EL PRINCIPIO DE HASSE PARA CÓNICAS EN TRES VARIABLES

HOMERO GALLEGOS

Definición. Una *cónica* $\mathcal{C}$ *definida sobre* $\mathbb{Q}$ es una ecuación de la forma

$$F(\mathbf{X}) = a_0X^2 + a_1XY + a_2XZ + a_3Y^2 + a_4YZ + a_5Z^2,$$

donde $\mathbf{X} = (X, Y, Z)$, los $a_i \in \mathbb{Q}$ y el determinante de la matriz

$$\begin{pmatrix} a_0 & a_1/2 & a_2/2 \\ a_1/2 & a_3 & a_4/2 \\ a_2/2 & a_4/2 & a_5 \end{pmatrix}$$

es distinto de cero.

Vamos a demostrar el siguiente teorema.

Teorema 0.1 (Principio de Hasse)**.** *Una cónica* $\mathcal{C}$ *definida sobre* $\mathbb{Q}$ *tiene un punto racional si y sólo si tiene un punto en* $\mathbb{R}$ *y un punto en* $\mathbb{Q}_p$ *para todo primo* p*.*

Es evidente que si una cónica tiene un punto racional, entonces tiene un punto definido sobre los reales y sobre cada $\mathbb{Q}_p$. Vamos a probar la otra dirección usando el teorema de Minkowski. Pero antes será útil reducir el problema.

Notemos que para $q \in \mathbb{Q}\backslash\{0\}$ la ecuación $qF(\mathbf{X}) = 0$ tiene las mismas soluciones que $F(\mathbf{X}) = 0$. Entonces, multiplicando por un denominador común, podemos asumir que la cónica está definida por coeficientes $a_i \in \mathbb{Z}$.

También podemos hacer cambios de variables definidos sobre los racionales del tipo $X' = q_1X + q_2Y + q_3Z$ y similares con Y', Z' tales que la cónica en la nueva base sea de la forma $aX'^2 + bY'^2 + cZ'^2$, con $a, b, c \in \mathbb{Z}$. Más aún, podemos dividir la ecuación entre $\mathrm{mcd}(a, b, c)$ y los coeficientes de la cónica no tendrán un factor común en la nueva ecuación. Si a y b tienen factores comunes, podemos hacer el cambio de variable $Z' = \mathrm{mcd}(a, b)Z$ y los puntos racionales de la nueva cónica corresponden a los puntos racionales de la anterior, y lo mismo es cierto de los puntos reales y los p-ádicos. Los coeficientes de la nueva cónica tendrán un factor común que podemos eliminar y ahora $\mathrm{mcd}(a, b) = 1$. Continuando este proceso con los otros pares, podemos asumir que los coeficientes a, b, c son coprimos por pares. Finalmente, si un primo p^{2i} divide a a con $i > 0$, podemos hacer el cambio de variable $X' = p^{2i}X$. Repitiendo el proceso con b y c obtenemos el siguiente resultado.

Lema 0.2. *Toda cónica racional es equivalente sobre los racionales a una cónica dada por una ecuación de la forma*

$$F(\mathbf{X}) = aX^2 + bY^2 + cZ^2,$$

con $a, b, c \in \mathbb{Z}$ *tales que* $abc \neq 0$ *es libre de cuadrados (es decir, ningún entero* > 1 *de la forma* n^2 *divide al producto* abc*).*

Ahora veremos que la condición *tiene un punto en $\mathbb{Q}_p$ para todo primo p* no es tan imponente como parece.

Lema 0.3. *Sea $\mathcal{C}$ una cónica racional de la forma*

$$F(\mathbf{X}) = aX^2 + bY^2 + cZ^2,$$

con $a, b, c \in \mathbb{Z}$ tales que abc es libre de cuadrados. Si p es un primo que no divide a $2abc$, entonces existe un punto $\mathbf{x}_p \in \mathbb{Q}_p^3$ tal que $F(\mathbf{x}_p) = 0$ en $\mathbb{Q}_p$.

Demostración. Como $p \nmid b$, entonces $by^2 + c$ toma $(p+1)/2$ valores incongruentes en $\mathbb{Z}/p\mathbb{Z}$. Luego, para algún valor de y, $-a^{-1}(by^2+c)$ es un cuadrado en $\mathbb{Z}/p\mathbb{Z}$. Existen pues $x_0, y_0 \in \mathbb{Z}$ tales que $ax_0^2 + by_0^2 + c \equiv 0 \pmod{p}$. Ahora, p no puede dividir a x_0 y a y_0, pues entonces $p \mid c$. Supongamos que $p \nmid x_0$. El polinomio $f(x) = F(x, y_0, 1)$ satisface $f(x_0) \equiv 0 \pmod{p}$, y como p no divide a $2ax_0$ entonces podemos usar el lema de Hasse y existe un $x_p \in \mathbb{Z}_p$ tal que $F(x_p, y_0, 1) = 0$. De manera similar podemos encontrar una solución si p no divide a y_0. Así pues, existe $\mathbf{x}_p \in \mathbb{Z}_p^3$ tal que $F(\mathbf{x}_p) = 0$. □

El principio de Hasse se convierte entonces en el siguiente criterio: $\mathcal{C}$ tiene una solución racional si y sólo si tiene una solución en $\mathbb{R}$ y en $\mathbb{Q}_p$ para los primos $p \mid 2abc$.

Demostremos ahora el principio de Hasse.

Demostración. Supongamos que $\mathcal{C}$ tiene una solución en $\mathbb{R}$ y en $\mathbb{Q}_p$ para los primos $p \mid 2abc$. Queremos demostrar que existe una solución racional. Notemos que para $\lambda \in \mathbb{Q}\backslash\{0\}$ y $\mathbf{x} \in \mathbb{Q}^3\backslash\{0\}$ se tiene que $F(\lambda\mathbf{x}) = 0$ si y solo si $F(\mathbf{x}) = 0$, pues $F(\lambda\mathbf{x}) = \lambda^2 F(\mathbf{x})$. Entonces $\mathcal{C}$ tiene una solución racional no trivial si y sólo si tiene una solución en $\mathbb{Z}^3\backslash\{0\}$.

Queremos usar el teorema de Minkowski para encontrar una solución entera no trivial. Vamos a definir una retícula $\Lambda \subset \mathbb{Z}^3$ de índice $4|abc|$ tal que para todo punto $\mathbf{x} \in \Lambda$, $F(\mathbf{x}) \equiv 0 \pmod{4|abc|}$. Para lograr esto impondremos ciertas congruencias en las variables x, y, z. (El conjunto $\{F(\mathbf{x}) \equiv 0 \pmod{4|abc|}\}$ podría no ser una retícula.)

Sea C el conjunto convexo y simétrico

$$C = \{(x, y, z) \in \mathbb{R}^3 : |a|x^2 + |b|y^2 + |c|z^2 < 4|abc|\}.$$

Este elipsoide tiene volumen

$$\frac{\pi}{3} 2^3 |4abc| > 2^3 |4abc|.$$

Entonces, por el teorema de Minkowski va a existir un punto $\mathbf{x}_0 = (x_0, y_0, z_0)$ distinto de cero en $\Lambda \cup C$. Por la desigualdad del triángulo

$$|F(\mathbf{x}_0)| \leq |a|x_0^2 + |b|y_0^2 + |c|z_0^2 < 4|abc|,$$

y como $F(\mathbf{x}_0) \equiv 0 \pmod{4|abc|}$, entonces se debe tener que $F(\mathbf{x}_0) = 0$.

Ahora, a imponer congruencias. Para p primo con $p \mid 2abc$, sea $\mathbf{x}_p = (x_p, y_p, z_p)$ la solución no trivial en $\mathbb{Q}_p^3$ que existe por hipótesis.

Supongamos primero que $p \mid abc$. Sin pérdida de generalidad, asumamos que $p \mid a$. Multiplicando por una constante, podemos asumir que $\max\{|x_p|_p, |y_p|_p, |z_p|_p\} = 1$. Supongamos por un momento que $|y_p|_p < 1$. Entonces

$$|cz_p^2|_p = |ax_p^2 + by_p^2|_p < 1.$$

Como p no divide a c, entonces $|z_p|_p < 1$. Ahora,

$$|ax_p^2|_p = |by_p^2 + cz_p^2|_p \leq p^{-2}.$$

Pero a es libre de cuadrados. Entonces $|x_p|_p < 1$, lo cual es una contradicción, ya que habíamos asumido máx$\{|x_p|_p, |y_p|_p, |z_p|_p\} = 1$. Por tanto $|y_p|_p = |z_p|_p = 1$.

Vamos proceder por casos.

Caso 1. *p impar, $p \mid a$.* (Los casos $p \mid b, c$ se tratan de manera similar.) Como vimos, $|y_p|_p = |z_p|_p = 1$, así que y_p, z_p son unidades en $\mathbb{Z}_p$. Como

$$|ax_p^2|_p = |b + c(z_p/y_p)^2|_p < 1,$$

entonces existe un entero $r_p \in \mathbb{Z}$ tal que

$$b + cr_p^2 \equiv 0 \pmod{p}.$$

Para definir Λ impondremos la congruencia

$$z \equiv r_p y \pmod{p}.$$

Entonces se tiene que

$$F(x, y, z) \equiv ax^2 + by^2 + cz^2 \equiv (b + r_p^2 c)y^2 \equiv 0 \pmod{p},$$

pues $p \mid a$. Recorriendo cada divisor primo e impar de abc obtenemos un sistema de congruencias que define una retícula en $\mathbb{Z}^3$, pero aún no tiene el índice deseado.

Caso 2. *$p = 2$, $p \mid a$.* De nuevo, $|y_2|_2 = |z_2|_2 = 1$. Ahora, para un entero n impar se tiene que $n^2 \equiv 1 \pmod 8$. Entonces, evaluando $F(x_2, y_2, z_2)$ vemos que se cumple alguno de los siguientes casos:

$$\begin{cases} b + c \equiv 0 \pmod 8 & \text{si } |x_2|_2 < 1, \\ a + b + c \equiv 0 \pmod 8 & \text{si } |x_2|_2 = 1. \end{cases}$$

Sea $s \in \{0, 1\}$ el entero tal que $as^2 + b + c \equiv 0 \pmod 8$, e impongamos las congruencias

$$\begin{cases} y \equiv z & \pmod 4 \\ x \equiv sz & \pmod 2. \end{cases}$$

Entonces, si (x, y, z) satisface las congruencias, $F(x, y, z) \equiv (as^2 + b + c)z^2 \equiv 0 \pmod 8$.

Ahora pasaremos al caso en el que $p \nmid abc$.

Caso 3. *$p = 2$, $p \nmid abc$.* Considerando la ecuación módulo 2 vemos que precisamente dos valores de entre x_2, y_2, z_2 son unidades. Digamos que $|x_2|_2 < 1$ y $|y_2|_2 = |z_2|_2 = 1$. Entonces, evaluando $F(x_2, y_2, z_2)$ vemos que $b + c \equiv 0 \pmod 4$. Impondremos, pues, las congruencias

$$\begin{cases} x \equiv 0 & \pmod 2, \\ y \equiv z & \pmod 2. \end{cases}$$

Si (x, y, z) satisface las congruencias, entonces

$$F(x, y, z) \equiv 0 + (b + c)z^2 \equiv 0 \pmod 4.$$

Definimos ahora $\Lambda \subset \mathbb{Z}^3$ como la retícula de los puntos (x, y, z) que satisfacen todas las congruencias impuestas. La retícula Λ tiene índice $4|abc|$, y la aplicación del teorema de Minkowski descrita al principio de la demostración nos da la existencia de una solución racional no trivial a la ecuación $F(\mathbf{x}) = 0$. □

Observación 1. En la demostración no se usó que la cónica $\mathcal{C}$ tiene soluciones reales. La existencia de soluciones reales también es una consecuencia de las soluciones en $\mathbb{Q}_p$ para todo p.

Observación 2. La demostración tiene una aplicación práctica: si quieres encontrar soluciones racionales de una cónica, redúcela a la forma $aX^2 + bY^2 + cZ^2 = 0$, con abc libre de cuadrados y busca alguna solución en la región acotada

$$C = \{(x, y, z) \in \mathbb{Z}^3 : |a|x^2 + |b|y^2 + |c|z^2 < 4|abc|\}.$$

Esta región no depende de las soluciones en $\mathbb{Q}_p$, sino sólo de lo coeficientes a, b, c. Si la cónica tiene soluciones en $\mathbb{Q}_p$ para todo p, el teorema garantiza la existencia de una solución en la región. Si la cónica no tiene solución en la región, entonces no debe tener alguna solución para algún $\mathbb{Q}_p$ con $p \mid 2abc$. Este algoritmo podrá no ser el más eficiente, pero puede ser útil.