Formas Cuadráticas

Xabier Legaspi Juanatey

Dirixido por: *Javier Majadas Soto*

Universidade de Santiago de Compostela

FACULTADE DE MATEMÁTICAS

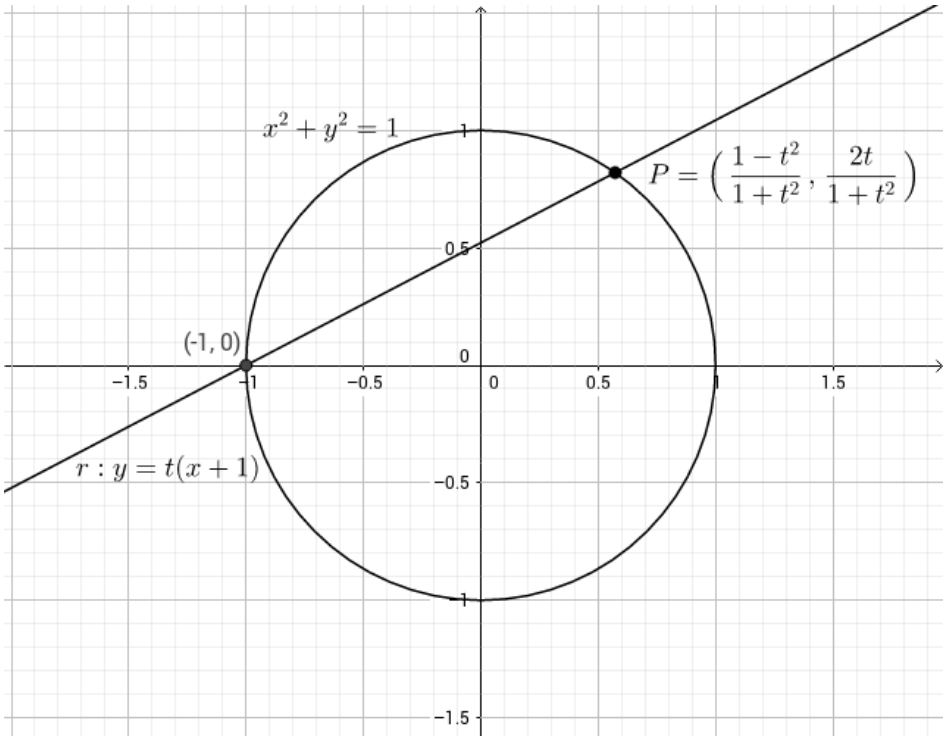
Índice

1. Problema
2. Corpos p–ádicos $\mathbb{Q}_p$
3. Ferramentas
4. Caso $\mathbb{Q}_\infty := \mathbb{R}$
5. Caso $\mathbb{Q}_p$
6. Caso $\mathbb{Q}$: Teorema de Hasse-Minkowski

Problema

Problema

- $(a, b, c) \in \mathbb{Z}^3$ solución de $x^2 + y^2 = z^2 \longrightarrow (\frac{a}{c}, \frac{b}{c})$ punto de $x^2 + y^2 = 1$.
- E reciprocamente.

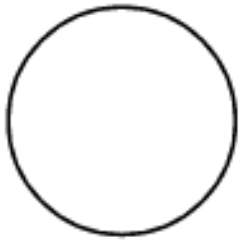


$$t \in \mathbb{Q} \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$$

Problema

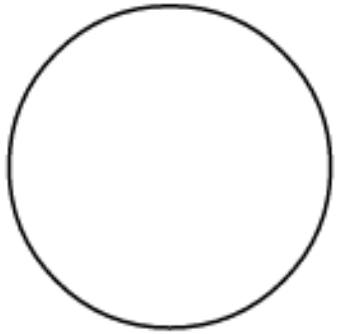
$x^2 + y^2 = z^2$

$x^2 + y^2 = 1$



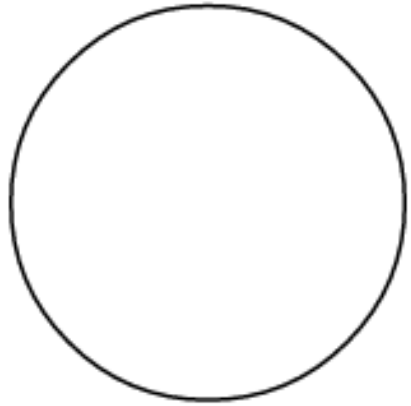
$x^2 + y^2 = 2z^2$

$x^2 + y^2 = 2$



$x^2 + y^2 = 3z^2$

$x^2 + y^2 = 3$



Definición 1.1.1

Unha *forma cuadrática* q sobre K é un polinomio homoxéneo de grao 2 sobre K. Como $car(K) \neq 2$, podemos escribir q como

$$q(x_1, ..., x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \text{ con } a_{ij} = a_{ji} \; \forall i, j$$

A matriz $A := (a_{ij})$ chámase matriz da forma cuadrática q.
Chamaremos *discriminante* de q a $d := det(A)$.

Corpos p–ádicos $\mathbb{Q}_p$

Definición 2.2.4

Chámase *anel dos enteiros p–ádicos* ao anel (conmutativo)

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$$

onde os homomorfismos $\varphi_{n+1}\colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ son os homomorfismos de paso ao cociente (polo ideal $p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$ de $\mathbb{Z}/p^{n+1}\mathbb{Z}$).

Corpos p–ádicos $\mathbb{Q}_p$

Definición 2.2.4

Chámase *anel dos enteiros p–ádicos* ao anel (conmutativo)

$$\mathbb{Z}_p := \varprojlim \mathbb{Z}/p^n\mathbb{Z} \subset \prod_{n\geq 1} \mathbb{Z}/p^n\mathbb{Z}$$

onde os homomorfismos $\varphi_{n+1}\colon \mathbb{Z}/p^{n+1}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ son os homomorfismos de paso ao cociente (polo ideal $p^n\mathbb{Z}/p^{n+1}\mathbb{Z}$ de $\mathbb{Z}/p^{n+1}\mathbb{Z}$).

Definición 2.2.14

Defínese o *corpo dos números p–ádicos* $\mathbb{Q}_p$ como o corpo de fraccións do dominio $\mathbb{Z}_p$.

Corpos p–ádicos $\mathbb{Q}_p$

- Todo elemento non nulo de $\mathbb{Z}_p$ pódese escribir de forma única como $p^n u$ con $u \in \mathbb{Z}_p^*$, $n \in \mathbb{N}$.
- Todo elemento non nulo de $\mathbb{Q}_p$ pódese expresar como $p^t w$ con $t \in \mathbb{Z}$, w unidade de $\mathbb{Z}_p$ e ademais temos que o elemento $\frac{1}{p}$ de $\mathbb{Q}_p$ xera $\mathbb{Q}_p$ como $\mathbb{Z}_p$–subáxlebra, i.e., $\mathbb{Z}_p[\frac{1}{p}] = \mathbb{Q}_p$.

Corpos p–ádicos $\mathbb{Q}_p$

- Todo elemento non nulo de $\mathbb{Z}_p$ pódese escribir de forma única como $p^n u$ con $u \in \mathbb{Z}_p^*$, $n \in \mathbb{N}$.
- Todo elemento non nulo de $\mathbb{Q}_p$ pódese expresar como $p^t w$ con $t \in \mathbb{Z}$, w unidade de $\mathbb{Z}_p$ e ademais temos que o elemento $\frac{1}{p}$ de $\mathbb{Q}_p$ xera $\mathbb{Q}_p$ como $\mathbb{Z}_p$–subáxlebra, i.e., $\mathbb{Z}_p[\frac{1}{p}] = \mathbb{Q}_p$.

Definición 2.2.9

(Valoración p–ádica) Defínese a *valoración p–ádica* en $\mathbb{Z}_p$ como:

$$\nu_p(0) = \infty$$
$$\nu_p(p^n u) = n, \text{ sendo } u \text{ unha unidade}$$

Tamén definimos $|a| := p^{-\nu_p(a)}$ e $d(a,b) := |a-b|$ para $a, b \in \mathbb{Z}_p$.

Corpos p–ádicos $\mathbb{Q}_p$

- Todo elemento non nulo de $\mathbb{Z}_p$ pódese escribir de forma única como $p^n u$ con $u \in \mathbb{Z}_p^*$, $n \in \mathbb{N}$.
- Todo elemento non nulo de $\mathbb{Q}_p$ pódese expresar como $p^t w$ con $t \in \mathbb{Z}$, w unidade de $\mathbb{Z}_p$ e ademais temos que o elemento $\frac{1}{p}$ de $\mathbb{Q}_p$ xera $\mathbb{Q}_p$ como $\mathbb{Z}_p$–subáxlebra, i.e., $\mathbb{Z}_p[\frac{1}{p}] = \mathbb{Q}_p$.

Definición 2.2.9

(Valoración p–ádica) Defínese a *valoración p–ádica* en $\mathbb{Z}_p$ como:

$$\nu_p(0) = \infty$$
$$\nu_p(p^n u) = n, \text{ sendo } u \text{ unha unidade}$$

Tamén definimos $|a| := p^{-\nu_p(a)}$ e $d(a,b) := |a-b|$ para $a, b \in \mathbb{Z}_p$.

- d é métrica en $\mathbb{Z}_p$ e esténdese a $\mathbb{Q}_p$; así dá unha estrutura de espazo métrico en $\mathbb{Q} \subset \mathbb{Q}_p$. $\mathbb{Q}_p$ resulta completación de $\mathbb{Q}$.

Ferramentas

Definición 3.1.1

Sexa p un primo impar e $a \in \mathbb{Z}$. Defínese o *símbolo de Legendre* de a con respecto a p como

$$(a/p) := \begin{cases} 0 & \text{se } p \mid a \\ +1 & \text{se } a \text{ é un cadrado módulo } p \\ -1 & \text{se } a \text{ non é un cadrado módulo } p \end{cases}$$

Sexa $V = \{p \in \mathbb{N} : p \text{ primo}\} \cup \{\infty\}$, e poñamos $\mathbb{Q}_\infty = \mathbb{R}$. Se $a, b \in \mathbb{Q}^*$, denotaremos por $(a,b)_\nu$ o símbolo de Hilbert das imaxes de a e b en $\mathbb{Q}_v$.

Definición 3.4.1

Sexa $v \in V$ e sexan $a, b \in \mathbb{Q}_v^*$. Definimos o *símbolo de Hilbert* de a e b como

$$(a,b) := \begin{cases} 1 & \text{se } ax^2 + by^2 = z^2 \text{ ten algunha solución} \\ & \mathbb{Q}_v^3 \ni (x,y,z) \neq (0,0,0) \\ -1 & \text{en caso contrario} \end{cases}$$

Sexa $V = \{p \in \mathbb{N} : p \text{ primo}\} \cup \{\infty\}$, e poñamos $\mathbb{Q}_\infty = \mathbb{R}$. Se $a, b \in \mathbb{Q}^*$, denotaremos por $(a,b)_\nu$ o símbolo de Hilbert das imaxes de a e b en $\mathbb{Q}_v$.

Definición 3.4.1

Sexa $v \in V$ e sexan $a, b \in \mathbb{Q}_v^*$. Definimos o *símbolo de Hilbert* de a e b como

$$(a,b) := \begin{cases} 1 & \text{se } ax^2 + by^2 = z^2 \text{ ten algunha solución} \\ & \mathbb{Q}_v^3 \ni (x,y,z) \neq (0,0,0) \\ -1 & \text{en caso contrario} \end{cases}$$

Teorema 3.5.1

(Fórmula produto). Se $a, b \in \mathbb{Q}^*$, verifícase:

(I) $(a,b)_v = 1$ para todo $\nu \in V$ salvo en grao sumo un número finito.

(II) $\prod_{v \in V} (a,b)_v = 1$

Corolario 3.4.11

Sexan $a, b \in \mathbb{Q}_p^*$. Poñamos $a = up^\alpha, b = vp^\beta$ con $u, v \in \mathbb{Z}_p^*$.

(I) Se $p \neq 2$, tense

$$(a, b) = (-1)^{\alpha\beta\frac{p-1}{2}} (\overline{u}/p)^\beta (\overline{v}/p)^\alpha$$

onde $\overline{u}$ é a imaxe de u polo homomorfismo de redución módulo p, $\mathbb{Z}_p^* \to (\mathbb{Z}/p\mathbb{Z})^*$, e $(\overline{u}/p)$ é o *símbolo de Legendre*.

(II) Se $p = 2$,

$$(a, b) = (-1)^{\varepsilon(u)\varepsilon(v)+\alpha\omega(v)+\beta\omega(u)}$$

onde $\varepsilon(u)$ é a clase de $\frac{u-1}{2}$ módulo 2 e $\omega(u)$ é a clase de $\frac{u^2-1}{8}$ módulo 2.

Caso $\mathbb{Q}_\infty := \mathbb{R}$

Caso $\mathbb{Q}_\infty := \mathbb{R}$

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{R}$. Como todo número real é un cadrado ou o oposto dun cadrado, eliminando cadrados podemos atopar unha base ortogonal na que

$$q = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2$$

con $r + s = n$

Caso $\mathbb{Q}_\infty := \mathbb{R}$

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{R}$. Como todo número real é un cadrado ou o oposto dun cadrado, eliminando cadrados podemos atopar unha base ortogonal na que

$$q = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2$$

con $r + s = n$

Teorema 4.2.1

(r, s) é independente da base elixida.

Caso $\mathbb{Q}_\infty := \mathbb{R}$

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{R}$. Como todo número real é un cadrado ou o oposto dun cadrado, eliminando cadrados podemos atopar unha base ortogonal na que

$$q = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2$$

con $r + s = n$

Teorema 4.2.1

(r, s) é independente da base elixida.

Definición 4.2.2

Chámase signatura de q ao par de números naturais (r, s).

Caso $\mathbb{Q}_\infty := \mathbb{R}$

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{R}$. Como todo número real é un cadrado ou o oposto dun cadrado, eliminando cadrados podemos atopar unha base ortogonal na que

$$q = x_1^2 + \ldots + x_r^2 - x_{r+1}^2 - \ldots - x_{r+s}^2$$

con $r + s = n$

Teorema 4.2.1

(r, s) é independente da base elixida.

Definición 4.2.2

Chámase signatura de q ao par de números naturais (r, s).

Corolario 4.2.3

Dúas formas cuadráticas non singulares sobre $\mathbb{R}$ son equivalentes se e só se teñen a mesma signatura.

Caso $\mathbb{Q}_p$

Caso $\mathbb{Q}_p$

Sexa $q = a_1x_1^2 + ... + a_nx_n^2$ unha forma cuadrática non singular de rango n sobre $\mathbb{Q}_p$.

- Na *definición 1.1.1* tamén definimos o discriminante $d := \prod_{i=1}^{n} a_i$ de q, que se pode pensar como un elemento de $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$
- Na *definición 4.1.1* definimos un invariante $\varepsilon := \prod_{i<j}(a_i, a_j)_v$ asociado á forma cuadrática q.

Caso $\mathbb{Q}_p$

Sexa $q = a_1x_1^2 + ... + a_nx_n^2$ unha forma cuadrática non singular de rango n sobre $\mathbb{Q}_p$.

- Na *definición 1.1.1* tamén definimos o discriminante $d := \prod_{i=1}^{n} a_i$ de q, que se pode pensar como un elemento de $\mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$
- Na *definición 4.1.1* definimos un invariante $\varepsilon := \prod_{i<j}(a_i, a_j)_v$ asociado á forma cuadrática q.

Teorema 4.1.7

Dúas formas cuadráticas non singulares sobre $\mathbb{Q}_p$ son equivalentes se e só se teñen o mesmo rango, o mesmo discriminante d e o mesmo invariante ε.

Caso $\mathbb{Q}$: Teorema de Hasse-Minkowski

Caso $\mathbb{Q}$: Teorema de *Hasse-Minkowski*

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{Q}$ e sexa $v \in V$. Denotemos por q_v a forma cuadrática obtida vía a inclusión $\mathbb{Q} \to \mathbb{Q}_v$ cando $v = p$. Cando $v = \infty$, podemos definir ε_∞ analogamente ao caso $v = p$.

Caso $\mathbb{Q}$: Teorema de *Hasse-Minkowski*

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{Q}$ e sexa $v \in V$. Denotemos por q_v a forma cuadrática obtida vía a inclusión $\mathbb{Q} \to \mathbb{Q}_v$ cando $v = p$. Cando $v = \infty$, podemos definir ε_∞ analogamente ao caso $v = p$.

Teorema 5.0.1

(Hasse-Minkowski). Unha forma cuadrática non singular q sobre $\mathbb{Q}$ representa cero se e só se q_v representa cero para todo $v \in V$.

Caso $\mathbb{Q}$: Teorema de *Hasse-Minkowski*

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{Q}$ e sexa $v \in V$. Denotemos por q_v a forma cuadrática obtida vía a inclusión $\mathbb{Q} \to \mathbb{Q}_v$ cando $v = p$. Cando $v = \infty$, podemos definir ε_∞ analogamente ao caso $v = p$.

Teorema 5.0.1

(Hasse-Minkowski). Unha forma cuadrática non singular q sobre $\mathbb{Q}$ representa cero se e só se q_v representa cero para todo $v \in V$.

Corolarios 5.0.4 e 5.0.5

- *5.0.4*. Dúas formas cuadráticas racionais non singulares q, q' son equivalentes sobre $\mathbb{Q}$ se e só se o son sobre $\mathbb{Q}_v$ para todo $v \in V$.
- *5.0.5*. Dúas formas cuadráticas racionais non singulares son equivalentes se e só se teñen o mesmo rango, a mesma signatura, o mesmo discriminante (módulo cadrados) e para todo $v \in V$ o mesmo invariante ε_v.

Corolario 4.1.6

Sexa q unha forma cuadrática non singular de rango n sobre $\mathbb{Q}_p$, $a \in \mathbb{Q}_p^*/(\mathbb{Q}_p^*)^2$. Entón

(I) Se $n = 1$, q representa a se e só se $a = d$.

(II) Se $n = 2$, q representa a se e só se $(-d, a) = \varepsilon$.

(III) Se $n = 3$, q representa a se e só se

$$-d \neq a \quad \text{ou} \quad \{-d = a \quad \text{e} \quad (-1, -d) = \varepsilon\}$$

(IV) Se $n = 4$, q sempre representa a.

Bibliografía

- Borevich, Z.I. and Shafarevich, I. *Number theory*. Academic Press, 1966.
- Neukirch, J. *Algebraic number theory*. Springer-Verlag, Berlin, 1999.
- Rousseau, G. *On the quadratic reciprocity law*. J.Austral. Math. Soc. (Series A), p. 423-425, 1991.
- Scharlau, W. *Quadratic and hermitian forms*. Springer-Verlag, Berlin, 1985.
- Selmer, E.S. *The diophantine equation* $ax^3 + by^3 + cz^3 = 0$. Acta Math. 85, p. 203-36, 1951.
- Serre, J-P. *A course in arithmetic*. Springer-Verlag, New York, 1973.
- Voloch, F. *Local-global principles for integral points on curves*. Talk, September 2012.

Graciñas!