabemos que para *ese* valor de k hay infinitas soluciones con $x > 0$ e $y > 0$. □

Notamos que los valores de k se pueden acotar, efectivamente, por $1 + 2\sqrt{d}$, si fuese de utilidad.

Teorema 1.36. *La ecuación* (12) *tiene, al menos, una solución con $y \neq 0$. En particular, admite al menos una solución con x e y ambos positivos.*

Demostración. Sea $k \in \mathbb{Z}$ ($0 < |k| < 1 + 2\sqrt{d}$) como en el Teorema 1.35, para el cual existen infinitos pares (x, y), $x > 0$ e $y > 0$, tales que $x^2 - d\, y^2 = k$. Estos infinitos pares se separan en $|k|^2$ clases, tomando módulo $|k|$ en cada coordenada. Si (x_1, y_1) y (x_2, y_2) son dos pares distintos que cumplen

- $x_1^2 - d\,y_1^2 = x_2^2 - d\,y_2^2 = k$ $(k \neq 0)$,
- $x_1, x_2, y_1, y_2 > 0$,
- $x_1 \equiv x_2 \,(\mathsf{mod}\,|k|)$ e $y_1 \equiv y_2 \,(\mathsf{mod}\,|k|)$ y
- $x_1 \neq x_2$ o bien $y_1 \neq y_2$,

y definimos

$$x \,:=\, \frac{x_1x_2 - dy_1y_2}{k} \qquad \text{e} \qquad y \,:=\, \frac{x_1y_2 - y_1x_2}{k}\ ,$$

entonces el par (x, y) cumple:

- $x, y \in \mathbb{Z}$,
- $x^2 - d\,y^2 = 1$ e
- $y \neq 0$.

□

Sea $\mathsf{Nm} : \mathbb{Q}(\sqrt{d})^\times \to \mathbb{Q}^\times$ la norma de la extensión:

$$\mathsf{Nm}(x + \sqrt{d}\,y) \,=\, x^2 \,-\, d\,y^2 \qquad (\ x, y \in \mathbb{Q}\ ).$$

Resolver la ecuación (12) es, esencialmente, hallar todos los elementos de $\mathbb{Q}(\sqrt{d})$ de la forma $x + \sqrt{d}\,y$ con $x, y \in \mathbb{Z}$ y de norma igual a 1, es decir, hallar las unidades de norma 1 en el orden $\mathbb{Z}[\sqrt{d}]$. Esto no es lo mismo que hallar las unidades de norma 1 en el anillo de enteros de la extensión, porque $\mathbb{Z}[\sqrt{d}]$ podría ser un suborden propio del anillo de enteros. En todo caso, vamos a usar que Nm es un morfismo de grupos.

El siguiente resultado es que las soluciones de (12) forman un grupo, esencialmente; mejor dicho, que el conjunto de soluciones es cerrado por el producto. Porque puede ser útil, generalizamos un poco el problema: buscamos $x, y \in \mathbb{Z}$ tales que

$$x^2 \,-\, d\,y^2 \,=\, t\,h^2\ . \tag{16}$$

En (16), $t, h \in \mathbb{Z}$. Tenemos en mente el caso $t \in \{\pm 1\}$ y $h \in \{1, 2\}$, pero podría ser general. Seguimos asumiendo que $d > 0$ y libre de cuadrados; en particular, para $h = 0$ no hay soluciones.

Teorema 1.37. *Si $x_1^2 - d\,y_1^2 = x_2^2 - d\,y_2^2 = h^2$ y $r^2 - d\,s^2 = t$, entonces el par (x_3, y_3) determinado por:*

$$(r + \sqrt{d}\,s)\left(\frac{x_1 + \sqrt{d}\,y_1}{h}\right)\left(\frac{x_2 + \sqrt{d}\,y_2}{h}\right) \,=\, \frac{x_3 + \sqrt{d}\,y_3}{h} \tag{17}$$

es una solución de (16).

Demostración. Aplicar Nm en la identidad que sirve de definición de (x_3, y_3). □

En particular, si (x_1, y_1) y (x_2, y_2) son soluciones de (16) con $t = h = 1$, entonces el par (x_3, y_3) definido por

$$\pm\,(x_1 + \sqrt{d}\,y_1)\,(x_2 + \sqrt{d}\,y_2) \;=\; x_3 + \sqrt{d}\,y_3 \;,$$

para cualquier elección del signo $\pm$, también es una solución de la misma ecuación.

El siguiente resultado permite subdividir el conjunto de soluciones de manera conveniente.

Teorema 1.38. *Si (x, y) es una solución a (16) con $t = 1$ e $y \neq 0$ y si definimos*

$$\eta \;:=\; \frac{x + \sqrt{d}\,y}{h} \;,$$

entonces, los signos de las coordenadas y la ubicación de η en la recta real están relacionados según la Tabla 3.

$x > 0$ e $y > 0$	$1 < \eta$
$x > 0 > y$	$0 < \eta < 1$
$x < 0 < y$	$-1 < \eta < 0$
$x < 0$ e $y < 0$	$\eta < -1$

Tabla 3: Relación entre los signos de las coordenadas x e y y la ubicación de $\frac{x+\sqrt{d}\,y}{h}$ en la recta

Demostración. Si x e y son positivos, $x + \sqrt{d}\,y > x > h$, con lo cual $\eta > 1$. Si $x > 0$ e $y < 0$, entonces $x - \sqrt{d}\,y > h (> 0)$,[11] con lo cual

$$h^2 \;=\; x^2 \,-\, d\,y^2 \;=\; (x + \sqrt{d}\,y)\,(x - \sqrt{d}\,y) \;>\; 0 \quad \text{y}$$
$$1 \;>\; \frac{x + \sqrt{d}\,y}{h} \;>\; 0 \;.$$

Los otros dos casos se pueden ver cambiando el signo a ambas coordenadas y aplicando lo visto en estos dos casos. □

Observación 1.39. Si (x_1, y_1), (x_2, y_2) son soluciones de (16) con $t = 1$ y (r, s) es solución de (16) con $h = 1$, entonces, por el Teorema 1.37, el par (x_3, y_3) definido por (17) es una solución de (16), pero las coordenadas x_3 e y_3 son, *a priori*, racionales. Hay dos casos en los que podemos garantizar que, si x_1, x_2, y_1 e y_2 son enteros entonces x_3 e y_3 también lo son:

- $t = 1$, $(r, s) = (\pm 1, 0)$ y $h = 1$ y
- $t = 1$, $(r, s) = (\pm 1, 0)$ y $h = 2$.

[11] $\bar{\eta} > 1$

Si $t = 1$ y $(r, s) = (\pm 1, 0)$, entonces

$$x_3 \,=\, \pm\frac{x_1x_2 + dy_1y_2}{h} \qquad \text{y} \qquad y_3 \,=\, \pm\frac{x_1y_2 + y_1x_2}{h}\ .$$

Si $h = 1$, no hay nada que probar. Si $h = 2$, entonces $x_1 \equiv x_1^2 = d\,y_1^2 + 4 \equiv d\,y_1 \,(\mathsf{mod}\,2)$, de lo que se deduce que

$$\begin{aligned} x_1x_2 + dy_1y_2 \;&\equiv\; d^2\,y_1y_2 + dy_1y_2 \;\equiv\; d\,y_1y_2 + d\,y_1y_2 \;\equiv\; 0\,(\mathsf{mod}\,2) \quad \text{y} \\ x_1y_2 + y_1x_2 \;&\equiv\; d\,y_1y_2 + d\,y_1y_2 \;\equiv\; 0\,(\mathsf{mod}\,2)\ . \end{aligned}$$

Como consecuencia, también es cierto que, si $t \in \{\pm 1\}$ y $(r, s) \in \mathbb{Z}^2$ es solución entera de $r^2 - d\,s^2 \,=\, t$, entonces la expresión (17) define, si $h \,\in\, \{1, 2\}$, una solución *con coordenadas enteras* de la ecuación (16) con $h \in \{1, 2\}$ y $t \in \{\pm 1\}$, según corresponda.

De ahora en adelante, suponemos $t = 1$ y $h \in \{1, 2\}$. Todas las soluciones de (12) se obtienen a partir de una solución fundamental.[12]

Teorema 1.40. *Sea (x_0, y_0) una solución de (16) con $t = 1$ y $h \in \{1, 2\}$ tal que $x_0 > 0$ e $y_0 > 0$ y, además, y_0 toma el valor más chico posible.*[13] *Entonces, la solución general a (16) con $t = 1$ y $h \in \{1, 2\}$ es (x, y) definido por*

$$\pm\,\Big(\frac{x_0 + \sqrt{d}\,y_0}{h}\Big)^n \,=\, \frac{x + \sqrt{d}\,y}{h} \qquad (\ n \in \mathbb{Z}\ ). \tag{18}$$

Demostración. La expresión (18) define soluciones a (16), por el Teorema 1.37, y, en este caso, como $t = 1$ y $h \in \{1, 2\}$, las coordenadas x e y son enteras, por la Observación 1.39. Resta ver que toda solución se obtiene de esta manera. Sea ϵ la solución fundamental:

$$\epsilon \,=\, \frac{x_0 + \sqrt{d}\,y_0}{h}\ .$$

Las soluciones $(x, y) = (\pm h, 0)$ son de la forma (18) con $n = 0$. Dejamos de lado estas soluciones y nos concentramos en aquellas soluciones con $y \neq 0$. Dado que $(\frac{x+\sqrt{d}\,y}{h})^{-1} = \frac{x-\sqrt{d}\,y}{h}$, si $x^2 - d\,y^2 = h^2$ y dado que, por el Teorema 1.38, $\epsilon > 1$, alcanzará con probar que todas las soluciones (x, y) que verifiquen $x + \sqrt{d}\,y > h$ son de la forma

$$\frac{x + \sqrt{d}\,y}{h} \,=\, \epsilon^n\ ,$$

con $n > 0$.[14]

[12] Quisiera decir "primitiva", pero no sería en el mismo sentido en que se usa esta palabra en otros contextos (cercanos a este mismo problema).

[13] Como $y_0 \in \mathbb{Z}_{\geq 1}$, *hay* un valor más chico.

[14] El resto de las soluciones se obtiene negando o invirtiendo estas soluciones. La condición sobre $x + \sqrt{d}\,y$ equivale a $x > 0$ e $y > 0$, por el Teorema 1.38.

El argumento consiste en probar que ϵ es la solución más chica en la semirecta $(1, +\infty)$. Sea (x, y) una solución con $x > 0$ e $y > 0$ y sea $\eta = \frac{x+\sqrt{d}\,y}{h} > 1$. Por la minimalidad de ϵ, se cumple que $\eta \geq \epsilon$. En caso contrario, $\epsilon > \eta > 1$ y

$$(x_0 - x) \,>\, \sqrt{d}\,(y - y_0) \;.$$

Como estamos asumiendo $x, y > 0$, debe ser $y \geq y_0$ y, por lo tanto, $x_0 > x$. Si $y = y_0$, entonces

$$x^2 \,=\, h^2 + d\,y_0^2 \,=\, x_0^2 \;,$$

con lo que $x = x_0$, pues ambos tienen el mismo signo. Si $y > y_0$, entonces

$$x^2 \,>\, h^2 + d\,y_0^2 \,=\, x_0^2 \;,$$

con lo cual $x > x_0$, pues ambos son positivos. En ambos casos, se llega a una condición que contradice $x_0 > x$. El absurdo viene de asumir que $\eta < \epsilon$.

Como $\epsilon > 1$, existe un (único) $n \geq 1$ tal que

$$\epsilon^n \,\leq\, \eta \,<\, \epsilon^{n+1} \;.$$

Así, $1 \leq \eta' := \eta\,\epsilon^{-n} < \epsilon$ es una nueva solución. Pero, entonces $\eta' = 1$, por el argumento del párrafo anterior. □

El problema de hallar todas las unidades de norma 1 en el anillo de enteros de $\mathbb{Q}(\sqrt{d})$ queda resuelto al resolver *ambas* ecuaciones $x^2 - d\,y^2 = h^2$ con $h \in \{1, 2\}$ para valores enteros de x y de y.

Observación 1.41. El conjunto de pares $(x, y) \in \mathbb{Q}^2$ tales que $x^2 - d\,y^2 = h^2$ $(t = 1)$ forma un grupo. Sea

$$G \,:=\, \big\{\mathsf{Nm} = 1\big\} \,\subset\, \mathbb{Q}(q)^\times \;.$$

Cada elemento de G tiene una única expresión de la forma $u + \sqrt{d}\,v$ con $u, v \in \mathbb{Q}$. Definiendo $x = h\,u$ e $y = h\,v$, queda determinada una correspondencia entre elementos de G y pares $(x, y) \in \mathbb{Q}^2$ que satisfacen $x^2 - d\,y^2 = h^2$.

$$\mathsf{Nm}(u + \sqrt{d}\,v) \,=\, 1 \qquad \text{si y sólo si} \qquad x^2 \,-\, d\,y^2 \,=\, h^2 \;.$$

Es decir, vía la biyección[15]

$$\sigma(x, y) \,=\, \frac{x + \sqrt{d}\,y}{h} \;,$$

estamos trasladando la estructura de grupo de G a los pares (x, y); explícitamente, esto fue lo que hicimos en el Teorema 1.37, aprovechando la unicidad de la escritura de elementos de $\mathbb{Q}(\sqrt{q})$:

$$\sigma(x_1, y_1)\,\sigma(x_2, y_2) \,=\, \Big(\frac{x_1 + \sqrt{d}\,y_1}{h}\Big)\Big(\frac{x_2 + \sqrt{d}\,y_2}{h}\Big) \,=\, \sigma(x_3, y_3) \;,$$

[15] La función σ es una biyección. Si nos restringimos a x e y enteros es inyectiva; no estamos diciendo cuál es el conjunto del lado de la imagen con el que está en correspondencia.

donde

$$x_3 \,=\, \frac{x_1x_2 + d\,y_1y_2}{h} \qquad \text{e} \qquad y_3 \,=\, \frac{x_1y_2 + y_1x_2}{h}\ .$$

El neutro de este grupo es el par $(h,0)$, que corresponde a $1 \in G$; en cuanto al inverso,

$$\sigma(x,y)^{-1} \,=\, \Big(\frac{x+\sqrt{d}\,y}{h}\Big)^{-1} \,=\, \frac{x-\sqrt{d}\,y}{h} \,=\, \sigma(x,-y)\ .$$

Como mencionamos en la Observación 1.39, fijado $h \in \{1,2\}$,

- si $(x_1,y_1),(x_2,y_2) \in \mathbb{Z}^2$ entonces $\sigma(x_1,y_1)\sigma(x_2,y_2) = \sigma(x_3,y_3)$ con $(x_3,y_3) \in \mathbb{Z}^2$;
- si $(x,y) \in \mathbb{Z}^2$, $\sigma(x,y)^{-1} = \sigma(x,-y)$;
- en cuanto al neutro, $(h,0) \in \mathbb{Z}^2$

En definitiva, el conjunto de pares $(x,y) \in \mathbb{Z}^2$ tales que $x^2 - d\,y^2 = h^2$ (para un $h \in \{1,2\}$ fijo) es un subgrupo. El contenido del Teorema 1.40, expresado en estos términos, es que, si $\epsilon := \frac{x_0+\sqrt{d}\,y_0}{h}$, es decir, si

$$\epsilon \,:=\, \sigma(x_0,y_0)\ ,$$

donde $x_0 > 0$, $y_0 > 0$ e y_0 es el valor (entero) más chico posible, entonces el grupo de soluciones enteras (con la estructura dada por σ) es isomorfo a

$$\big\{\pm\,\epsilon^n \,:\, n \in \mathbb{Z}\big\} \,=\, \langle -1\rangle \,\times\, \langle \epsilon\rangle\ .$$

Observación 1.42. Un poco más en general, si conocemos una solución $(r,s) \in \mathbb{Z}^2$ a $r^2 - d\,s^2 = -1$, entonces todas las soluciones a $x^2 - d\,y^2 = -h^2$ se obtienen a partir de ella y del grupo de soluciones a $x^2 - d\,y^2 = h^2$ (seguimos asumiendo que $h \in \{1,2\}$ y que está fijo). Si (x_1,y_1) e (x_2,y_2) son soluciones enteras $x^2 - d\,y^2 = -h^2$, entonces

$$\sigma(x_1,y_1)\,\sigma(x_2,y_2)^{-1} \,=\, \sigma(x_1,y_1)\,\sigma(-x_2,y_2) \,=\, \sigma(x_3,y_3)$$

con $(x_3,y_3) \in \mathbb{Z}^2$, pues $-1 \equiv 1\,(\mathsf{mod}\,2)$. Pero $\mathsf{Nm}(\sigma(x_3,y_3)) = (-1)\,(-1)^{-1} = 1$, con lo cual (x_3,y_3) es una solución entera a la ecuación $x_3^2 - d\,y_3^2 = h^2$.

Pregunta. ¿Es cíclico el grupo de pares enteros (x,y) que verifica $\mathsf{Nm}(\sigma(x,y)) = \pm 1$?

Observación 1.43. Si $d < 0$, ya hemos dicho cómo son las soluciones a $x^2 - d\,y^2 = 1$ ¿Qué pasa con

$$x^2 \,-\, d\,y^2 \,=\, 4\ ? \tag{19}$$

Los pares $(\pm 2, 0)$ son solución, cualquiera sea d;

- si $d = -1$, entonces la ecuación (19) tiene como únicas soluciones los pares $(0,\pm 2)$ y $(\pm 2,0)$;
- si $d = -2$, no hay otras soluciones (módulo 8);

- si $d = -3$, las únicas soluciones son $\pm(\pm 1, 1)$ y $(\pm 2, 0)$;
- si $d = -4$, las únicas soluciones son $(0, \pm 1)$ y $(\pm 2, 0)$;
- si $d < -4$, no hay otras soluciones.

En la sección § 2.4, Observación 2.23, relacionaremos estos grupos con grupos de matrices.

2 Formas cuadráticas binarias

Usaremos la siguiente nomenclatura para referirnos a distintos conjuntos de formas y clases de formas, así como a sus respectivos cardinales, tratando de que resulten deescriptivos:

- $\mathsf{Clases}(d)$: el conjunto de clases de formas de discriminante d,
- $\mathsf{Clases}_g(d)$: el subconjunto de clases de formas de discriminante d y *contenido* $(a : b : c) = g$,
- $\mathsf{Primitivas}(d) = \mathsf{Clases}_1(d)$: el subconjunto de clases de formas *primitivas*.

2.1 El discriminante

Definición 2.1. Una *forma cuadrática binaria* es una expresión de la forma

$$\{a, b, c\} \;=\; a\,x^2 \;+\; b\,xy \;+\; c\,y^2 \;.$$

El *discriminante* de $F = \{a, b, c\}$ es

$$\mathsf{disc}(F) \;=\; b^2 \;-\; 4\,ac \;.$$

En general, vamos a considerar formas cuadráticas binarias con coeficientes enteros, $a, b, c \in \mathbb{Z}$. Entonces, $\mathsf{disc}(\{a, b, c\})$ es un entero y congruente con 0 o 1 módulo 4.

Observación 2.2. Dado $d \in \mathbb{Z}$ congruente con 0 módulo 4, la forma $\{1, 0, -d/4\}$ tiene coeficientes enteros y discriminante d; si d es congruente con 1 módulo 4, la forma $\{1, 1, -(d-1)/4\}$ tiene coeficientes enteros y discriminante d. En ambos casos, el coeficiente a es positivo.

El producto de formas lineales da lugar a formas cuadráticas:

$$(k\,x + l\,y)\,(m\,x + n\,y) \;=\; km\,x \;+\; (kn + lm)\,xy \;+\; ln\,y \tag{20}$$

es una forma cuadrática. Una forma cuadrática que es producto de formas lineales, como en (20) debería considerarse como un caso degenerado. En estos casos, el discriminante es un cuadrado:

$$(kn + lm)^2 \;-\; 4\,(km)\,(ln) \;=\; (kn - lm)^2 \;.$$

Teorema 2.3. *Una forma cuadrática binaria es un producto de dos formas lineales, si y sólo si su discriminante es un cuadrado perfecto.*

Demostración. Sea $F = \{a, b, c\}$. Si $\mathsf{disc}(F) = h^2$, entonces

$$4a\,F \;=\; (2a\,x + b\,y)^2 \;-\; (b^2 - 4ac)\,y^2 \;=\; (2a\,x + (b+h)\,y)\,(2a\,x + (b-h)\,y) \;.$$

Sobre un cuerpo, esto da una factorización de F como producto de factores lineales, si $a \neq 0$; si $a = 0$, $F = (b\,x + c\,y)\,y$, que es producto de factores lineales. Sobre un anillo, específicamente, sobre $\mathbb{Z}$, necesitamos algún resultado del estilo del Lema de Gauss para poder pasar de una factorización en $\mathbb{Q}$ a una factorización en $\mathbb{Z}$. □

Lema 2.4. *Si $F = \{a, b, c\}$ es una forma cuadrática binaria con coeficientes enteros y existe una factorización*

$$F \;=\; (\kappa\,x + \lambda\,y)\,(\rho\,x + \sigma\,y) \;,$$

con $\kappa, \lambda, \rho, \sigma \in \mathbb{Q}$, entonces existe una factorización

$$F \;=\; (k\,x + l\,y)\,(r\,x + s\,y) \;,$$

con $k, l, r, s \in \mathbb{Z}$.

Demostración. Si F se factoriza en $\mathbb{Q}$, entonces existe algún entero $m > 0$ tal que

$$m\,F \;=\; (k\,x + l\,y)\,(r\,x + s\,y) \;.$$

Dividiendo por el máximo común divisor entre m, k y l, podemos suponer que m, k y l son coprimos. Análogamente, dividiendo por el máximo común divisor entre m, r y s, podemos suponer que m, r y s son coprimos. La relación con los coeficientes a, b y c de F es:

$$ma \;=\; kr \qquad , \qquad mb \;=\; ks + lr \qquad \text{y} \qquad mc \;=\; ls \;,$$

con $a, b, c \in \mathbb{Z}$. De esto se deduce que m debe ser $m = 1$. □

Observación 2.5. Un argumento análogo funciona sobre cualquier dominio de factorización única.

Nomenclatura. De ahora en adelante, d denotará un entero no cuadrado y congruente con 0 o con 1 módulo 4.

Definición 2.6. Dado $n \in \mathbb{Z}$, decimos que una forma cuadrática binaria $F = \{a, b, c\}$ con coeficientes enteros *representa* n, si existen x e y enteros tales que

$$F(x, y) \;=\; n \;. \tag{21}$$

2.2 Clases de formas

Si nos interesa estudiar las distintas maneras de representar un entero por una forma cuadrática, dos representaciones que se relacionan por un cambio de variables no deberían considerarse como diferentes.

Definición 2.7. El grupo $\mathsf{GL}_2(\mathbb{Z})$ actúa en el conjunto de formas cuadráticas binarias (con coeficientes enteros) vía composición:

$$\left(\{a,b,c\} \cdot \begin{bmatrix} k & l \\ r & s \end{bmatrix} \right)(x,y) \;=\; a\,(k\,x+l\,y)^2 + b\,(k\,x+l\,y)\,(r\,x+s\,y) + c\,(r\,x+s\,y)^2 \;. \quad (22)$$

Observación 2.8. Si $\gamma = \left[\begin{smallmatrix} k & l \\ r & s \end{smallmatrix}\right] \in \mathsf{GL}_2(\mathbb{Z})$ y si $\{a_1,b_1,c_1\} = \{a,b,c\}\cdot\gamma$ es la forma (22), entonces

$$\begin{aligned} a_1 \;&=\; a\,k^2 \,+\, b\,kr \,+\, c\,r^2 \;=\; F(k,r)\;, \\ b_1 \;&=\; 2a\,kl \,+\, b\,(ks+lr) \,+\, 2c\,rs \quad \text{y} \\ c_1 \;&=\; a\,l^2 \,+\, b\,ls \,+\, c\,s^2 \;=\; F(l,s)\;. \end{aligned} \quad (23)$$

En cuanto a los discriminantes, si $d = \mathsf{disc}(\{a,b,c\})$ y $d_1 = \mathsf{disc}(\{a_1,b_1,c_1\})$, entonces

$$\mathsf{det}(\gamma)^2\, d \;=\; d_1\;.$$

En particular, como en este caso el único cuadrado en $\mathbb{Z}^\times = \{\pm 1\}$ es 1, $d_1 = d$.

Definición 2.9. Dos formas $F = \{a,b,c\}$ y $F_1 = \{a_1,b_1,c_1\}$ son *equivalentes*, si existe $\gamma \in \mathsf{GL}_2(\mathbb{Z})$ tal que $F_1 = F\cdot\gamma$. Si $\mathsf{det}(\gamma) > 0$, entonces F y F_1 son *estrictamente equivalentes*.

Observación 2.10. Como se mostró en la Observación 2.8, el discriminante de una forma cuadrática binaria es un invariante de la clase de equivalencia de la forma; en particular es un invariante de la clase de equivalencia estricta. En general, este invariante estará definido salvo cuadrados. El conjunto de enteros representados por una forma también es un invariante de la clase: dos formas equivalentes representan los mismos enteros; de nuevo, éste también es un invariante de la clase de equivalencia estricta.

Como mencionamos en la Observación 2.10, el conjunto de enteros representados por una forma depende únicamente de su clase de equivalencia. De esta manera, podemos dividir las formas cuadráticas –o, mejor dicho, sus clases– en familias.

Teorema 2.11. *Sea $F = \{a,b,c\}$ es una forma cuadrática binaria de discriminante $d = \mathsf{disc}(F)$. Si $d > 0$, entonces F representa tanto números positivos como negativos; si $d < 0$ y $a > 0$, entonces F representa únicamente números no negativos, representa a 0 y la única solución a $F(x,y) = 0$ es la trivial, $(x,y) = (0,0)$; si $d < 0$ pero $a < 0$, entonces F representa únicamente números no positivos, representa a 0 y la única solución a $F(x,y) = 0$ es la trivial.*

Definición 2.12. Una forma cuadrática binaria $F = \{a,b,c\}$ se dice *indefinida*, si $d > 0$, *definida positiva*, si $d < 0$ y $a > 0$ y *definida negativa*, si $d < 0$ y $a < 0$.

Observación 2.13. Las formas definidas positivas y las formas definidas negativas están en biyección por $\{a, b, c\} \mapsto \{-a, -b. - c\}$. Esta correspondencia respeta la acción de $\mathsf{GL}_2(\mathbb{Z})$ (y de $\mathsf{SL}_2(\mathbb{Z})$) y, por lo tanto, las clases de equivalencia (estricta). Será suficiente considerar formas definidas positivas, en el caso $d < 0$.

Nomenclatura. De ahora en más, nos concentraremos en equivalencia estricta y diremos, simplemente, que dos formas estrictamente equivalentes son "equivalentes". Por "clase de equivalencia" nos referiremos a las clases de equivalencia estricta. De ser necesario, nos referiremos a la equivalencia con respecto a la acción de todo el grupo $\mathsf{GL}_2(\mathbb{Z})$, o bien de esta manera, o bien por "equivalencia en sentido laxo" (o algún apelativo apropriado).

Lema 2.14. *Cada clase de equivalencia contiene, al menos, un representante* $\{a, b, c\}$ *que verifica* $|b| \leq |a| \leq |c|$.

Demostración. Dada $F_0 = \{a_0, b_0, c_0\}$, sea $a \in \mathbb{Z}$ un entero que cumple:

- $a \neq 0$ es representado por (la clase de) F_0 y
- $|a|$ es mínimo entre los enteros representados.

Por minimialidad, si $F_0(k, l) = a$, entonces $(k : l) = 1$; si no,

$$\left|F_0\Big(\frac{k}{(k:l)}, \frac{l}{(k:l)}\Big)\right| = \left|\frac{a}{(k:l)^2}\right| < |a| \ .$$

Completamos el par (k, l) a una matriz $\gamma = \left[\begin{smallmatrix} k & l \\ r & s \end{smallmatrix}\right] \in \mathsf{SL}_2(\mathbb{Z})$ $F' = F_0 \cdot \gamma$ es de la forma $\{a, b', c'\}$. Aplicando $\left[\begin{smallmatrix} 1 & h \\ 1 \end{smallmatrix}\right]$ a F', se obtiene la forma (estrictamente) equivalente $F(x, y) = F'(x + h, y)$. Pero $F = \{a, b, c\}$, donde a no cambia, pero $b = 2ah + b'$. Eligiendo h convenientemente, $|b| \leq |a|$. Finalmente, si $c \neq 0$, entonces debe cumplirse $|a| \leq |c|$, por minimalidad de a. □

Teorema 2.15. *El número de clases de formas cuadráticas binarias con coeficientes enteros de discriminante dado, d, es finito.*

Demostración. Sea $\{a, b, c\}$ una forma de discriminante $d = b^2 - 4ac$ que verifica $|b| \leq |a| \leq |c|$. Si $d > 0$, $|ac| \geq |b|^2 = d + 4ac > 4ac$. En particular, $ac < 0$ y $4|a|^2 \leq 4|ac| = -4ac = d - b^2 \leq d$. El coeficiente a sólo puede ser uno de una cantidad finita, la condición $|b| \leq |a|$ implica lo mismo acerca de b y c queda determinado por a, b y d (fijo). Si $d < 0$, asumimos que la forma es definida positiva y, por lo tanto, $a > 0$ y $c > 0$. Así, $4a^2 \leq 4ac = b^2 - d \leq |d| + a^2$. De nuevo, el coeficiente a puede ser sólo uno de una cantidad finita, la condición $|b| \leq a$ implica lo mismo de b y c queda determinado por a, b y d. □

Observación 2.16. En el caso $d > 0$, la cota para a es $|a| \leq \sqrt{d}/2$; en el caso $d < 0$ $(a > 0)$, la cota es $a \leq \sqrt{|d|/3}$.

Observación 2.17. Teniendo en cuenta que el grupo $\mathsf{SL}_2(\mathbb{Z})$ está generado por las matrices

$$S = \begin{bmatrix} & 1 \\ -1 & \end{bmatrix} \quad \text{y} \quad T = \begin{bmatrix} 1 & 1 \\ & 1 \end{bmatrix} ,$$

y que $\mathsf{GL}_2(\mathbb{Z}) = \left\langle \mathsf{SL}_2(\mathbb{Z}), C = \left[\begin{smallmatrix} 1 & \\ & -1 \end{smallmatrix}\right] \right\rangle$, veamos qué efecto tiene cada una de estas transformaciones en una forma. Si $F = \{a, b, c\}$,

$$F \cdot S = \{c, -b, a\} \quad , \quad F \cdot T = \{a, 2a + b, a + b + c\} \quad \text{y} \quad F \cdot C = \{a, -b, c\} \ .$$

Notamos que $-I_2 = \left[\begin{smallmatrix} -1 & \\ & -1 \end{smallmatrix}\right]$ actúa trivialmente.

2.3 Formas definidas

Corolario 2.18. *Cada clase de equivalencia de formas definidas positivas contiene, al menos, un representante que cumple*

$$-a < b \leq a < c \qquad \textit{o bien} \qquad 0 \leq b \leq a = c \ .$$

Demostración. Dados a, b y c,

$$\{a, -a, c\} \cdot T = \{a, a, c\} \quad \text{y} \quad \{a, b, \epsilon\, a\} \cdot S = \{\epsilon\, a, -b, a\} \quad (\ \epsilon = \pm 1\ ).$$

Si $\{a_0, b_0, c_0\}$ es definida positiva, entonces $a_0 > 0$ y $c_0 > 0$. Supongamos que $|b_0| \leq a_0 \leq c_0$. Si $a_0 = c_0$, obtenemos una forma con $a = a_0 = c = c_0$ y $b = |b_0| \geq 0$, aplicando S de ser necesario; si $b_0 = -a_0$, obtenemos una forma con $a = b = a_0$ y $c = c_0$, aplicando T. La nueva forma cumple con alguna de las dos condiciones. □

Teorema 2.19. *Si $d < 0$, el número de clases de equivalencia de formas definidas positivas de discriminante d es igual a la cantidad de ternas $a, b, c \in \mathbb{Z}$ tales que $b^2 - 4ac = d$ y que cumplen alguna de las condiciones del Corolario 2.18.*

Demostración. El resultado se reduce a la afirmación de que cada clase de equivalencia de formas definidas positivas de discriminante d está representada por exactamente una forma que cumple algunas de las condiciones. Sean $\{a, b, c\}$ y $\{a_1, b_1, c_1\}$ dos formas de discriminante d, definidas positivas y que cumplen, cada una, alguna de las dos condiciones del Corolario 2.18. Si son formas equivalentes, existe γ de determinante $\det(\gamma) = 1$ tal que

$$\{a_1, b_1, c_1\} = \{a, b, c\} \cdot \gamma \ .$$

Supongamos, sin pérdida de generalidad, que $a \geq a_1$ y que

$$\{a_1, b_1, c_1\} = \{a, b, c\} \cdot \begin{bmatrix} k & l \\ r & s \end{bmatrix} \ .$$

De las fórmulas (23), como $a \leq c$ y $|b| \leq a$,

$$a_1 \geq a\, k^2 - a\, |kr| + a\, r^2 \geq a\, |kr| \ .$$

La última desigualdad es consecuencia de $p^2 + q^2 \geq 2\,|pq|$ para todo par p, q. En consecuencia, $|kr| \leq 1$. Para cualquiera de los tres casos $|kr| \in \{-1, 0, 1\}$, se deduce que $k^2 - |kr| + r^2 = 1$ y que $a \geq a_1 \geq a$, o sea $a = a_1$.

Si $c = a$ y $c_1 = a_1$, entonces $c = c_1$ y, por $d = b^2 - 4ac = b_1^2 - 4a_1c_1$, $b_1 = \pm b$. Pero, por otro lado, $b \geq 0$ y $b_1 \geq 0$. Entonces, $b = b_1$, también.

Si $c > a$ o $c_1 > a_1$, podemos suponer que se cumple $c > a$. Si

$$\{a_1, b_1, c_1\} \,=\, \{a, b, c\} \cdot \begin{bmatrix} k & l \\ r & s \end{bmatrix} \ ,$$

no necesariamente la misma matriz, entonces $k^2 - |kr| + r^2 = 1$, como antes. Si fuese $r \neq 0$, entonces $c\,r^2 > a\,r^2$ y

$$a \,=\, a_1 \,=\, ak^2 \,+\, b\,kr \,+ c\,r^2 \,>\, a\,(k^2 - |kr| + r^2) \,=\, a \ ,$$

lo que es absurdo. Así, $r = 0$. Pero $ks - rl = 1$ implica $ks = 1$ y, por lo tanto, de la fórmula para b_1,

$$b_1 \,=\, 2a\,kl \,+\, b\,(ks + lr) \,+ 2c\,rs \,\equiv\, b\,(\mathsf{mod}\,2a) \ .$$

Pero $-a = -a_1 < b, b_1 \leq a = a_1$ implica $b = b_1$. De la positividad de c y de c_1, vale $c = c_1$. □

2.4 El estabilizador de una forma

Volvemos al caso de formas de discriminante arbitrario, formas definidas o indefinidas.

Definición 2.20. El *estabilizador* o *grupo de isotropía* de una forma F es el subgrupo

$$\mathsf{Stab}(F)^+ \,=\, \Big\{\gamma \in \mathsf{SL}_2(\mathbb{Z}) \,:\, F \cdot \gamma = F\Big\}$$

de $\mathsf{SL}_2(\mathbb{Z})$.

Más en general, podríamos definir

$$\mathsf{Stab}(F) \,=\, \Big\{\gamma \in \mathsf{GL}_2(\mathbb{Z}) \,:\, F \cdot \gamma = F\Big\} \ .$$

Observación 2.21. Si F y F_1 son formas equivalentes, entonces los grupos $\mathsf{Stab}(F)^+$ y $\mathsf{Stab}(F_1)^+$ son conjugados. Precisamente, si $\gamma \in \mathsf{SL}_2(\mathbb{Z})$, entonces

$$\mathsf{Stab}(F \cdot \gamma)^+ \,=\, \gamma^{-1}\,\mathsf{Stab}(F)^+\,\gamma \ .$$

Lo mismo vale para $\mathsf{Stab}(F)$ en lugar de $\mathsf{Stab}(F)^+$ y, también, si permitimos $\gamma \in \mathsf{GL}_2(\mathbb{Z})$.

Pregunta. ¿Si $\mathsf{disc}(F) = \mathsf{disc}(G)$, son conjugados –o bien isomorfos– sus estabilizadores?

Teorema 2.22. *Dada una forma cuadrática $F = \{a, b, c\}$, el subgrupo $\mathsf{Stab}(F)^+$ contiene todas las matrices de la forma*

$$\begin{bmatrix} \frac{u-bv}{2} & -cv \\ av & \frac{u+bv}{2} \end{bmatrix} , \tag{24}$$

donde el par u, v saisface

$$u^2 - d\,v^2 = 4 . \tag{25}$$

Si $(a : b : c) = 1$, entonces estas son todas las matrices que dejan fija F.

Demostración. Se puede corroborar que las matrices de la forma (24) preservan F, a partir de las fórmulas para los coeficientes (23) (alcanza con mirar a_1 y b_1). Finalmente, si $\left[\begin{smallmatrix} k & l \\ r & s \end{smallmatrix}\right] \in \mathsf{Stab}(F)^+$, entonces

$$\begin{aligned} a &= a\,k^2 + b\,kr + c\,r^2 \quad \text{y} \\ b &= 2a\,kl + b\,(ks + lr) + 2c\,rs = 2a\,kl + b\,(1 + 2lr) + 2c\,rs . \end{aligned}$$

De estas dos ecuaciones,

$$\begin{aligned} 0 &= a\,kl + b\,lr + c\,rs , \\ l\,a &= l\,a - k\,0 = c\,r\,(lr - ks) = -c\,r \quad \text{y} \\ s\,a &= s\,a - r\,0 = a\,k\,(ks - lr) + b\,r\,(ks - lr) = a\,k + b\,r \end{aligned}$$

O sea, $a\,l = -c\,r$ y $a\,(s - k) = b\,r$. En particular, $a \mid c\,r$ y $a \mid b\,r$.

Ahora asumimos $(a : b : c) = 1$. De lo anterior, $a \mid r$. Si $r = a\,v$, entonces $l = -c\,v$ y $s - k = b\,v$. De esto y de $ks - lr = 1$, se deduce que $(k + s)^2 = d\,v^2 + 4$. Elegimos, entonces, $u = k + s$. □

Observación 2.23. Las matrices de la forma (24) conforman un grupo; son un subgrupo de $\mathsf{SL}_2(\mathbb{Z})$ y, por lo tanto, de $\mathsf{Stab}(F)^+$: si, para $(u, v) \in \mathbb{Z}^2$ que verifica (25), definimos

$$M(u, v) = \begin{bmatrix} \frac{u-bv}{2} & -cv \\ av & \frac{u+bv}{2} \end{bmatrix} ,$$

entonces

$$M(u_1, v_1)\,M(u_2, v_2) = M(u_3, v_3) ,$$

donde $(u_3, v_3) \in \mathbb{Z}^2$ está definido por[16]

$$u_3 = \frac{u_1u_2 + d\,v_1v_2}{2} \qquad \text{y} \qquad v_3 = \frac{u_1v_2 + v_1u_2}{2} .$$

La aplicación M es inyectiva y permite trasladar la estuctura de grupo del lado de las matrices a los pares $(u, v) \in \mathbb{Z}^2$ que cumplen $u^2 - d\,v^2 = 4$. Por otro lado, si

[16] Estas definiciones son análogas a las de la Observación 1.41; la demostación de que u_3 y v_3 son enteros es análoga a la realizada en la Observación 1.39.

$q^2 = d = b^2 - 4ac$, las soluciones a la ecuación (25) forman un grupo, identificando (u, v) con $\sigma(u, v) = \frac{u+q\,v}{2}$.[17] La aplicación

$$\sigma(u,v) \;=\; \frac{u+q\,v}{2} \;\mapsto\; M(u,v) \;=\; \begin{bmatrix} \frac{u-bv}{2} & -cv \\ av & \frac{u+bv}{2} \end{bmatrix} \tag{26}$$

es un morfismo de grupos entre este grupo y el grupo $\mathsf{Stab}(F)^+$. En particular, si $(a : b : c) = 1$, entonces es un isomorfismo. Se puede verificar formalmente que,

$$\begin{array}{ccccc} [\sigma(u_1,v_1),\sigma(u_2,v_2)] & \longleftarrow & [(u_1,v_1),(u_2,v_2)] & \longmapsto & [M(u_1,v_1),M(u_2,v_2)] \\ \big\downarrow & & & & \big\downarrow \\ \sigma(u_1,v_1)\,\sigma(u_1,v_2) & \xmapsto{\sigma^{-1}} & (u_3,v_3) & \xmapsto{M^{-1}} & M(u_1,v_1)\,M(u_2,v_2) \end{array}$$

conmuta, donde $u_3 = \frac{u_1u_2+d\,v_1v_2}{2}$ y $v_3 = \frac{u_1v_2+v_1u_2}{2}$. Además, se verifica que

$$\begin{aligned} \mathsf{det}(M(u,v)) \;&=\; \mathsf{Nm}(\sigma(u,v))\;, \\ \mathsf{tr}(M(u,v)) \;&=\; \mathsf{Tr}(\sigma(u,v)) \quad \text{y} \\ \mathsf{adj}(M(u,v)) \;&=\; \overline{\sigma(u,v)} \end{aligned}$$

Sea d un discriminante no cuadrado y sea

$$\mathcal{S} \;=\; \Big\{(u,v) \in \mathbb{Z}^2 \;:\; u^2 - d\,v^2 = 4\Big\}$$

el conjunto de soluciones enteras a la ecuación (24). Sea $q^2 = d$ una raíz y sea $G = \sigma(\mathcal{S}) \subset \mathbb{Q}(q)^\times$; si $d > 0$, elegimos $q = \sqrt{d} > 0$ y $\epsilon = \frac{u_0+q\,v_0}{2}$ correspondiente a la solución (u, v) con $u > 0$ y $v > 0$ lo más chico posible, la "solución fundamental".

d	$\mathcal{S}$	G	w
> 0		$\{\pm\epsilon^n \;:\; n \in \mathbb{Z}\}$	
-3	$\{\pm(-1,1), \pm(1,1), \pm(2,0)\}$	$\{\pm\omega, \pm\bar{\omega}, \pm 1\}$	6
-4	$\{\pm(0,1), \pm(2,0)\}$	$\{\pm i, \pm 1\}$	4
< -4	$\{\pm(2,0)\}$	$\{\pm 1\}$	2

Tabla 4: Conjunto de soluciones a la ecuación (24) y el grupo correspondiente en $\mathbb{Q}(\sqrt{d})^\times$, ordenados por discriminante.

Fijada la correspondencia $\sigma : \mathcal{S} \to G$, por cada forma $\{a, b, c\}$ de discriminante $d = b^2 - 4ac$, hay un morfismo inyectivo

$$M \circ \sigma^{-1} \;:\; G \to \mathsf{SL}_2(\mathbb{Z})\;.$$

Dos formas equivalentes dan lugar a embeddings conjugados.[18]

[17] Fijada q, hay dos isomorfismos: $\sigma(u,v) = u + q\,v$ y $\sigma'(u,v) = u - q\,v = \overline{\sigma(u,v)}$, dado por elegir la otra raíz de $q^2 = d$.

[18] Si, en lugar de σ tomamos $\bar{\sigma} = \bar{\cdot} \circ \sigma$, entonces la relación es: $M \circ (\bar{\sigma})^{-1} = \mathsf{adj} \circ M \circ \sigma^{-1}$. Conjugar, es decir, aplicar $\bar{\cdot}$ no es holomorfa, pero conjugar por la matriz $\left[\begin{smallmatrix} -1 & \\ & 1 \end{smallmatrix}\right]$, sí, aunque ésta está en $\mathsf{GL}_2(\mathbb{Z})$.

Ejemplo 2.24. Para cada discriminante d, podemos considerar la forma *principal*. Si $d \equiv 0 \,(\mathsf{mod}\, 4)$, la forma principal es $\{1, 0, -d/4\}$ y, si $d = 4m$, el embedding es

$$\begin{bmatrix} \frac{u}{2} & m\,v \\ v & \frac{u}{2} \end{bmatrix} \; ;$$

si $d \equiv 1 \,(\mathsf{mod}\, 4)$, la forma principal es $\{1, 1, (1-d)/4\}$ y, si $d = 1 + 4m$, el embedding es

$$\begin{bmatrix} \frac{u-v}{2} & m\,v \\ v & \frac{u+v}{2} \end{bmatrix} \; .$$

Ver cómo quedan con $d = -4$ y $d = -3$.

Pregunta. ¿Si dos embeddings son conjugados, corresponden a formas equivalentes?

2.5 Formas primitivas

Definición 2.25. Una forma $F = \{a, b, c\}$ se dice *primitiva*, si $(a : b : c) = 1$. En otro caso, se dice que es *imprimitiva*.

Observación 2.26. La propiedad de una forma de ser primitiva es, en realidad, una propiedad de la clase. La relación

$$\{a, b, c\} \cdot \begin{bmatrix} k & l \\ r & s \end{bmatrix} \; = \; \{a_1, b_1, c_1\}$$

junto con las fórmulas (23) implica que $(a_1 : b_1 : c_1)$ sea un múltiplo de $(a : b : c)$. Invirtiendo la relación, $(a : b : c)$ es un múltiplo de $(a_1 : b_1 : c_1)$, con lo cual, son asociados. En particular,

$$(a : b : c) \; = \; (a_1 : b_1 : c_1) \; .$$

En general, el ideal generado por el máximo común divisor también es un invariante de la clase.

Observación 2.27. Si $F = \{a, b, c\}$ con $d = \mathsf{disc}(F)$ y $g \mid (a : b : c)$, entonces $g^2 \mid d$ y la forma $\left\{ \frac{a}{g}, \frac{b}{g}, \frac{c}{g} \right\}$ es una forma con coeficientes enteros de discriminante d/g^2; además, si $g > 0$ y $a > 0$, entonces $\frac{a}{g} > 0$. En particular, si $g = (a : b : c)$, entonces la nueva forma es primitiva. Recíprocamente, si $F' = \{a', b', c'\}$ es una forma de discriminante d' y $g \in \mathbb{Z}$, entonces $\{g\,a', g\,b', g\,c'\}$ es una forma con coeficientes enteros, de discriminante $g^2\,d'$; además, si $g > 0$ y $a' > 0$, entonces $g\,a' > 0$. En definitiva,

$$\mathsf{Clases}(d) \; = \; \bigsqcup_{\substack{g>0 \\ g^2 \mid d}} \mathsf{Clases}_g(d) \; = \; \bigsqcup_{\substack{g>0 \\ g^2 \mid d}} \mathsf{Clases}_1\left(\tfrac{d}{g^2}\right) \; .$$

Teorema 2.28. *El número de clases de formas de discriminante d, primitivas o imprimitivas, es igual a*

$$\#\mathsf{Clases}(d) \;=\; \sum_{\substack{g>0\\ g^2|d}} \#\mathsf{Primitivas}\left(\tfrac{d}{g^2}\right) \;.$$

Observación 2.29. Por la Observación 2.2, sabemos que, para todo entero $d \equiv 0, 1 \,(\mathsf{mod}\, 4)$, existe una forma de discriminante d. Más aun, si $d < 0$, existe una forma con coeficiente $a > 0$, es decir definida positiva. Los mismos ejemplos mencionados allí muestran que, para cada d existe una forma *primitiva* de discriminante d (definida positiva, si $d < 0$).

Definición 2.30. Un *discriminante fundamental* es un entero d que cumple

- $d \equiv 1 \,(\mathsf{mod}\, 4)$ y es libre de cuadrados, o bien
- $d = 4m$, donde $m \equiv 2$ o $3 \,(\mathsf{mod}\, 4)$ y es libre de cuadrados.

Teorema 2.31. *Un entero $d \equiv 0, 1 \,(\mathsf{mod}\, 4)$ es un discriminante fundamental, si y sólo si toda forma de discriminante d es primitiva.*

Demostración. Sea $\{a, b, c\}$ una forma de discriminante d. Si $g \mid (a : b : c)$, entonces $g^2 \mid d$. Supongamos que $g > 1$. Si $d \equiv 1 \,(\mathsf{mod}\, 4)$, como no es libre de cuadrados, no es fundamental; si $d \equiv 0 \,(\mathsf{mod}\, 4)$ con $d = 4m$ y m libre de cuadrados, como $g^2 \mid d$, vale $g = 2$ y $4m = b^2 - 4ac = 4\,(b'^2 - 4a'c')$, con lo que $m \equiv 0, 1 \,(\mathsf{mod}\, 4)$ y d no es fundamental.

Supongamos, ahora, que $d = 4m$ no es fundamental. Entonces,

- si m no es libre de cuadrados y $f > 1$ es tal que $f^2 \mid m$, la forma $\left\{1, 0, -\frac{m}{f^2}\right\}$ tiene discriminante $4\frac{m}{f^2}$ y la forma $\left\{f, 0, -\frac{m}{f}\right\}$ no es primitiva y tiene discriminante d;
- si $m \equiv 0 \,(\mathsf{mod}\, 4)$, la forma $\left\{1, 0, -\frac{m}{4}\right\}$ tiene discriminante m y la forma $\left\{2, 0, -\frac{m}{2}\right\}$ no es primitiva y tiene discriminante d;
- si $m \equiv 1 \,(\mathsf{mod}\, 4)$, la forma $\left\{1, 1, \frac{1-m}{4}\right\}$ tiene discriminante m y la forma $\left\{2, 2, \frac{1-m}{2}\right\}$ no es primitiva y tiene discriminante d.

Supongamos que $d \equiv 1 \,(\mathsf{mod}\, 4)$ no es fundamental. Entonces, no es libre de cuadrados y existe $g > 1$ tal que $g^2 \mid d$. Si $d = g^2 d'$, como d es impar, $d \equiv d' \,(\mathsf{mod}\, 4)$. La forma $\left\{1, 1, \frac{1-d'}{4}\right\}$ tiene discriminante d' (y, además, es primitiva). La forma $\left\{g, g, g\,\frac{1-d'}{4}\right\}$ no es primitiva y tiene discriminante d. □

3 Contando representaciones

Usaremos la siguiente nomenclatura para referirnos a distintos conjuntos de representaciones, así como a sus respectivos cardinales, tratando de que resulten descriptivos:

- $\mathsf{Representaciones}(n, F)$: el conjunto de todas las representaciones de un entero n por una forma F,
- $\mathsf{Representaciones}_t(n, F)$: el subconjunto de aquellas representaciones $F(x, y) = n$ con $(x : y) = t$,
- $\mathsf{Propias}(n, F) = \mathsf{Representaciones}_1(n, F)$: el subconjunto de representaciones *propias*,
- $\mathsf{Primarias}(n, F)$: el subconjunto de representaciones *primarias*,
- $\mathsf{Primarias}_t(n, F)$: el subconjunto de representaciones primarias $F(x, y) = n$ con $(x : y) = t$.

3.1 Representaciones propias

Definición 3.1. Una representación $F(x, y) = n$ de un entero n por una forma cuadrática se dice *propia*, si $(x : y) = 1$. En otro caso, se dice que es *impropia*.

Observación 3.2. Fijado n, los conjuntos $\mathsf{Representaciones}_t(n, F)$ (y, por lo tanto, $\mathsf{Representaciones}(n, F)$ y $\mathsf{Propias}(n, F)$) dependen únicamente de la clase de la forma F. Es decir, si F y F_1 son equivalentes, entonces

$$\mathsf{Representaciones}_t(n, F_1) \;=\; \mathsf{Representaciones}_t(n, F) \;.$$

Podemos hablar, entonces, de las representaciones por la clase de una forma, o por un representante de la misma.

Observación 3.3. Si $(x, y) \in \mathsf{Representaciones}(n, F)$ es una representación y $t \mid (x : y)$, entonces la representación $F(x, y) = n$ proviene de una representación $F(x', y') = \frac{n}{t^2}$. Entonces,

$$\mathsf{Representaciones}(n, F) \;=\; \bigsqcup_{\substack{t>0 \\ t^2|n}} \mathsf{Representaciones}_t(n, F) \;=\; \bigsqcup_{\substack{t>0 \\ t^2|n}} \mathsf{Representaciones}_1\big(\tfrac{n}{t^2}, F\big) \;.$$

Observación 3.4. El grupo modular actúa en $\mathbb{Z}^2$ por la operación usual de matrices. Si $\gamma = \left[\begin{smallmatrix} k & l \\ r & s \end{smallmatrix}\right] \in \mathsf{SL}_2(\mathbb{Z})$ y $(x, y) \in \mathbb{Z}^2$, entonces

$$(k\,x + l\,y : r\,x + s\,y) \;=\; (x : y) \;\;.$$

Como ya vimos, este grupo también actúa en el conjunto de formas cuadráticas vía composición. Fijada una forma F, si $\gamma \in \mathsf{SL}_2(\mathbb{Z})$ es tal que $F \cdot \gamma = F$, entonces

$$F(k\,x + l\,y, r\,x + s\,y) \;=\; F\big(\gamma \cdot (x, y)\big) \;=\; \big(F \cdot \gamma\big)(x, y) \;=\; F(x, y) \;.$$

En consecuencia, dada una representación $F(x, y) = n$, obtenemos otras representaciones actuando por aquellas matrices que dejan fija a la forma F. El subgrupo

$$\mathsf{Stab}(F)^+ \;=\; \Big\{\gamma \in \mathsf{SL}_2(\mathbb{Z}) \;:\; F \cdot \gamma = F\Big\} \;\subset\; \mathsf{SL}_2(\mathbb{Z})$$

del grupo modular actúa en cada uno de los conjuntos $\mathsf{Representaciones}_t(n, F)$, de manera que podemos subdividir cada uno de ellos en órbitas por esta acción.

Pregunta. ¿La cantidad de óribtas en $\mathsf{Representaciones}_t(n, F)$ es finita?

Lema 3.5. *Sea $n > 0$ y sea $F(x, y) = n$ una representación* propia *de n. Existen únicos $l, s, r \in \mathbb{Z}$ tales que*

$$\begin{vmatrix} x & l \\ y & s \end{vmatrix} = 1 \qquad , \qquad r^2 \equiv d \,(\mathsf{mod}\, 4n) \qquad y \qquad 0 \leq r < 2n$$

de manera que $F \cdot \left[\begin{smallmatrix} x & l \\ y & s \end{smallmatrix}\right] = \{n, r, m\}$, donde $m \in \mathbb{Z}$ está determinado por $r^2 - 4nm = d$.

Demostración. Dada una representación propia $F(x, y) = n$ de un entero positivo $n > 0$, las matrices que transforman F en una forma del tipo $\{n, *, *\}$ son $\left[\begin{smallmatrix} x & l \\ y & s \end{smallmatrix}\right]$ con $xs - yl = 1$; alguna existe, porque $(x : y) = 1$. Si $xs_0 - yl_0 = 1$, todos las matrices que cumplen estas condiciones están parametrizadas por $l = l_0 + h\,x$ y $s = s_0 + h\,y$; el valor de l está determinado módulo x y el de s está determinado módulo y. Si $F = \{a, b, c\}$, $F \cdot \left[\begin{smallmatrix} x & l_0 \\ y & s_0 \end{smallmatrix}\right] = \{n, r_0, m_0\}$ y $F \cdot \left[\begin{smallmatrix} x & l \\ y & s \end{smallmatrix}\right] = \{n, r, m\}$, entonces $r = 2a\,xl + b\,(xs + yl) + 2c\,ys = r_0 + 2h\,n$. O sea que el coeficiente r está determinado módulo $2n$. □

O sea, hay una aplicación bien definida

$$\rho \,:\, \mathsf{Propias}(n, F) \,\to\, \left\{0 \leq r < 2n \,:\, r^2 \equiv d \,(\mathsf{mod}\, 4n)\right\} \,. \tag{27}$$

La cantidad de elementos en el conjunto de la derecha la calculamos en el Teorema 1.25 y en la Observación 1.26. Es igual a $\sum'_{f|n} (d/f)$, donde la suma se realiza sobre los divisores de n que son libres de cuadrados.

Observación 3.6. Fijado $n > 0$ y una forma $F = \{a, b, c\}$, las matrices $\gamma = \left[\begin{smallmatrix} x & l \\ y & s \end{smallmatrix}\right]$ tales que $F \cdot \gamma$ tiene primer coeficiente n están en correspondencia con el producto cartesiano de los conjuntos $\mathsf{Propias}(n, F)$ y $\{(l, s) \,:\, xs - yl = 1\}$. Dos matrices en este conjunto con $F \cdot \gamma = \{n, r, *\}$ y $0 \leq r < 2n$ están relacionadas por un elemento de $\mathsf{Stab}(F)^+$ y, en particular, las representaciones correspondientes a la primera columna de cada una de estas dos matrices están en la misma órbita.

Lema 3.7. *Si $F(x_1, y_1) = F(x_2, y_2) = n$ son dos representaciones propias de $n > 0$ tales que $\rho(x_1, y_1) = \rho(x_2, y_2)$, entonces existe $\gamma \in \mathsf{Stab}(F)^+$ tal que $\gamma\,(x_1, y_1) = (x_2, y_2)$.*

Demostración. Sea $r = \rho(x_1, y_1) = \rho(x_2, y_2)$ y sean $\gamma_1 = \left[\begin{smallmatrix} x_1 & * \\ y_1 & * \end{smallmatrix}\right]$ y $\gamma_2 = \left[\begin{smallmatrix} x_2 & * \\ y_2 & * \end{smallmatrix}\right]$ matrices de $\mathsf{SL}_2(\mathbb{Z})$ tales que

$$F \,\cdot\, \gamma_1 \,=\, F \,\cdot\, \gamma_2 \,=\, \{n, r, m\} \,.$$

Como n, r y el discrimante d coinciden, el valor de m está determinado y es el mismo para ambas transformaciones de F. El producto $\gamma_1\gamma_2^{-1}$ pertenece a $\mathsf{Stab}(F)^+$ y transforma la representación $F(x_2, y_2) = n$ en $F(x_1, y_1) = n$. □

Corolario 3.8. *El conjunto de órbitas de representaciones propias de un entero $n > 0$ por un forma F dada, $F(x, y) = n$, está en correspondencia con un subconjunto de $r \in \mathbb{Z}$ tales que $0 \leq r < 2n$ y $r^2 \equiv d \,(\mathsf{mod}\, 4n)$. En particular, son una cantidad finita.*

Observación 3.9. Si $d < 0$, a cada entero r proveniente de una representación propia $F(x, y) = n$ (de $n > 0$ por una forma primitiva de discriminante d) como en el Lema 3.5 le corresponden $w = w(d)$ representaciones propias (todas equivalentes, por el Corolario 3.8), donde $w \in \{2, 4, 6\}$ está definido en la Tabla 4.

Pregunta. ¿Induce (27) una biyección entre el conjunto de órbitas

$$\mathsf{Stab}(F)^+ \backslash \mathsf{Propias}(n, F)$$

y el conjunto de soluciones $\left\{0 \le r < 2n \,:\, r^2 \equiv d \,(\mathsf{mod}\, 4n)\right\}$?

3.2 Representaciones primarias

Si bien puede parecer más natural contar órbitas, es decir, clases de *representaciones*, para $d < 0$ ésa no es la manera clásica de dar respuesta a la pregunta anterior. Para $d > 0$ es casi inevitable contar órbitas en lugar de representaciones, porque las mismas son una cantidad infinita. Probablemente, esta aparente diferencia conceptual se deba a que la noción de *representación primaria* apareció antes que la noción de acción; a su vez, existiendo una cantidad finita de representaciones propias cuando $d < 0$, no debe haber resultado relevante elegir un representante de una manera *canónica*.

Sea $F = \{a, b, c\}$ una forma de discriminante $d > 0$ y sea $\sqrt{d} > 0$ la raíz positiva. La forma F se descompone (en $\mathbb{Q}(\sqrt{d})$) de la siguiente manera:

$$a\,x^2 \,+\, b\,xy \,+\, c\,y^2 \,=\, a\,\big(x - \theta\,y\big)\,\big(x - \bar{\theta}\,y\big)\ ,$$

donde

$$\theta \,=\, \frac{-b + \sqrt{d}}{2a} \qquad \text{y} \qquad \bar{\theta} \,=\, \frac{-b - \sqrt{d}}{2a}\ ;$$

es decir, el cambio de vaiables $(\xi, \upsilon) = (x - \theta\,y, x - \bar{\theta}\,y)$ descompone F. En términos de matrices,

$$\begin{bmatrix} 1 & 1 \\ -\theta & -\bar{\theta} \end{bmatrix} \begin{bmatrix} & a/2 \\ a/2 & \end{bmatrix} \begin{bmatrix} 1 & -\theta \\ 1 & -\bar{\theta} \end{bmatrix} \,=\, \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}$$

Si actuamos por una matriz de la forma (24), sabemos que

$$\begin{bmatrix} \frac{u - b\,v}{2} & a\,v \\ -c\,v & \frac{u + b\,v}{2} \end{bmatrix} \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix} \begin{bmatrix} \frac{u - b\,v}{2} & -c\,v \\ a\,v & \frac{u + b\,v}{2} \end{bmatrix} \,=\, \begin{bmatrix} a & b/2 \\ b/2 & c \end{bmatrix}\ .$$

Pero

$$\begin{bmatrix} 1 & -\theta \\ 1 & -\bar{\theta} \end{bmatrix} \begin{bmatrix} \frac{u - b\,v}{2} & -c\,v \\ a\,v & \frac{u + b\,v}{2} \end{bmatrix} \,=\, \begin{bmatrix} \frac{u - \sqrt{d}\,v}{2} & \\ & \frac{u + \sqrt{d}\,v}{2} \end{bmatrix} \begin{bmatrix} 1 & -\theta \\ 1 & -\bar{\theta} \end{bmatrix}\ .$$

O sea, si (x_1, y_1) y (x_2, y_2) están relacionadas por una matriz de la forma (24), es decir,

$$\begin{bmatrix} x_2 \\ y_2 \end{bmatrix} \,=\, \begin{bmatrix} \frac{u - b\,v}{2} & -c\,v \\ a\,v & \frac{u + b\,v}{2} \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix}\ ,$$

entonces

$$x_2 - \theta\, y_2 \;=\; \left(\tfrac{u-\sqrt{d}\,v}{2}\right)\left(x_1 - \theta\, y_1\right)\;,$$
$$x_2 - \bar{\theta}\, y_2 \;=\; \left(\tfrac{u+\sqrt{d}\,v}{2}\right)\left(x_1 - \bar{\theta}\, y_1\right)\;.$$

En particular, si $\frac{u+\sqrt{d}\,v}{2} = \pm\epsilon^m$, el cociente es igual a:

$$\frac{x_2 - \bar{\theta}\, y_2}{x_2 - \theta\, y_2} \;=\; \frac{\frac{1}{2}\left(u+\sqrt{d}\,v\right)}{\frac{1}{2}\left(u-\sqrt{d}\,v\right)}\,\frac{x_1 - \bar{\theta}\, y_1}{x_1 - \theta\, y_1} \;=\; \epsilon^{2m}\,\frac{x_1 - \bar{\theta}\, y_1}{x_1 - \theta\, y_1}\;.$$

Definición 3.10. Si $d > 0$ llamaremos *representación primaria* de $n > 0$ por una forma $F = \{a, b, c\}$ de discriminante d a una representación *propia* $F(x, y) = n$ que verifica

$$1 \;\le\; \frac{x - \bar{\theta}\, y}{x - \theta\, y} \;<\; \epsilon^2 \qquad \text{y} \qquad 0 \;<\; x - \theta\, y\;. \tag{28}$$

Observación 3.11. Si $F = \{a, b, c\}$ es una forma de discriminante $d > 0$ y $n > 0$, entonces cada representación de n por F es equivalente, por matrices de la forma (24), a exactamente una representación primaria. Es decir, si $\mathsf{Stab}(F)_0^+$ el subgrupo de $\mathsf{Stab}(F)^+$ conformado por las matrices de la forma (24), *para* $d > 0$, existe una correspondencia

$$\mathsf{Stab}(F)_0^+ \backslash \mathsf{Representaciones}(n, F) \;\simeq\; \mathsf{Primarias}(n, F)\;;$$

cada órbita contiene exactamente una representante primaria. La cantidad de representaciones primarias es finita: si $F(x, y) = n$ es una representación primaria y si $(\xi, \upsilon) = (x - \theta\, y, x - \bar{\theta}\, y)$, entonces

$$\xi\,\upsilon \;=\; n/a \quad , \quad 1 \;\le\; \upsilon/\xi \;<\; \epsilon^2 \quad (\text{ y } \quad 0 \;<\; \xi\ ).$$

Pero, entonces los puntos (ξ, υ) constituyen un subconjunto discreto dentro de un compacto del plano.

Observación 3.12. Si F es primitiva, entonces $\mathsf{Stab}(F)_0^+ = \mathsf{Stab}(F)^+$; toda representación propia es equivalente a una única representación primaria. Como, en tal caso, las órbitas por la acción de $\mathsf{Stab}(F)^+$ son una cantidad finita, la cantidad de representaciones primarias de n por F también es finita. Ésta es otra manera de deducir la finitud de las representaciones primarias, en este caso.

Nomenclatura. Si $d < 0$, "representación propia" y "representación primaria" serán tratadas como sinónimos.

Observación 3.13. El conjunto de representaciones primarias de un entero positivo por una forma dada se descompone como unión disjunta según el máximo común divisor de las coordenadas:

$$\mathsf{Primarias}(n, F) \;=\; \bigsqcup_{\substack{t>0\\ t^2|n}} \mathsf{Primarias}_t(n, F) \;=\; \bigsqcup_{\substack{t>0\\ t^2|n}} \mathsf{Primarias}_1\left(\tfrac{n}{t^2}, F\right)\;.$$

La correspondencia entre órbitas de representaciones y representaciones primarias de la Observación 3.11 induce la siguiente correspondencia:

$$\mathsf{Stab}(F)_0^+\backslash\mathsf{Representaciones}_t(n,F) \simeq \mathsf{Primarias}_t(n,F)$$

y, en particular,

$$\mathsf{Stab}(F)_0^+\backslash\mathsf{Propias}(n,F) \simeq \mathsf{Primarias}_1(n,F) \ .$$

3.3 Fórmula para la cantidad de representaciones

El objetivo es obtener una fórmula para la cantidad de representaciones de un entero positivo n por formas de discriminante dado d. Lo que esto significa depede del signo de d. Asumiremos que $(n:d)=1$. En ese caso, sólo tiene sentido considerar representaciones por formas primitivas; si $(n:r:m)=g$, entonces $g^2 \mid d$ y $g \mid (n:d)$.

Lema 3.14. *Si $n>0$ y d es un discriminante coprimo con n, entonces*

$$\sum_{[F]}{}' \left|\mathsf{Stab}(F)^+\backslash\mathsf{Propias}(n,F)\right| = \sum_{f|n}{}' \left(\frac{d}{f}\right) ,$$

donde la primera suma se realiza sobre las clases de formas primitivas de discriminante d, mientras que la segunda se realiza sobre los divisores libres de cuadrados de n.

Demostración. Si la clase de F representa a n propiamente, entonces contiene un representante del tipo $\{n,r,m\}$, donde $0 \le r < 2n$; si no, $[F]$ no aporta a la suma. Así, el lado izquierdo es igual a:

$$\sum_{[n,r,m]}{}' 1 = \#\big\{0 \le r < 2n \,:\, r^2 \equiv d \,(\mathsf{mod}\, 4n)\big\} = \sum_{f|n}{}' \left(\frac{d}{f}\right) .$$

□

Lema 3.15. *Si $n>0$ y d es un discriminante coprimo con n, entonces*

$$\sum_{[F]}{}' \left|\mathsf{Stab}(F)^+\backslash\mathsf{Representaciones}(n,F)\right| = \sum_{k|n} \left(\frac{d}{k}\right) ,$$

donde la segunda suma se realiza sobre todos los divisores positivos de n.

Demostración. Por la Observación 3.3 y el Lema 3.14, el lado izquierdo es igual a:

$$\sum_{[F]}{}' \sum_{\substack{t>0\\ t^2|n}} \left|\mathsf{Stab}(F)^+\backslash\mathsf{Propias}\left(\tfrac{n}{t^2},F\right)\right| = \sum_{\substack{t>0\\ t^2|n}} \sum_{f|\frac{n}{t^2}}{}' \left(\frac{d}{f}\right) = \sum_{k|n} \left(\frac{d}{k}\right) .$$

□

Teorema 3.16. *Sea $n > 0$ y sea d un discriminante coprimo con n.*

- *Si $d < 0$,*

$$\sum_{[F]}{}' \, |\mathsf{Representaciones}(n, F)| \; = \; w(d) \sum_{k|n} \left(\frac{d}{k}\right) \, .$$

- *Si $d > 0$,*

$$\sum_{[F]}{}' \, |\mathsf{Primarias}(n, F)| \; = \; \sum_{k|n} \left(\frac{d}{k}\right) \, .$$

Demostración. Como $(n : d) = 1$, consideramos clases de formas primitivas. En particular, $\mathsf{Stab}(F)^+ = \mathsf{Stab}(F)_0^+$. Si $d < 0$, $w = w(d)$ es la cantidad de elementos en el grupo de isotropía de F; si $d > 0$, la Observación 3.13. □

Referencias

[Dav80] H. Davenport. *Multiplicative Number Theory*. 2nd. ed. Vol. 74. Grad. Texts Math. Springer, Cham, 1980.

[Lan99] E. Landau. *Elementary Number Theory*. Reprint of the 1966 2nd edition. Providence, RI: American Mathematical Society (AMS), 1999.