Un principio local-global: el Teorema de Hasse-Minkowski

Silvia Arbeloa Larraz

Trabajo de fin de grado en Matemáticas
Universidad de Zaragoza

Director del trabajo: Carlos de Vera Piquero
13 de junio de 2023

Prólogo

En la Teoría de Números, que comenzó a ser estudiada en profundidad por el matemático Fermat a lo largo del siglo XVII, uno de los problemas históricamente más relevantes es el de decidir la existencia de soluciones enteras y racionales de ecuaciones polinómicas. Dicha existencia de soluciones enteras y racionales ha sido la motivación para importantes teoremas a lo largo de la historia, en concreto para el Teorema de Hasse-Minkowski. Este teorema enunciado y demostrado por Helmut Hasse y Hermann Minkowski en 1923, está relacionado con la existencia de soluciones racionales de una forma cuadrática. En concreto, el Teorema de Hasse-Minkowski da un criterio para decidir si una forma cuadrática con coeficientes racionales tiene soluciones racionales o no. De hecho, puede parecer que la parte importante de resolver una ecuación es dar la forma explícita de las soluciones, pero a menudo es más complejo el simple hecho de saber si existen soluciones racionales o no.

El principal objetivo del presente trabajo es enunciar el Teorema de Hasse-Minkowski para el caso de n variables, y demostrarlo únicamente para el caso $n = 3$. Pero antes de introducirnos con la demostración el teorema, debemos definir y estudiar un nuevo cuerpo que no ha sido visto a lo largo del grado. Este cuerpo es el de los números p-ádicos, con p primo. Dedicaremos parte del trabajo a estudiar su construcción y propiedades básicas.

Este trabajo se divide en 4 capítulos diferentes. El primero consiste en una breve introducción del tema a tratar. El segundo se centra en definir y entender el cuerpo de los números p-ádicos, además de dar algunos resultados para la existencia de soluciones p-ádicas para ecuaciones polinómicas. En el tercer capítulo, el principal del trabajo, se enuncia el teorema para el caso de n variables, y luego se demuestra únicamente para el caso $n = 3$. El trabajo se finaliza con el cuarto capítulo que consiste en dos contraejemplos, uno de grado 3 y otro de grado 4, que muestran que el Teorema de Hasse-Minkowski deja de ser válido en general para ecuaciones polinómicas de grado mayor que dos.

Antes de dar paso al trabajo me gustaría agradecer en estas líneas, en primer lugar a mi tutor del trabajo, Carlos de Vera, por su implicación a lo largo de todo el trabajo. En segundo lugar y no por ello menos importante me gustaría nombrar a Zaragoza y a todos los amigos y buenos momentos que me ha dado esta ciudad a lo largo de toda carrera. Y en último lugar dar las gracias a mi familia por haberme ayudado siempre.

Summary

Finding rational solutions of a quadratic form F is a problem with some complexity, but the essential part of the problem is to know if there exist rational solutions or not. The Hasse-Minkowski Theorem, which is the theorem of this essay, is an important result related to the existence of such solutions. It is a very helpful result that simplifies this question.

Let us summarize the contents of this project. After a brief introduction in the first chapter, the second is devoted to the field of p-adic numbers, which is a central ingredient for the theorem. p-adic numbers are based on a new notion of distance, in which two numbers are closer when their difference is divisible by a raised power of p. For example with 3-adic distance, 4 is much further away from 3 than 84. Although the construction of the p-adic field can be done in different ways, we are going to focus on completing $\mathbb{Q}$ with the p-adic norm. We can see this as adding to $\mathbb{Q}$ all the limits of Cauchy sequences. We will see the main properties of these numbers, and some results that will help us to prove our main theorem as for example, Hensel's Lemma.

We begin the third chapter with the definition of a quadratic form and we also talk about the motivation of our theorem. After that, we state the theorem for the case of n variables, however in the development of the proof we focus only on the case of $n = 3$ variables. The rest of the chapter is dedicated to the details of the proof of the theorem. This is divided into four parts. The first of them is based on reducing the proof to diagonal quadratic forms like:

$$f(x_1,x_2,x_3) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2 \tag{1}$$

with $f_j \in \mathbb{Z}, \forall j = 1,2,3$ and $f_1f_2f_3$ square-free, so that we greatly simplify the proof.

In the second part of the proof we investigate the conditions on the coefficients derived from local solubility. Conditions that give us valuable clues about the existence of integer solutions.

Then we continue with the third part of the proof, which consists in once we have the conditions on the coefficients of the quadratic form with an expression as in (1), defining a set of solutions for this equation. This subset with the sum will have a subgroup structure of $(\mathbb{Z}^3,+)$.

In the final part of the proof, we make use of some elementary geometry results, to show that with the subset we have obtained in the previous argument the only option is that our quatratic form (1) has rational solutions, what gives validity to our theorem for equations of degree two with three variables.

Finally, in the last chapter we give two famous examples in order to show that the Hasse-Minkowski Theorem only holds for equations of degree two. That is to say, we consider these two examples:

$$3x^3 + 4y^3 + 5z^3 = 0, \tag{2}$$

$$x^4 - 17 = 2y^2. \tag{3}$$

One of them is a cubic equation and the other one is of degree four. In both of them, there are solutions in all completions of $\mathbb{Q}$, but this does not imply solubility on $\mathbb{Q}$, so the theorem is not satisfied.

Índice general

Capítulo 1

Introducción

Durante toda la historia, decidir la existencia de soluciones enteras y racionales en ecuaciones ha sido un problema muy recurrente que de hecho, tiene relación con en "décimo problema de Hilbert", para el que hay muchos resultados. En este trabajo nos vamos a centrar en el enunciado del Teorema de Hasse-Minkowski y en su demostración para el caso de $n = 3$ variables, que en particular se trata de uno de los resultados clásicos de Legendre.

El Teorema debe su nombre a los matemáticos Helmut Hasse y Hermann Minkowski. Helmut Hasse demostró este teorema en 1923, y Hermann Minkowski hizo contribuciones previas muy importantes para el desarrollo de formas cuadráticas.

Este resultado establece una relación entre la existencia de soluciones racionales y la existencia de soluciones en todas las completaciones de $\mathbb{Q}$. La completación de un cuerpo es un proceso que permite extender un cuerpo dado para incluir elementos adicionales que completan ciertas propiedades o estructuras. A lo largo de la carrera, hemos tratado siempre con el cuerpo de los número reales $\mathbb{R}$, que es la principal completación de $\mathbb{Q}$, realizada respecto al valor absoluto usual. Pero vamos a ver que existen infinitas completaciones de $\mathbb{Q}$, en concreto una para cada primo p. Estas completaciones, realizadas respecto a la norma p-ádica, que luego la definiremos y explicaremos, dan lugar a los cuerpos $\mathbb{Q}_p$ de los números p-ádicos. Los números p-ádicos fueron descritos por primera vez por Kurt Hensel en torno al 1897.

En términos generales, el Teorema de Hasse-Minkowski establece que una ecuación polinómica de segundo grado tiene soluciones en $\mathbb{Q}$ si y solo si tiene solución en todas sus completaciones, es decir si tiene solución en $\mathbb{Q}_p$ para todo p primo y en $\mathbb{R}$. Es por esto que el Teorema de Hasse-Minkowski es un ejemplo de principio local-global, en el sentido de que soluciones locales (soluciones en $\mathbb{Q}_p$ y en $\mathbb{R}$) implican la existencia de soluciones globales (soluciones en $\mathbb{Q}$).

La importancia de este teorema se debe a que el estudio de soluciones racionales de una ecuación polinómica es un problema en ocasiones muy complicado. Puede parecer que con este teorema lo único que hemos conseguido es pasar de buscar soluciones en un cuerpo a buscarlas en infinitos de ellos. Sin embargo, veremos resultados que nos ayudarán a descartar todas estas completaciones excepto un número finitos de ellas. Además, hay una gran cantidad de resultados, de los cuales enunciaremos alguno, como por ejemplo el Lema de Hensel, que nos dan métodos para la búsqueda de soluciones de ecuaciones polinómicas en los cuerpos p-ádicos. Por lo que hemos convertido un problema de alta complejidad como puede ser la búsqueda de soluciones racionales de una forma cuadrática, en una serie de problemas más elementales, para los que tenemos métodos o herramientas disponibles.

Capítulo 2

Números p-ádicos

En este primer capítulo del trabajo, nuestro objetivo es definir y entender la construcción del cuerpo $\mathbb{Q}_p$ de los números p-ádicos. La construcción de $\mathbb{Q}_p$ que vamos a presentar realiza este cuerpo como completación de $\mathbb{Q}$ respecto a cierta norma. De esta forma, esta construcción es análoga a la obtención de $\mathbb{R}$ como completación de $\mathbb{Q}$ respecto a la norma dada por el valor absoluto habitual.

Para el desarrollo de este capítulo del trabajo hemos seguido mayormente [1, cap.1].

2.1. Normas p-ádicas

Para comenzar con la construcción de los números p-ádicos, primero vamos a dar algunas definiciones sobre sucesiones y normas en espacios métricos que van a ser muy recurrentes a lo largo del trabajo. Sea M un espacio métrico con una función distancia $d : M \times M \to \mathbb{R}$.

Definición. Dada una sucesión $\{x_n\}_{n\in\mathbb{N}} \subseteq M$, diremos que **converge** a $x \in M$ si para cada $\varepsilon > 0, \exists n_\varepsilon \in \mathbb{N}$ tal que para $n \geq n_\varepsilon, d(x_n, x) < \varepsilon$.

Definición. Diremos que una sucesión $\{x_n\}_{n\in\mathbb{N}} \subseteq M$ es de **Cauchy** si para cada $\varepsilon > 0, \exists n_\varepsilon \in \mathbb{N}$ tal que para cada $n, m \geq n_\varepsilon, d(x_n, x_m) < \varepsilon$. Es decir, los términos de una sucesión se acercan entre sí a medida que los índices crecen.

En particular una sucesión convergente es de Cauchy, pero el recíproco no es cierto.

Definición. Un espacio métrico M se dice **completo** si toda sucesión $\{x_n\}_{n\subseteq\mathbb{N}} \in M$ de Cauchy es convergente en M.

$\mathbb{Q}$ no es completo respecto a ninguna métrica: fijada una métrica pueden definirse sucesiones de Cauchy que no converjan, o que converjan a un número $x \notin \mathbb{Q}$.

Ejemplo. *Consideramos $\mathbb{Q}$ junto con el valor absoluto. Sabemos que aunque $\sqrt{2}$ es un número irracional, es posible encontrar una sucesión de Cauchy $\{x_n\}$ de números racionales cuyo límite x verifica que $x^2 = 2$. Esto muestra que $\mathbb{Q}$ no es completo ya que no existe ningún número racional que cumpla esta ecuación.*

Para definir el cuerpo de los números p-ádicos (el cual veremos que sí es completo) necesitamos definir una nueva norma, para la que requerimos un concepto previo.

Definición. Sea $p \in \{2, 3, 5, 7...\}$ un número primo. Para cualquier entero $a \neq 0$, sea $\text{ord}_p a$ la máxima potencia de p tal que divide a a, es decir, el máximo m tal que $a \equiv 0 (\text{ mód } p^m)$. (La notación $a \equiv b (\text{ mód } c)$ significa: c divide $a - b$.) Si $a = 0$, escribimos $\text{ord}_p 0 = +\infty$.

A continuación definimos el concepto de norma p-ádica, que será muy importante a la hora de definir el cuerpo de los números p-ádicos. Primero vamos a recordar qué es una norma.

Definición. Sea A un cuerpo. Una aplicación $||.|| : A \to \mathbb{R}_{\geq 0}$ se dice que es una **norma** si cumple que:

1. $||x|| = 0 \Leftrightarrow x = 0$
2. $||xy|| = ||x||||y|| \quad \forall x, y \in A$
3. $||x+y|| \leq ||x|| + ||y|| \quad \forall x, y \in A$

Una norma $||.||$ define una distancia sobre el conjunto A dada por $d(x,y) = ||x-y||$. Esta función cumple las propiedades de distancia, con lo cual un cuerpo dotado con una norma es en particular un espacio métrico.

Definición. La norma **p-ádica** es la norma $|.|_p$ en $\mathbb{Q}$ caracterizada por:

$$|x|_p = \begin{cases} \frac{1}{p^{\text{ord}_p x}} & \text{si } x \neq 0, \\ 0 & \text{si } x = 0 \end{cases}$$

Es decir, respecto a esta norma, dos números están cerca cuando su diferencia es divisible por una potencia elevada de p.

Vamos a comprobar que la norma p-ádica cumple las condiciones de norma:

1. $x = 0 \Leftrightarrow |x|_p = 0$, obvio por la definición.
2. $\forall x, y \in \mathbb{Q}$ tenemos:

$$|xy|_p = \frac{1}{p^{\text{ord}_p xy}} = \frac{1}{p^{\text{ord}_p x + \text{ord}_p y}} = \frac{1}{p^{\text{ord}_p x} p^{\text{ord}_p y}} = \frac{1}{p^{\text{ord}_p x}} \frac{1}{p^{\text{ord}_p y}} = |x|_p |y|_p.$$

3. Si $x = 0$, $y = 0$, o si $x + y = 0$ es obvio. Asumimos $x, y, x+y \neq 0$. Escribimos $x = \frac{a}{b}, y = \frac{c}{d}$ fracciones irreducibles. Tenemos que:

$$x + y = \frac{ad + bc}{bd}, \quad \text{ord}_p(x+y) = \text{ord}_p(ad+bc) - \text{ord}_p b - \text{ord}_p d.$$

La máxima potencia de p que divide a la suma de dos números, es al menos el mínimo entre las máximas potencias de p que dividen a cada uno de los sumandos, luego tenemos que:

$$\begin{aligned} \text{ord}_p(x+y) &\geq \text{mín}(\text{ord}_p ad, \text{ord}_p bc) - \text{ord}_p b - \text{ord}_p d \\ &= \text{mín}(\text{ord}_p a + \text{ord}_p d, \text{ord}_p b + \text{ord}_p c) - \text{ord}_p b - \text{ord}_p d \\ &= \text{mín}(\text{ord}_p a - \text{ord}_p b, \text{ord}_p c - \text{ord}_p d) \\ &= \text{mín}(\text{ord}_p x, \text{ord}_p y). \end{aligned}$$

Entonces:

$$|x+y|_p = \frac{1}{p^{\text{ord}_p(x+y)}} \leq \text{máx}\left(\frac{1}{p^{\text{ord}_p(x)}}, \frac{1}{p^{\text{ord}_p(y)}}\right) = \text{máx}(|x|_p, |y|_p) \leq |x|_p + |y|_p.$$

Pero nos fijamos en que hemos demostrado una desigualdad todavía más fuerte que las desigualdad triangular, que en particular hace que la norma p-ádica sea una norma no arquimediana:

Definición. Sea A un cuerpo. Una aplicación $||.|| : A \to \mathbb{R}_{\geq 0}$ se dice que es una **norma no arquimediana** si cumple que:

1. $||x|| = 0 \Leftrightarrow x = 0$
2. $||xy|| = ||x||||y|| \quad \forall x, y \in A$

3. $||x+y|| \leq \max(||x||, ||y||) \quad \forall x, y \in A$

Ahora vamos a enunciar un teorema sobre la equivalencia de normas p-ádicas.

Definición. Dos normas $|.|$ y $|.|'$ se dicen **equivalentes** si se cumple que una sucesión arbitraria $\{x_n\}_{n\in\mathbb{N}} \subseteq M$ es de Cauchy respecto a $|.|$ si y solo si lo es también respecto a $|.|'$. Es decir, dos normas se dicen equivalentes si definen métricas (o topologías) equivalentes.

El siguiente teorema clasifica las normas en $\mathbb{Q}$. Salvo equivalencia, las únicas normas posibles sobre el cuerpo de los racionales son la norma habitual dada por el valor absoluto y las normas p-ádicas (una para cada número primo p).

Notación. Para unificar notación, vamos a denotar el valor absoluto habitual como $|.|_\infty = |.|$ (es decir, $|.|_p$ con $p = \infty$).

Teorema 2.1. *(de Ostrowski) Toda norma no trivial $||.||$ sobre $\mathbb{Q}$ es equivalente a $|.|_p$ para algún primo p o para $p = \infty$. Y dos normas p-ádicas no son equivalentes entre sí para primos distintos. Además, el valor absoluto usual no es equivalente a ninguna norma p-ádica.*

Demostración. Vamos a ver solo algunas indicaciones de esta demostración:

Caso 1. Vamos a suponer que existe un entero positivo n tal que $||n|| > 1$, y elegimos el menor n_0 que cumple esto, es decir $||n_0|| > 1$. Entonces existe $\alpha \in \mathbb{R}, \alpha > 0$ tal que $||n_0|| = n_0^\alpha$. También podemos poner cualquier entero n en base n_0 como:

$$n = a_0 + a_1 n_0 + a_2 n_0^2 + ... + a_s n_0^s, \quad 0 \leq a_i < n_0, \quad a_s \neq 0.$$

Entonces aplicando el hecho de que $||n_0|| = n_0^\alpha$, tras un cálculo se llega a que existe una constante C tal que:

$$||n|| \leq C n^\alpha, \forall n = 1, 2, 3, ...$$

Ahora si tomamos $n \in \mathbb{N}$ y $N > n$ y aplicamos la raíz N-ésima, tenemos que

$$||n|| \leq \sqrt[N]{C} n^\alpha,$$

que tomando el límite cuando $N \to \infty$ nos queda que $||n|| \leq n^\alpha$.

También es posible, con una serie de cálculos, obtener la desigualdad en el otro sentido, es decir $||n|| \geq n^\alpha$. De donde obtenemos que $||n|| = n^\alpha$. De aquí se sigue por las propiedades de norma que $||x|| = |x|^\alpha$, por lo que esta norma es equivalente al valor absoluto.

Caso 2. Suponemos $||n|| \leq 1, \forall n \in \mathbb{N}$. Tomamos n_0 el mínimo n que cumple esta condición, que existe ya que hemos supuesto que la norma es no trivial. Tenemos que n_0 es primo, ya que en caso contrario $n_0 = n_1 n_2, \quad n_1, n_2 < n_0$, luego $||n_1|| = ||n_2|| = 1$, luego $||n_0|| = ||n_1||||n_2|| = 1$ lo que sería una contradicción. Luego tomamos $p = n_0$.

Veamos que si q es un número primo distinto a p, entonces $||q|| = 1$. Supongamos lo contrario, es decir $||q|| < 1$. Entonces para algún N lo suficientemente grande, tendríamos que $||q^N|| = ||q||^N < \frac{1}{2}$, y también para algún M lo suficientemente grande, $||p^M|| < \frac{1}{2}$. Como p^M y q^N también son coprimos entre sí, entonces sabemos que existen $m, n \in \mathbb{Z}$ tales que $mp^M + nq^N = 1$, pero entonces

$$1 = ||1|| = ||mp^M + nq^N|| \leq ||mp^M|| + ||nq^N|| = ||m||||p^M|| + ||n||q^N||.$$

Pero $||m||, ||n|| \leq 1$, luego:

$$1 \leq ||p^M|| + ||q^N|| < 1/2 + 1/2 = 1,$$

lo que es una contradicción, así que $||q|| = 1$.

Sea ahora un entero positivo a. Lo factorizamos como producto de primos:

$$a = p_1^{b_1} p_2^{b_2} ... p_r^{b_r},$$

luego

$$a = ||p_1^{b_1}||||p_2^{b_2}||...||p_r^{b_r}||,$$

pero el único p_i que va a cumplir que $||p_i|| \neq 1$ va a ser $p_i = p$ y $b_i = \text{ord}_p a$. Entonces $||a|| = ||p||^{\text{ord}_p a}$. Se puede deducir de aquí que esto se cumple también para cualquier número racional x, luego esta norma es equivalente a $|.|_p$.

□

2.2. El cuerpo de los números p-ádicos

Vamos a volver al tema de la completación de $\mathbb{Q}$. Como hemos dicho antes, el cuerpo $\mathbb{Q}$ no es completo respecto a ninguna métrica.

Definición. Dado un espacio métrico M, decimos que dos sucesiones de Cauchy $\{a_i\}, \{b_i\} \subseteq M$ son **equivalentes** si $\lim_n d(a_n, b_n) = 0$.

Definición. Dado un espacio métrico M definimos su **completación** como el conjunto de clases de equivalencia de sucesiones de Cauchy.

Ahora vamos a explicar el proceso de construcción de los números p-ádicos, $\mathbb{Q}_p$, es decir la completación de $\mathbb{Q}$ respecto la norma p-ádica, que como hemos dicho es análogo al proceso de completar $\mathbb{Q}$ a $\mathbb{R}$. Primero vamos a dar la definición general de este conjunto.

Definición. El **conjunto de los números p-ádicos** $\mathbb{Q}_p$ es el conjunto de clases de equivalencia de sucesiones de Cauchy en $\mathbb{Q}$ con $|.|_p$. Es decir, la completación de $\mathbb{Q}$ respecto a $|.|_p$.

Definición. La **norma $|.|_p$ de una clase de equivalencia** a es el límite $\lim_{n\to\infty} |a_n|_p$ con $\{a_n\}$ cualquier representante de a.

Tenemos que ver que este límite está bien definido. En primer lugar, el límite existe. En efecto, si $a = 0$, entonces por definición tenemos que $\lim_{i\to\infty} |a_i|_p = 0$. En caso contrario, si $a \neq 0$, para algún ε y N, existe $i_N > N$ tal que $|a_{i_N}|_p > \varepsilon$. Entonces tomamos N lo suficientemente grande tal que $|a_i - a_{i'}|_p < \varepsilon$, cuando $i, i' > N$. Tenemos que $|a_i - a_{i_N}|_p < \varepsilon, \quad \forall i > N$. Pero como $|a_{i_N}|_p > \varepsilon$ y la norma p-ádica se trata de una norma no arquimediana tenemos que $|a_i|_p = |a_{i_N}|_p$. Entonces $\forall i > N$, $|a_i|_p = |a_{i_N}|_p$. Luego la sucesión $|a_i|_p$ converge y cumple que $\lim_{i\to\infty} |a_i|_p = |a_{i_N}|_p$.

Por otro lado, vamos a ver que dos sucesiones $\{a_n\}, \{b_n\}$, que representan a un mismo elemento $a \in \mathbb{Q}_p$, nos dan el mismo valor para la norma $|a|_p$, es decir $\lim_{n\to\infty} |a_n|_p = \lim_{n\to\infty} |b_n|_p$.

Como acabamos de ver en el caso de la existencia del límite, para $\{a_n\}$ existe N_1 tal que $\forall i > N_1$, $|a_i|_p = |a_{i_{N_1}}|_p$, y análogamente para $\{b_n\}$ existe N_2 tal que $\forall i > N_2$, $|b_i|_p = |b_{i_{N_2}}|_p$. Luego si tomamos $N = \max(N_1, N_2)$, $\forall i > N$, $|a_i|_p = |a_{i_N}|_p$ y $|b_i|_p = |b_{i_N}|_p$. Entonces, aplicando la desigualdad triangular inversa:

$$\lim_{n\to\infty} |a_n - b_n|_p \geq \lim_{n\to\infty} ||a_n|_p - |b_n|_p| = ||a_N|_p - |b_N|_p|.$$

Por otro lado, como hemos dicho $\{a_n\}, \{b_n\}$ representan el mismo elemento de $\mathbb{Q}_p$, por lo tanto son sucesiones de Cauchy equivalentes respecto a la norma p-ádica, luego $\lim_{n\to\infty} |a_n - b_n|_p = 0$. Entonces

$$0 = \lim_{n\to\infty} |a_n - b_n|_p \geq ||a_N|_p - |b_N|_p| \geq 0,$$

luego

$$|a_N|_p - |b_N|_p = 0,$$

y por tanto

$$\lim_{n\to\infty} |a_n|_p = |a_N|_p = |b_N|_p = \lim_{n\to\infty} |b_n|_p.$$

Vamos a ver un ejemplo que nos ayudará a entender esto:

Ejemplo. *Sea $p = 5$. Veamos que existe una sucesión de enteros que converge en $\mathbb{Q}_5$ a $-\frac{1}{3}$*

Sea $\{a_n\}$ la sucesión con $a_1 = 3, a_2 = 33, a_3 = 333, a_4 = 3333, \ldots$. Tenemos que $a_m \equiv a_n (\text{mód } 5^n) \quad \forall m \geq n$, o equivalentemente

$$|a_m - a_n|_5 \leq 5^{-n} \quad \forall m \geq n.$$

Es decir, se trata de una sucesión de Cauchy.

Observamos que $\forall n \geq 1$

$$3a_n = 99\cdots 9 \equiv -1 (\,\text{mód}\, 5^n).$$

o equivalentemente:

$$|3a_n + 1|_5 \leq 5^{-n},$$

lo que implica que $a_n \to -\frac{1}{3}$ 5-ádicamente.

En el siguiente ejemplo, mostramos que $\sqrt{-1} \in \mathbb{Q}_5$.

Ejemplo. *Sea $p = 5$. Definimos una sucesión $\{a_n\}$ de números entero de manera inductiva. Tomamos $a_1 = 2$, y para $n > 1$ definimos*

$$a_{n+1} = a_n + 5^2.$$

Por definición, es obvio que

$$a_{n+1} \equiv a_n (\,\text{mód}\, 5^n),$$

y se demuestra fácilmente por inducción que $a_n^2 + 1 \equiv 0 (\,\text{mód}\, 5^n) \forall n \geq 1$. Así, $\{a_n\}$ es una sucesión de Cauchy respecto a $|.|_5$, y $a_n^2 + 1 \to 0$ 5-ádicamente, luego $\{a_n\}$ representa $\sqrt{-1}$ en $\mathbb{Q}_5$.

Antes de ver que el cuerpo $\mathbb{Q}_p$ es completo, vamos a ver que en efecto es un cuerpo. Para ello, sean a y b clases de equivalencia de sucesiones de Cauchy, y tomamos dos representantes $\{a_i\} \in a$, $\{b_i\} \in b$, y definimos ab como la clase de equivalencia que representa las sucesión de Cauchy $\{a_i b_i\}$. Suponemos que hubiésemos elegido otros representantes $\{a_i'\} \in a$, $\{b_i'\} \in b$. Tendríamos que:

$$|a_i'b_i' - a_i b_i|_p = |a_i'(b_i' - b_i) + b_i(a_i' - a_i)|_p \leq \text{máx}\left(|a_i'(b_i' - b_i)|_p, |b_i(a_i' - a_i)|_p\right).$$

Como

$$|a|_p \lim_{i\to\infty} |b_i' - b_i|_p = 0,$$

$$|b|_p \lim_{i\to\infty} |a_i' - a_i|_p = 0,$$

tenemos que $|a_i'b_i' - a_i b_i|_p$ tiende a 0, luego $\{a_i'b_i'\} \sim \{a_i b_i\}$.

Análogamente podemos definir la suma de sucesiones de Cauchy: sean a y b clases de equivalencia de sucesiones de Cauchy, tomamos dos representantes $\{a_i\} \in a$, $\{b_i\} \in b$, y definimos $a+b$ como la clase de equivalencia que representa la sucesión de Cauchy $\{a_i + b_i\}$. Suponemos que hubiésemos elegido otros representantes $\{a_i'\} \in a$, $\{b_i'\} \in b$, tendíamos que:

$$|(a_i' + b_i') - (a_i + b_i)|_p = |(a_i' - a_i) + (b_i' - b_i)|_p \leq \text{máx}\left(|a_i' - a_i|_p, |b_i' - b_i|_p\right).$$

Como

$$\lim_{i\to\infty} |a_i' - a_i|_p = 0,$$

$$\lim_{i\to\infty} |b_i' - b_i|_p = 0,$$

tenemos que

$$\text{máx}\left(|a_i' - a_i|_p, |b_i' - b_i|_p\right) \to 0,$$

luego $\{a_i' + b_i'\} \sim \{a_i + b_i\}$.

Para la existencia de inversos hay que hacerlo más cuidadosamente: sean dos sucesiones de Cauchy equivalentes para un mismo representante $\{a_i\} \sim \{a'_i\}$ que ninguna es nula (si algún $a_i = 0$, podemos reemplazarlo por $a'_i = p^i$),

$$\left|\frac{1}{a'_i} - \frac{1}{a_i}\right|_p = \left|\frac{a_i - a'_i}{a'_i a_i}\right|_p.$$

Como

$$\lim_{i\to\infty} |a'_i - a_i|_p = 0,$$

tenemos que

$$\left|\frac{a_i - a'_i}{a'_i a_i}\right|_p \to 0,$$

luego $\left\{\frac{1}{a'_i}\right\} \sim \left\{\frac{1}{a_i}\right\}$.

Entonces ahora es fácil comprobar que el conjunto $\mathbb{Q}_p$ de clases de equivalencia de Cauchy es un cuerpo con el producto, la suma y la inversa como acabamos de definir.

Ahora vamos a demostrar que $\mathbb{Q}_p$ es en efecto completo. Para ello, tomamos una sucesión de Cauchy $\{a_j\}_{j=1,2,...}$ en $\mathbb{Q}_p$, y tenemos que ver que es convergente $\mathbb{Q}_p$. Como $a_j \in \mathbb{Q}_p$, para cada a_j de la sucesión, podemos tomar un representante, que a su vez sera una sucesión de Cauchy de la forma $\{a_{ji}\}_{i=1,2,...}$ en $\mathbb{Q}$. Para cada j fijado, como $\{a_{ji}\}$ es de Cauchy, se cumple que:

$$\exists N_j \in \mathbb{N}, |a_{ji} - a_{ji'}|_p < p^{-j}$$

para cualquier $i, i' \geq N_j$.

Con esto es fácil comprobar que la sucesión $\{a_j\}_{j=1,2,...}$ en $\mathbb{Q}_p$ converge al elemento representado por la sucesión $\{a_{jN_j}\}_{j=1,2,...}$, lo que implica que $\mathbb{Q}_p$ es completo.

Para continuar vamos a enunciar un teorema muy útil, que nos distingue una sucesión de Cauchy para representar a cada elemento $a \in \mathbb{Q}_p$. Pero antes de ello, vamos a enunciar un lema que nos va a ser necesario para la demostración de este teorema:

Lema 2.2. *Si $x \in \mathbb{Q}$ y $|x|_p \leq 1$, entonces para cualquier i existe un entero $\alpha \in \mathbb{Z}$ tal que $|\alpha - x| \leq p^{-i}$. El entero α puede ser tomado en el conjunto $\{0, 1, 2, 3, ..., p^i - 1\}$.*

Teorema 2.3. *Toda clase de equivalencia a en $\mathbb{Q}_p$ tal que $|a|_p \leq 1$ tiene exactamente una sucesión de Cauchy de la forma $\{a_n\}$ que lo representa que cumple:*

1. $0 \leq a_i < p^i$ *para* $i = 1, 2, 3, ...$
2. $a_i \equiv a_{i+1} (\text{mód}\, p^i)$ *para* $i = 1, 2, 3, ...$

Demostración. Unicidad Suponemos que existen dos sucesiones $\{a_i\}$ y $\{a'_i\}$ diferentes que satisfacen las condiciones (1) y (2). Si $a_{i_0} \neq a'_{i_0}$, entonces $a_{i_0} \not\equiv a'_{i_0} (\text{mód}\, p^{i_0})$ ya que ambos están en el intervalo $(0, p^{i_0})$. Entonces como para todo i

$$a_i \equiv a_{i_0} \not\equiv a'_{i_0} \equiv a'_i (\text{mód}\, p^{i_0}),$$

equivalentemente

$$a_i \not\equiv a'_i (\text{mód}\, p^{i_0}).$$

Entonces tenemos que

$$|a_i - a'_i|_p > \frac{1}{p^{i_0}}, \quad \forall i \geq i_0$$

y $\{a_i\} \not\sim \{a'_i\}$.

Existencia Sea $\{b_i\}$ una sucesión de Cauchy. Queremos buscar una sucesión $\{a_i\}$ que sea equivalente y que cumpla las condiciones (1) y (2). Para cada $j = 1,2,3,...$ sea $N(j)$ el menor número natural tal que $|b_i - b_i'|_p \leq p^{-j}$ cuando $i, i' \geq N(j)$. Tenemos que si $i \geq N(1)$, $|b_i|_p \leq 1$, ya que para todo $i' \geq N(1)$ tenemos que

$$|b_i|_p \leq \text{máx}\left(|b_i'|_p, |b_i - b_i'|_p\right) \leq \text{máx}\left(|b_i'|_p, 1/p\right)$$

y $|b_i'|_p \to |a|_p \leq 1$ cuando $i' \to \infty$.

Ahora por el Lema previo buscamos una sucesión de enteros a_j, donde $0 \leq a_j < pj$, tal que $|a_j - b_{N(j)}|_p \leq 1/p^j$. Tenemos que esta es la sucesión que buscábamos, nos falta comprobar la condición (2) y que $\{b_i\} \sim \{a_i\}$.

Primero vamos a ver que $a_{j+1} \equiv a_j (\text{ mód } p^j)$:

$$\begin{aligned} |a_{j+1} - a_j|p &= |a_{j+1} - b_{N(j+1)} + b_{N(j+1)} - b_{N(j)} - (a_j - b_{N(j)})|_p \\ &\leq \text{máx}\left(|a_{j+1} - b_{N(j+1)}|_p, |b_{N(j+1)} - b_{N(j)}|_p, |a_j - b_{N(j)})|_p\right) \\ &\leq \text{máx}\left(\frac{1}{p^{j+1}}, \frac{1}{p^j}, \frac{1}{p^j}\right) = \frac{1}{p^j}. \end{aligned}$$

De aquí se sigue la condición (2).

Ahora vamos a ver que $\{b_i\} \sim \{a_i\}$: Para cualquier j, para $i \geq N(j)$ tenemos que:

$$\begin{aligned} |a_i - b_i|_p &= |a_i - a_j + a_j - b_{N(j)} - (b_i - b_{N(j)})|_p \\ &\leq \text{máx}\left(|a_i - a_j|_p, |a_j - bN(j)|_p, |b_i - b_{N(j)}|_p\right) \\ &\leq \text{máx}\left(\frac{1}{p^{j+1}}, \frac{1}{p^j}, \frac{1}{p^j}\right) = \frac{1}{p^j}. \end{aligned}$$

Luego $|a_i - b_i|_p \to 0$ cuando $i \to \infty$, es decir, las sucesiones son equivalentes.

□

Pero este teorema solo nos da ese representante en el caso en el que $|a|_p \leq 1$. Vamos a ver qué ocurre en el caso en el que esto no se cumple, es decir $|a|_p > 1$. En este caso, lo que ocurre es que podemos multiplicar a por una potencia de p y obtener un número p-ádico $a' = ap^m$ que en este caso sí que cumpla que $|a'|_p \leq 1$, que era la hipótesis del teorema anterior. Luego podremos tomar un representante $\{a_n'\}$ que cumple las condiciones (2.3). Además a cumplirá que $a = a'p^{-m}$ y un representante será la sucesión $\{a_n\}$ con $a_i = a_i'p^{-m}$.

Por otro lado los elementos de la sucesión $\{a_n'\}$ los podemos escribir en base p con un número finito de potencias de p:

$$a_i = b_0 + b_1 p + ... + b_{i-1}p^{i-1}.$$

Como por (2.3) tenemos que $a_i \equiv a_{i+1} (\text{ mód } p^i)$, entonces

$$a_{i+1} = b_0 + b_1 p + ... + b_{i-1}p^{i-1} + b_i p^i.$$

Entonces, podríamos ver $a' \in \mathbb{Q}_p$ como el límite de añadir en cada paso otra potencia de p, pero como las potencias de p cada vez serán mayores, en la norma p-ádica tiende a cero.

Entonces el a inicial, con $|a|_p > 1$, también se puede ver en base de potencias de p, con un número finito de sumandos con potencias negativas, es decir:

$$a = \frac{b_0}{p^m} + \frac{b_1}{p^{m-1}} + ... + \frac{b_{m-1}}{p} + b_m + b_{m+1}p + b_{m+2}p^2 + ...$$

Para finalizar esta sección del capítulo, vamos a definir el anillo de los numero enteros p-ádicos.

Definición. Un número $a \in \mathbb{Q}_p$ es un **número entero p-ádico** si $|a|_p \leq 1$.

Definición. El **anillo de los números enteros p-ádicos** es $\mathbb{Z}_p = \{a \in \mathbb{Q}_p; |a|_p \leq 1\}$.

Vamos a destacar el hecho de que

$$\begin{array}{ccc} \mathbb{Q} & \subseteq & \mathbb{Q}_p \\ \cup| & & \cup| \\ \mathbb{Z} & \subseteq & \mathbb{Z}_p \end{array}$$

Aunque la construcción de $\mathbb{Q}_p$ que hemos presentado es analítica, existe una construcción algebraica en la que se define el anillo $\mathbb{Z}_p$ de los enteros p-ádicos, y a posteriori $\mathbb{Q}_p$ se define como su cuerpo de fracciones. Esta construcción se puede consultar detalladamente en [2, cap.2].

Merece la pena destacar algunos comentarios respecto del diagrama anterior. Por un lado recordamos que $\mathbb{Z}$ es un dominio de ideales principales. Además los ideales maximales de $\mathbb{Z}$ son precisamente los ideales de la forma $\langle q \rangle = q\mathbb{Z}$ con q primo. El cuerpo $\mathbb{Q}$ de los números racionales es el cuerpo de fracciones de $\mathbb{Z}$. Por otro lado, $\mathbb{Z}_p$ es también un dominio y $\mathbb{Q}_p$ es su cuerpo de fracciones. Sin embargo $\mathbb{Z}_p$ posee un único ideal maximal que es $p\mathbb{Z}_p$. En particular $\mathbb{Z}_p$ es un anillo local.

Podemos ver $\mathbb{Z}_p$ como unión de dos subconjuntos:

$$\mathbb{Z}_p = \{a \in \mathbb{Z}_p || a|_p < 1\} \cup \{a \in \mathbb{Z}_p || a|_p = 1\} = p\mathbb{Z}_p \cup \mathbb{Z}_p^*, \tag{2.1}$$

donde $p\mathbb{Z}_p$ es el conjunto de enteros p-ádicos múltiplos de p y es el único ideal maximal del anillo. $\mathbb{Z}_p^*$ es el conjunto de enteros p-ádicos que no son divisibles por p. Los elementos de $\mathbb{Z}_p^*$ son los únicos enteros p-ádicos cuyo inverso también es un entero p-ádico.

Además

$$\mathbb{Z}_p / p\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}.$$

2.3. Ecuaciones polinómicas en $\mathbb{Q}_p$

En esta última sección del capítulo de los números p-ádicos vamos a ver un lema que nos va ayudar a la hora de ver si una ecuación polinómica tiene soluciones p-ádicas enteras:

Lema 2.4. *(de Hensel) Sea $P(x) = c_0 + c_1 x + \ldots + c_n x^n$ un polinomio, cuyos coeficientes son enteros p-ádicos. Sea $P'(x) = c_1 + 2c_2 x + \ldots + nc_n x^{n-1}$ su derivada. Y sea a_0 un entero p-ádico tal que $P(a_0) \equiv 0 (\text{ mód } p)$ y $P'(a_0) \not\equiv 0 (\text{ mód } p)$. Entonces $\exists$ un único entero p-ádico a tal que $P(a) = 0$ y $a \equiv a_0 (\text{ mód } p)$.*

Demostración. Vamos a demostrar que existe una única sucesión $a_1, a_2, \ldots$ con $a_i \in \mathbb{Z}$ tal que $\forall n \geq 1$:

1. $F(a_n) \equiv 0 (\text{ mód } p^{n-1})$
2. $a_n \equiv a_{n+1} (\text{ mód } p^n)$
3. $0 \leq a_n < p^{n+1}$

Vamos a probar que tales a_n existen y son únicos por inducción sobre n.

Si $n = 1$, sea $\bar{a_0}$ el único entero en $\{0, 1, \ldots, p-1\}$ tal que $\bar{a_0} \equiv a_0 (\text{ mód } p)$. Cualquier a_1 que cumpla 2 y 3 va a ser de la forma $\bar{a_0} + b_1 p$, con $0 \leq b_1 \leq p-1$. Ahora, si nos fijamos en $F(\bar{a_0} + b_1 p)$ y expandimos el polinomio, recordando que solo necesitamos congruencia a 0 módulo p^2, por lo que cualquier término divisible por p^2 puede ser ignorado.

$$\begin{aligned} F(a_1) = F(\bar{a}_0 + b_1 p) &= \sum_i c_i (\bar{a}_0 + b_1 p)^i \\ &= \sum_i \left(c_i \bar{a}_0^i + i c_i \bar{a}_0^{i-1} b_1 p + \text{ términos divisibles por} p^2 \right) \\ &\equiv \sum_i c_i \bar{a}_0^i + \left(\sum_i i c_i \bar{a}_0^{i-1} \right) b_1 p \left(\text{mód } p^2 \right) \\ &= F(\bar{a}_0) + F'(\bar{a}_0) b_1 p. \end{aligned}$$

Como hemos asumido que $F(a_0) \equiv 0 (\text{ mód } p)$, podemos escribir $F(\bar{a}_0) \equiv \alpha p \left(\text{ mód } p^2\right)$ para algún $\alpha \in \{0,1,\ldots,p-1\}$. Entonces para obtener $F(a_1) \equiv 0 \left(\text{ mód } p^2\right)$, es equivalente a $\alpha p + F'(a_0) b_1 p \equiv 0 \left(\text{ mód } p^2\right)$, es decir, $\alpha + F'(\bar{a}_0) b_1 \equiv 0 (\text{ mód } p)$.

Como $F'(a_0) \neq 0 (\text{ mód } p)$, existe $b_1 \in \{0,1,\ldots,p-1\}$ tal que $\alpha + F'(a_0) b_1 \equiv 0 (\text{ mód } p)$. Claramente $b_1 \in \{0,1,\ldots,p-1\}$ es el único determinado por esta condición.

Para continuar con la inducción, suponemos que tenemos $a_1, a_2, \ldots, a_{n-1}$. Podemos encontrar a_n. Por 2 y 3, necesitamos $a_n = a_{n-1} + b_n p^n$ con $b_n \in \{0,1,\ldots,p-1\}$. Expandimos $F(a_{n-1} + b_n p^n)$ como hemos hecho en el caso $n = 1$, ignorando los términos divisibles por p^{n+1}. Se llega a:

$$F(a_n) = F(a_{n-1} + b_n p^n) \equiv F(a_{n-1}) + F'(a_{n-1}) b_n p^n \left(\text{ mód } p^{n+1}\right).$$

Como $F(a_{n-1}) \equiv 0 \left(\text{ mód } p^n\right)$ por hipótesis, podemos escribir $F(a_{n-1}) = \alpha' p^n \left(\text{ mód } p^{n+1}\right)$, y nuestra condición buscada $F(a_n) \equiv 0 \left(\text{ mód } p^{n+1}\right)$ ahora es:

$$\alpha' p^n + F'(a_{n-1}) b_n p^n \equiv 0 \left(\text{ mód } p^{n+1}\right),$$

es decir,

$$\alpha' + F'(a_{n-1}) b_n \equiv 0 (\text{ mód } p).$$

Ahora como $a_{n-1} \equiv a_0 (\text{mód } p)$, se puede comprobar que $F'(a_{n-1}) \equiv F'(a_0) \neq 0 \ (\text{mód } p)$, y podemos buscar $b_n \in \{0,1,\ldots,p-1\}$ con un procedimiento similar al de b_1, es decir, resolviendo $b_n \equiv \alpha'/F'(a_{n-1}) (\text{ mód } p)$.

El teorema se sigue de aquí, en efecto sea $a = \bar{a}_0 + b_1 p + b_2 p^2 + \cdots$. Como para todo n tenemos que $F(a) \equiv F(a_n) = 0 \left(\text{ mód } p^{n+1}\right)$, se sigue que el número p-ádico $F(a)$ debe ser 0. Recíprocamente, cualquier $a = \bar{a}_0 + b_1 p + b_2 p^2 + \cdots$, proporciona una sucesión como la que buscábamos. La unicidad de esta sucesión implica la unicidad de a. □

Para entender bien este lema, vamos a ver un ejemplo:

Ejemplo. *Consideramos el polinomio con coeficientes enteros*

$$P(x) = x^2 + 1.$$

En particular $P(x)$ tiene coeficientes en $\mathbb{Z}_5$. Por ejemplo veamos si existe algún $a \in \mathbb{Q}_5$ tal que $P(a) = 0$. Para ello calculamos primero su derivada: $P'(x) = 2x$. Tenemos que $a_0 = 2$ cumple que:

$$P(2) = 4 + 1 = 5 \equiv 0 (\text{ mód } 5),$$

$$P'(2) = 4 \not\equiv 0 (\text{ mód } 5).$$

Luego, gracias al Lema de Hensel, sabemos que el polinomio P tiene una raíz en $\mathbb{Q}_5$.

Existe una generalización de este Lema de Hensel para polinomios con n variables, que se puede encontrar en el Teorema 1 de [3, p.14].

Finalmente, vamos a ver un criterio para decidir si un elemento en $\mathbb{Q}_p$ es un cuadrado o no. En los reales es muy fácil ver esto, en efecto, un elemento $x \in \mathbb{R}$ es un cuadrado si y solo si es no negativo, pero en los p-ádicos no es tan sencillo. Así que para ello vamos a enunciar dos lemas, tenemos que separar el caso en el que $p = 2$, porque este necesita condiciones más fuertes. Para demostrar los dos siguientes lemas hemos consultado [2, cap.2].

Lema 2.5. *Sea $p \neq 2$ y $\alpha \in \mathbb{Q}_p$ una unidad. Entonces $\alpha = \beta^2$ para algún $\beta \in \mathbb{Q}_p$ si y solo si existe $\gamma \in \mathbb{Q}$ tal que $|\alpha - \gamma^2|_p < 1$.*

Demostración. $\Rightarrow$ Obvio.

$\Leftarrow$ Primero vamos a ver que podemos suponer que $|\alpha|_p, |\gamma|_p \leq 1$. En efecto, si $|\alpha|_p \geq 1$, tomando $k \in \mathbb{Z}$ suficientemente grande tal que $|p^{2k}\alpha|_p < 1$, y como α es un cuadrado si y solo si $p^{2k}\alpha$ lo es, podemos sustituir α por $p^{2k}\alpha$ sin pérdida de generalidad. Por otro lado, siendo $|\alpha|_p < 1$, la hipótesis $|\alpha - \gamma^2|_p < 1$, implica $|\gamma|_p < 1$.

Ahora definimos $\beta_1 = \gamma$ y construimos una sucesión de números racionales $\beta_1, \beta_2, \beta_3, ...$ de manera inductiva para $n > 1$, como

$$\beta_{n+1} = \beta_n + \frac{\alpha - \beta_n^2}{2\beta_n}.$$

Se puede comprobar por inducción utilizando propiedades de la norma p-ádica que esta sucesión es de Cauchy respecto a la norma p-ádica y que el limite de su cuadrado es α. De hecho, se puede verificar que

$$|\beta_n^2 - \alpha|_p \leq p^{-n}, \quad |\beta_{n+1} - \beta_n|_p \leq p^{-n}.$$

Luego esta sucesión define $\beta \in \mathbb{Q}_p$ tal que $\beta^2 = \alpha$. □

Para el caso $p = 2$ como hemos dicho necesitamos una condición más fuerte:

Lema 2.6. *Sea $p = 2$ y $\alpha \in \mathbb{Q}_2$ una unidad. Entonces $\alpha = \beta^2$ para algún $\beta \in \mathbb{Q}_2$ si y solo si cumple que $|\alpha - 1|_2 < 2^{-3}$.*

Para terminar con este capítulo sobre los números p-ádicos, vamos a ver el hecho de que $\mathbb{Q}_p$ no se trata de un cuerpo algebraicamente cerrado.

Definición. Un cuerpo F se dice algebraicamente cerrado si para cada polinomio de grado al menos 1 con coeficientes en F, tiene al menos un cero en F.

En el caso de completar $\mathbb{Q}$ con el valor absoluto, que obtenemos $\mathbb{R}$, el cual ya hemos dicho que es completo, pero no es algebraicamente cerrado. Por ejemplo el polinomio

$$x^2 + 1 = 0$$

no tiene soluciones en $\mathbb{R}$. La construcción de la clausura algebraica de $\mathbb{R}$, $\mathbb{C}$, es sencilla, ya que consiste en añadir a este cuerpo i.

El cuerpo de los p-ádicos tampoco es algebraicamente cerrado para ningún primo p, es decir existen polinomios con coeficientes en $\mathbb{Q}_p$ que no tienen ningún cero en $\mathbb{Q}_p$. Pero la construcción de la clausura algebraica del cuerpo de los p-ádicos es bastante más compleja que la de $\mathbb{R}$. Como no es necesario para la demostración del Teorema de Hasse-Minkowski, la dejamos a consultar en [1, sec.3 cap.3].

Capítulo 3

Teorema de Hasse-Minkowski

3.1. Motivación y enunciado del Teorema

El principal objetivo de nuestro trabajo es demostrar el Teorema de Hasse-Minkowski, que esta relacionado con las soluciones racionales de una forma cuadrática.

Definición. Sea K un cuerpo. Una **forma cuadrática** sobre K es una aplicación:

$$\begin{array}{rccc} F: & K^n & \to & K \\ & \mathbf{x} & \mapsto & \mathbf{x}^t A\mathbf{x} \end{array}$$

donde A es una matriz cuadrada simétrica de orden n con entradas en K.

Dada una forma cuadrática F sobre $\mathbb{Q}$, nos planteamos si existe algún criterio para decidir si la ecuación $F(\mathbf{x}) = 0$ tiene soluciones racionales. Vamos a empezar con un ejemplo:

Ejemplo.

$$x^2 - 2y^2 + z^2 = 0$$

Tiene una solución racional en el punto $(2,2,2)$*, lo que implica que también tiene solución en* $\mathbb{Q}_p$ *con* p *primo y* $p = \infty$ *ya que el cuerpo* $\mathbb{Q}$ *está contenido en estos cuerpos.*

Antes de nada vamos a aclarar que la cónica $f(x_1, x_2, x_3)$ tiene una solución en $\mathbb{Q}_p$ si existe

$$a = (a_1, a_2, a_3) \neq (0,0,0)$$

con $a_j \in \mathbb{Q}_p$ tal que $f(a_1, a_2, a_3) = 0$.

Con este ejemplo vemos muy claro que si una forma cuadrática tiene solución en $\mathbb{Q}$, también la tiene en todas sus completaciones, es decir en todo $\mathbb{Q}_p$ con p primo y $p = \infty$ ya que $\mathbb{Q} \subseteq \mathbb{Q}_p$.

Nuestra pregunta es si el recíproco es cierto, es decir, si tener soluciones en $\mathbb{Q}_p$ $\forall p$ primo y $p = \infty$ implica la existencia de soluciones en $\mathbb{Q}$.

El Teorema de Hasse-Minkowski nos asegura que el recíproco es cierto. Vamos a enunciarlo para el caso de n variables, aunque a la hora de desarrollar la demostración nos centraremos en el caso $n = 3$, es decir ecuaciones proyectivas de cónicas en el plano.

El hecho de ver cuando una forma cuadrática tiene soluciones racionales, geométricamente, está relacionado con ver si una cónica en el plano tiene puntos con coordenadas racionales o no. Para entender mejor el fin de este teorema, vamos a ver un ejemplo.

Supongamos que tenemos una ecuación de la forma

$$ax^2 + bxy + cy^2 = d, \quad a,b,c,d \in \mathbb{Q}, \tag{3.1}$$

que no es una forma cuadrática, pero las soluciones de esta ecuación están relacionada con las soluciones de

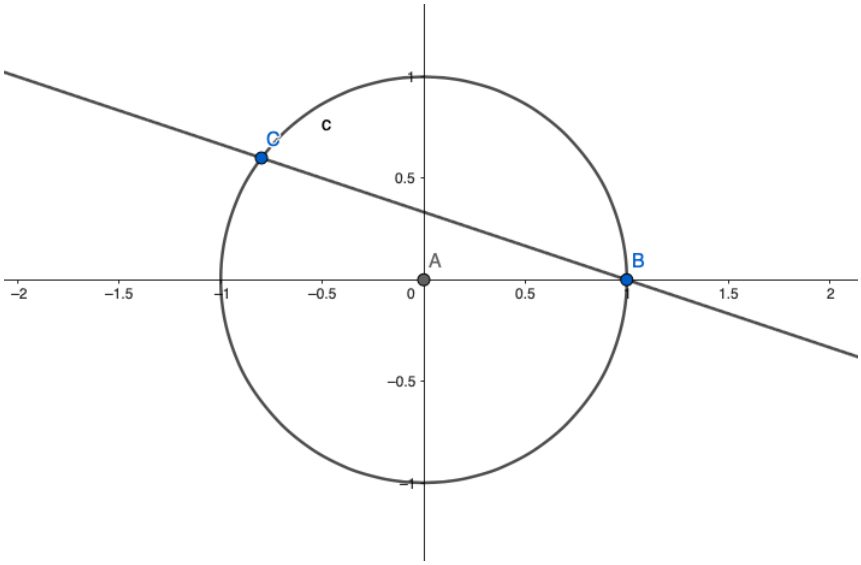
$$ax^2 + bxy + cy^2 - dz^2 = 0.$$

Nos planteamos el problema de encontrar todas las soluciones de esta ecuación $(x,y) \in \mathbb{Q} \times \mathbb{Q}$. Pero antes de abordar este problema, nos surge la duda de si existen soluciones racionales o no. Para ilustrar este problema vamos a ver el caso de la circunferencia unidad

$$x^2 + y^2 = 1.$$

Es evidente que esta ecuación tiene soluciones racionales, por ejemplo $(1,0), (-1,0), (0,1), (0,-1)$.

Si cogemos una de estas soluciones racionales, por ejemplo $(1,0)$, y trazamos rectas con un pendiente $m \in \mathbb{Q}$, es decir $y = m(x-1)$, en el punto en el que esta recta interseque con la circunferencia nos dará mas puntos racionales. Visualmente:



Tenemos el punto $B = (1,0)$, trazamos una recta con un pendiente m racional, y el punto C será otro punto de la circunferencia con coordenadas racionales.

Es decir, si tenemos las dos ecuaciones:

$$\begin{cases} x^2 + y^2 = 1 \\ y = m(x-1) \end{cases}$$

Introducimos la segunda ecuación en la primera:

$$x^2 + (m(x-1))^2 = 1 \Rightarrow (1+m^2)x^2 - 2m^2x + (m^2-1) = 0.$$

Resolviendo esta ecuación de segundo grado obtenemos

$$\begin{cases} x = 1 \\ x = \frac{m^2-1}{m^2+1}, \end{cases}$$

Introduciendo esto en y:

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

En conclusión, como teníamos un punto racional, trazando rectas desde ese punto, hemos obtenido todas las soluciones racionales de la circunferencia unidad que son:

$$\left(\frac{m^2-1}{m^2+1}, \frac{-2m}{m^2+1}\right), \quad m \in \mathbb{Q}.$$

Sabemos que todas las soluciones racionales de la circunferencia están recogidas de esta forma debido a que si tomamos un punto $(a,b) \in \mathbb{Q} \times \mathbb{Q}$ y trazamos un recta hasta el punto $(1,0)$, como ambos puntos tienen coordenadas racionales, claramente esta recta va a tener pendiente racional.

Volviendo al caso de una cónica general de la forma (3.1), funciona el mismo método que con la circunferencia.

Así, llegamos a la conclusión de que el problema de hallar todas las soluciones racionales, se limita a demostrar si hay soluciones racionales o no. El Teorema de Hasse-Minkowski, nos convierte el hecho de buscar soluciones racionales de una cónica, que es algo complicado, a buscar soluciones en los cuerpos p-ádicos. En estos cuerpos tenemos recursos para decidir si hay soluciones o no, por ejemplo el Lema de Hensel. Además, aunque puede parecer que hemos pasado de buscar solución en un cuerpo, a tener que buscarla en infinitos $\mathbb{Q}_p$, veremos en 3.2, que basta con hallar solución en un número finito de ellos.

Como ya hemos dicho, vamos a enunciar este teorema para n variables:

Teorema 3.1. *(de Hasse-Minkowski): Si $f(\boldsymbol{x})$ es una forma cuadrática con coeficientes en $\mathbb{Q}$, entonces, la ecuación $f(\boldsymbol{x}) = 0$ admite solución no trivial en $\mathbb{Q}^n$ si y solo si la ecuación $f(\boldsymbol{x}) = 0$ admite solución no trivial en $\mathbb{Q}_p^n$ $\forall p$ primo y $p = \infty$.*

El ejemplo previo nos ayuda a ver que la implicación a derecha es obvia, ya que el cuerpo $\mathbb{Q}$ está contenido en todas sus completaciones. Entonces, si tiene solución $\mathbb{Q}$ la va a tener por tanto en $\mathbb{Q}_p$ con p primo y $p = \infty$.

Para proceder con la demostración, como hemos dicho nos vamos a limitar al caso de formas cuadráticas en 3 variables con coeficientes en el cuerpo $\mathbb{Q}$ de los racionales, es decir:

$$\begin{array}{ccccc} F: & \mathbb{Q}^3 & \to & & \mathbb{Q} \\ & (x_1,x_2,x_3) & \mapsto & \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} \begin{pmatrix} \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \\ \bullet & \bullet & \bullet \end{pmatrix} \begin{pmatrix} x_1 & x_2 & x_3 \end{pmatrix}. \end{array}$$

En este caso, $n = 3$, el Teorema de Hasse-Miskowski es consecuencia de un resultado clásico de Legendre que podemos consultar en [4, sec.3 cap.17]. Si se quiere consultar la demostración para el caso de n variables, se encuentra en [2, cap.3 y cap.4]. Esta demostración requiere el uso de una herramienta que no hemos explicado, el símbolo de Hilbert.

Antes de empezar con la demostración, vamos a hacer un esquema de cómo vamos a proceder para poder luego entenderlo mejor:

Primero vamos a ver que sin pérdida de generalidad, es suficiente con demostrar el teorema para una forma cuadrática de la forma $f_1x_1^2 + f_2x_2^2 + f_3x_3^2$ con $f_1, f_2, f_3 \in \mathbb{Z}$ con $f_1f_2f_3$ libre de cuadrados.

Lo que haremos luego será suponer que la forma cuadrática tiene soluciones no triviales en todas la completaciones de $\mathbb{Q}$, es decir en $\mathbb{Q}_p$ para todo p primo y $p = \infty$, lo que nos impondrá unas condiciones en los coeficientes de la forma cuadrática, condiciones que nos llevarán a demostrar la existencia de soluciones no triviales también sobre el cuerpo $\mathbb{Q}$.

3.2. Demostración caso n=3

Para el desarrollo de esta sección nos hemos basado en [2, cap.3 y cap.5].

3.2.1. Reducción al caso diagonal

Vamos a comenzar esta sección demostrando el hecho de que basta con demostrar este teorema para formas cuadráticas diagonales

$$f(x_1,x_2,x_3) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2.$$

Lema 3.2. *Para probar el Teorema de Hasse-Minkowski es suficiente con probarlo para formas cuadráticas*

$$f(x_1,x_2,x_3) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2$$

con $f_j \in \mathbb{Z} \quad \forall j = 1,2,3$ *y* $f_1f_2f_3$ *libre de cuadrados.*

Demostración. Primero vamos a ver que es suficiente con considerar solo formas cuadráticas diagonales

$$f(x_1,x_2,x_3) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2$$

Esto se debe a que si tomamos una transformación T que venga dada por

$$T(x_i) = \sum_i t_{ij}y_j$$

con $t_{ij} \in \mathbb{Q}$, $\det(t_{ij}) \neq 0$, esta nos lleva una forma cuadrática de la forma $f(X)$ a otra $g(Y)$. Luego si tenemos un punto (x_1,x_2,x_3) que cumple $f(x_1,x_2,x_3) = 0$, T nos lo lleva a un (y_1,y_2,y_3) que cumple $g(y_1,y_2,y_3) = 0$. Luego el teorema se cumple para $f(X) = 0$ si y solo si se cumple para $g(Y) = 0$. Como toda matriz real simétrica diagonaliza, existe una transformación que convierte la forma inicial F en una forma diagonal.

En segundo lugar, para ver que podemos suponer que $f_j \in \mathbb{Z} \quad \forall j = 1,2,3$, podemos tomar una transformación T que en este caso venga dada por:

$$T(x_j) = t_jx_j$$

con $t_j \in \mathbb{Q}$, tales que $t_j \cdot f_j \in \mathbb{Z}$. De esta forma podemos suponer que los coeficientes serán números enteros.

Finalmente podemos suponer que $f_1f_2f_3$ libre de cuadrados. Si los tres coeficientes tuviesen un factor común primo p, podríamos reemplazar $F(X)$ por $p^{-1}F(X)$, o por ejemplo si solo lo tuviesen dos de los coeficientes, suponemos f_1 y f_2 sin pérdida de generalidad, podríamos reemplazar x_3 por px_3 y $F(X)$ por $p^{-1}F(X)$. Luego así llegaríamos a que $f_1f_2f_3$ libre de cuadrados. □

Una vez demostrado esto, sabemos que de ahora en adelante, para simplificar la demostración, supondremos formas cuadráticas como la que hemos descrito.

Así que vamos a suponer en todo momento que tenemos una forma cuadrática de la forma

$$f(x_1,x_2,x_3) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2 \tag{3.2}$$

con $f_j \in \mathbb{Z} \quad \forall j = 1,2,3$ y $f_1f_2f_3$ libre de cuadrados.

Ahora, vamos a demostrar que en todos los cuerpos p-ádicos menos en un número finito, siempre hay solución. Como hemos dicho en la sección anterior, el fin de nuestro teorema es pasar de buscar soluciones en $\mathbb{Q}$ a buscarlas en un número finito de $\mathbb{Q}_p$'s. Así que gracias a la proposición que vamos a enunciar ahora, vamos a reducir el número de primos en los que hay que buscar soluciones.

Lema 3.3. *Sea una forma cuadrática de la forma (3.2). Sea p primo tal que* $p \nmid f_1f_2f_3$. *Entonces la ecuación en congruencias*

$$f(x_1,x_2,x_3) \equiv 0 (\text{ mód } p)$$

siempre tiene solución.

Demostración. Vamos a buscar las soluciones en el conjunto $\mathbb{F}_p$. Los elementos invertibles de $\mathbb{F}_p$ forman un grupo con la multiplicación, grupo de unidades que vamos a denotar como $\mathbb{F}_p^*$. Este grupo cumple que $|\mathbb{F}_p^*| = p-1$ y es cíclico. Es decir, $\mathbb{F}_p^* = \langle a \rangle$ donde a es una unidad de orden $p-1$ (la mínima potencia de a que cumple $a^\alpha = 1$ es $\alpha = p-1$).

Por otro lado, los elementos de $\mathbb{F}_p^*$ pueden ser cuadrados o no, si lo son serán de la forma a^{2k} y si no lo son, serán a^{2k+1}, con $k = 1,2,...,\frac{p-1}{2}$. Luego tanto el subconjunto de cuadrados, como no cuadrados tienen cardinal $\frac{p-1}{2}$. Sea

$$S^* = \left\{x^2 | x \in \mathbb{F}_p^*\right\},$$

el subgrupo de los cuadrados de $\mathbb{F}_p^*$, $|S^*| = \frac{p-1}{2}$. Además se cumplen las siguientes propiedades que vamos a necesitar:

- Si b es un cuadrado $\Rightarrow b^{-1}$ también, lo mismo con no cuadrados.
- Si b,c son cuadrados $\Rightarrow b \cdot c$ también es un cuadrado.
- Si b,c son no cuadrados $\Rightarrow b \cdot c$ es un cuadrado.

Volvemos a la ecuación inicial:

$$f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2 = 0.$$

Reduciendo módulo p obtenemos la ecuación en $\mathbb{F}_p$:

$$\bar{f}_1 x_1^2 + \bar{f}_2 x_2^2 + \bar{f}_3 x_3^2 = 0, \quad \bar{f}_1, \bar{f}_2, \bar{f}_3 \in \mathbb{F}_p^*. \tag{3.3}$$

Podemos suponer que esta ecuación tiene al menos dos coeficientes que son cuadrados. En efecto, suponemos que 2 son no cuadrados, suponemos también que $\bar{f}_1$ no es cuadrado (si no, reordenamos). Dividimos toda la igualdad por $\bar{f}_1$:

$$x_1^2 + \frac{\bar{f}_2}{\bar{f}_1} x_2^2 + \frac{\bar{f}_3}{\bar{f}_1} x_3^2 = 0,$$

que tiene las mismas soluciones que (3.3). Pero ahora tenemos que el coeficiente de x_1 es 1, es decir, es un cuadrado, y al menos el coeficiente de x_2 o x_3 es un cuadrado ya que es un producto de dos no cuadrados.

Entonces tomamos la ecuación (3.3) con al menos dos de los coeficientes cuadrados, supongo $\bar{f}_1, \bar{f}_2$ (si no, reordenamos). Entonces existen $r,s \in \mathbb{Z}$ tales que $r^2 = \bar{f}_1, s^2 = \bar{f}_2$. Hacemos el cambio de variable $y_1 = rx_1, y_2 = sx_2, y_3 = x_3$, luego:

$$y_1^2 + y_2^2 = -\bar{f}_3 y_3.$$

Veamos que $\exists y_1, y_2 \in \mathbb{F}_p$ tales que

$$y_1^2 + y_2^2 = -\bar{f}_3$$

de manera que $(y_1, y_2, 1)$ es una solución de la ecuación y así quedará demostrado el lema. En efecto, definimos

$$S = \left\{y_1^2 | y_1 \in \mathbb{F}_p\right\}, T = \left\{-\bar{f}_3 - y_2^2 | y_2 \in \mathbb{F}_p\right\}.$$

Tenemos que

$$|S| = |T| = \frac{p+1}{2} > \frac{p}{2},$$

luego S y T tienen intersección no vacía. Es decir, existen $y_1, y_2 \in \mathbb{F}_p$ tales que

$$y_1^2 = -\bar{f}_3 - y_2^2 \Rightarrow y_1^2 + y_2^2 = -\bar{f}_3.$$

□

La siguiente proposición, nos afirma que para la mayoría de los cuerpos p-ádicos existe solución $(x_1, x_2, x_3) \in \mathbb{Q}_p$ para la forma cuadrática.

Proposición 3.1. *Sea una forma cuadrática de la forma (3.2). Entonces la ecuación*

$$f(x_1,x_2,x_3)=0$$

tiene solución en $\mathbb{Q}_p$ para todo primo p tal que $p \nmid f_1f_2f_3$.

Demostración. Es consecuencia de (3.3) y de (2.4) (que como hemos comentado se puede generalizar a n variables). □

Para concluir con esta sección, observamos que la existencia de soluciones en $\mathbb{R}$ para $f(x_1,x_2,x_3)$ con f como en (3.2) se decide fácilmente. Aun así, este criterio no será necesario en la demostración del Teorema de Hasse-Minkowski.

Observación 3.1. *(3.2) tiene soluciones en $\mathbb{R}$ si y solo si los coeficientes f_1, f_2 y f_3 no son todos del mismo signo.*

3.2.2. Condiciones en los coeficientes derivadas de la solubilidad local

A lo largo de esta sección vamos a suponer que la cónica de la forma (3.2) tiene soluciones en $\mathbb{Q}_p$, para todo p primo y $p=\infty$.

Como indicamos en el capítulo anterior, la siguiente parte de la demostración consiste en usar el hecho de que la cónica tiene soluciones en todas las completaciones de $\mathbb{Q}$ para extraer condiciones sobre los coeficientes de la ecuación.

También de ahora en adelante solo tomaremos el caso de primos p tales que p divide a $f_1f_2f_3$ o $p=2$, ya que hemos visto que en el resto de casos siempre hay solución.

Además podemos suponer que la terna (a_1,a_2,a_3) que es solución cumple que máx $|a_j|_p=1$, es decir los a_j son enteros p-ádicos y en concreto al menos una de las componentes de la solución es una unidad, dado que si no podemos multiplicar la ecuación por el elemento de $\mathbb{Q}_p$ para conseguir esto.

Volvemos a buscar las condiciones sobre los coeficientes. Separamos en los siguientes lemas los casos $p\neq 2$ y $p=2$.

Lema 3.4. *Sea p primo con $p\neq 2$ y $p|f_1f_2f_3$. Si tenemos una forma cuadrática como (3.2) que tiene soluciones en $\mathbb{Q}_p$, entonces existe $r_p\in\mathbb{Z}$ tal que los coeficientes cumplen la ecuación de congruencia:*

$$f_2+r_p^2f_3\equiv 0(\text{ mód }p).$$

Demostración. Suponemos sin pérdida de generalidad que $p|f_1$, luego como los f_i son coprimos entre si p no divide a f_2 ni a f_3. Entonces $|f_1a_1^2|_p<1$ ya que $\text{ord}_p(f_1a_1^2)\geq 1$. Vamos a demostrar por reducción al absurdo que $|a_2|_p=|a_3|_p=1$.
Supongamos que $|a_2|_p<1$, entonces

$$|f_3a_3^2|_p=|f_1a_1^2+f_2a_2^2|_p\leq \text{máx}\left(|f_1a_1^2|_p,|f_2a_2^2|_p\right)<1$$

y como p no divide a f_3 tenemos que $|a_3|_p<1$.
También

$$|f_1a_1^2|_p=|f_2a_2^2+f_3a_3^2|_p\leq \text{máx}\left(|f_2a_2^2|_p,|f_3a_3^2|_p\right)\leq\frac{1}{p^2}.$$

Como f_1 es libre de cuadrados, al menos $p|a_1$, lo que implica que $|a_1|_p<1$ lo que es una contradicción. De manera análoga con a_3, luego $|a_2|_p=|a_3|_p=1$. Entonces tenemos que:

$$|f_2a_2^2+f_3a_3^2|_p<1$$

y dividiendo este por a_2 que sabemos que es una unidad, tenemos que existe $r_p\in\mathbb{Z}$ tal que

$$f_2+r_p^2f_3\equiv 0(\text{ mód }p).$$

□

Ahora vamos a ver el caso $p = 2$.

Lema 3.5. *Sea ahora $p = 2$. Si tenemos una forma cuadrática como (3.2), con solución en $\mathbb{Q}_2$, entonces:*

1. *Si $2 \nmid f_1 f_2 f_3$ entonces se cumple la ecuación de congruencia:*

$$f_2 + f_3 \equiv 0 (\text{ mód } 4).$$

2. *Si $2 | f_1 f_2 f_3$ entonces se cumple la ecuación de congruencia:*

$$s^2 f_1 + f_2 + f_3 \equiv 0 (\text{ mód } 8)$$

con $s = 0$ o 1.

Demostración.

1. Si $2 \nmid f_1 f_2 f_3$ es fácil comprobar que dos de los a_i son pares y uno impar. Ya que la congruencia

$$f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2 \equiv 0 (\text{ mód } 2)$$

es imposible si los tres son impares o si solo uno es par.

Luego tenemos que dos de los a_j son unidades, suponemos sin pérdida de generalidad que son a_2 y a_3. Como (a_1, a_2, a_3) es una solución de la ecuación, tenemos también la ecuación de congruencia:

$$f_1 a_1^2 + f_2 a_2^2 + f_3 a_3^2 \equiv 0 (\text{ mód } 4).$$

Por otro lado, para $a \in \mathbb{Z}$:

- Si a es par, entonces $a = 2n$ con $n \in \mathbb{Z}$, luego $a^2 = 4n^2 \equiv 0 (\text{ mód } 4)$.
- Si a es impar, entonces $a = 2n + 1$ con $n \in \mathbb{Z}$, luego $a^2 = 4n^2 + 4n + 1 \equiv 1 (\text{ mód } 4)$.

Luego como a_1 es par y a_2 y a_3 impares, tenemos que la ecuación de congruencia queda:

$$f_2 + f_3 \equiv 0 (\text{ mód } 4).$$

2. Si $2 | f_1 f_2 f_3$, supongamos sin pérdida de generalidad que $2 | f_1$. De nuevo podemos comprobar que $|a_2|_2 = |a_3|_2 = 1$. Como (a_1, a_2, a_3) es una solución de la ecuación, tenemos también la ecuación de congruencia:

$$f_1 a_1^2 + f_2 a_2^2 + f_3 a_3^2 \equiv 0 (\text{ mód } 8).$$

Además, si tenemos b impar, este número cumple que $b^2 \equiv 1 (\text{mód } 8)$ (si $b = 2n + 1$, entonces $b^2 = 4n^2 + 4n + 1 = 4n(n + 1) + 1 \equiv 1 (\text{ mód } 8)$), luego

$$a_2^2 \equiv 1 (\text{ mód } 8) \text{ y } a_3^2 \equiv 1 (\text{ mód } 8).$$

Entonces la ecuación anterior queda:

$$f_1 a_1^2 + f_2 + f_3 \equiv 0 (\text{ mód } 8).$$

Por otro lado, tenemos que a_1 puede ser par o impar, veamos qué ocurre en cada caso:

- a_1 par, entonces $a_1 = 2n$ para algún n entonces $a_n^2 = 4n^2$ y como f_1 par, esto implica que $f_1 a_1^2 \equiv 0 (\text{ mód } 8)$.
- a_1 impar, entonces ya hemos comprobado que $a_1^2 \equiv 1 (\text{ mód } 8)$ luego $f_1 a_1^2 \equiv f_1 (\text{ mód } 8)$.

Y con todo esto tenemos que la ecuación de congruencia anterior nos queda que:

$$sf_1 + f_2 + f_3 \equiv 0(\text{ mód } 8)$$

con $s = 0$ o 1.

□

En resumen, acabamos de demostrar que si nuestra ecuación tiene soluciones en $\mathbb{Q}_p$ para todo p primo, los coeficientes cumplen ciertas condiciones, que son :

- Si p primo, $p \neq 2$, $p|f_1f_2f_3$, entonces existe $r_p \in \mathbb{Z}$ tal que $f_2 + r_p^2 f_3 \equiv 0(\text{ mód } p)$.
- Si $p = 2$, $p \not| f_1f_2f_3$, entonces $f_2 + f_3 \equiv 0(\text{ mód } 4)$.
- Si $p = 2$, $p|f_1f_2f_3$, entonces $sf_1 + f_2 + f_3 \equiv 0(\text{ mód } 8)$ con $s = 0$ o 1.

3.2.3. Buscando soluciones enteras

El siguiente paso consiste en tomando una cónica como (3.2) y suponiendo que cumple las condiciones obtenidas en (3.2.2), ver que existe un subconjunto Λ de $\mathbb{Z}^3$ cuyos elementos son soluciones de la cónica. De nuevo vamos a separar el caso $p \neq 2$ y $p = 2$ ya que nos han dado condiciones diferentes.

Lema 3.6. *Sea p primo, $p \neq 2$ y $p|f_1f_2f_3$. Sea una forma cuadrática como en (3.2), y supongamos que existe $r_p \in \mathbb{Z}$ tal que los coeficientes cumplen la ecuación de congruencia:*

$$f_2 + r_p^2 f_3 \equiv 0(\text{ mód } p).$$

Entonces $\forall x = (x_1, x_2, x_3) \in \mathbb{Z}^3$ tal que $x_3 \equiv r_p x_2(\text{ mód } p)$ tenemos que

$$F(x) \equiv 0(\text{ mód } p).$$

Demostración. Supongamos sin pérdida de generalidad que $p|f_1$, y supongamos que existe $r_p \in \mathbb{Z}$ tal que los coeficientes cumplen la ecuación de congruencia:

$$f_2 + r_p^2 f_3 \equiv 0(\text{ mód } p).$$

Si (x_1, x_2, x_3) cumple que

$$x_3 \equiv r_p x_2(\text{ mód } p),$$

tenemos que

$$F(x) = f_1x_1^2 + f_2x_2^2 + f_3x_3^2 \equiv (f_2 + r_p^2 f_3)x_2^2 \equiv 0(\text{ mód } p).$$

□

Lema 3.7. *Sea $p = 2$. Si tenemos una forma cuadrática como (3.2):*

1. *Si $2 \not| f_1f_2f_3$ y se cumple la ecuación de congruencia:*

$$f_2 + f_3 \equiv 0(\text{ mód } 4),$$

entonces $\forall x = (x_1, x_2, x_3) \in \mathbb{Z}^3$ tal que $x_1 \equiv 0(\text{ mód } 2), x_2 \equiv x_3(\text{ mód } 2)$ tenemos que

$$F(x) \equiv 0(\text{ mód } 4).$$

2. *Si $2|f_1f_2f_3$ y se cumple la ecuación de congruencia:*

$$s^2 f_1 + f_2 + f_3 \equiv 0(\text{ mód } 8)$$

con $s = 0$ o 1, entonces $\forall x = (x_1, x_2, x_3) \in \mathbb{Z}^3$ tal que $x_1 \equiv 0(\text{ mód } 2), x_2 \equiv x_3(\text{ mód } 4)$ tenemos que

$$F(x) \equiv 0(\text{ mód } 4).$$

Demostración.

1. Supongamos $2 \not| f_1 f_2 f_3$. Si
$$f_2 + f_3 \equiv 0 (\text{ mód } 4),$$
y (x_1, x_2, x_3) cumple que:
$$\begin{cases} x_1 \equiv 0 (\text{ mód } 2), \\ x_2 \equiv x_3 (\text{ mód } 2), \end{cases}$$
entonces
$$F(x) = f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2 \equiv f_2 x_2^2 + f_3 x_3^2 \equiv 0 (\text{ mód } 4).$$

2. Supongamos $2 | f_1 f_2 f_3$ y sin pérdida de generalidad $2 | f_1$. Si
$$s^2 f_1 + f_2 + f_3 \equiv 0 (\text{ mód } 8)$$
con $s = 0$ o 1 y (x_1, x_2, x_3) cumple que:
$$\begin{cases} x_1 \equiv 0 (\text{ mód } 2), \\ x_2 \equiv x_3 (\text{ mód } 4), \end{cases}$$
entonces
$$F(x) = f_1 x_1^2 + f_2 x_2^2 + f_3 x_3^2 \equiv f_2 x_2^2 + f_3 x_3^2 \equiv 0 (\text{ mód } 4).$$

□

En vista de las condiciones de los últimos lemas, definimos un subconjunto Λ de $\mathbb{Z}^3$ de la siguiente manera. El subconjunto $\Lambda \subseteq \mathbb{Z}^3$ viene dado por el conjunto de puntos $(x_1, x_2, x_3) \in \mathbb{Z}^3$ que cumplen la siguiente lista de congruencias:

- Si $p \neq 2$ es primo, $p | f_1 f_2 f_3$, entonces $x_3 \equiv r_p x_2 (\text{ mód } p)$.
- Si $2 \not| f_1 f_2 f_3$, entonces $x_1 \equiv 0 (\text{ mód } 2), x_2 \equiv x_3 (\text{ mód } 2)$.
- Si $2 | f_1 f_2 f_3$, entonces $x_1 \equiv 0 (\text{ mód } 2), x_2 \equiv x_3 (\text{ mód } 4)$.

Vamos a demostrar que el subconjunto Λ de $\mathbb{Z}^3$ tiene estructura de subgrupo junto con la operación suma. Recordamos primero la definición de subgrupo.

Definición. Sea $(G, +)$ un grupo y H un subconjunto $H \subset G$. $(H, +)$ se llama **subgrupo** de $(G, +)$ si y solo si:

- H contiene el elemento identidad de G: $e \in H$.
- H es cerrado para $+$: $\forall a, b \in H \Rightarrow a + b \in H$.
- H es cerrado para opuesto: $\forall a \in H \Rightarrow -a \in H$.

Ahora vamos a demostrar que Λ tiene estructura de subgrupo de $\mathbb{Z}^3$.

Proposición 3.2. *Sea el subconjunto Λ como lo hemos definido antes. Entonces $(\Lambda, +)$ tiene estructura de subgrupo de $(\mathbb{Z}^3, +)$.*

Demostración. Dado $x = (x_1, x_2, x_3)$ en $\mathbb{Z}^3$, las condiciones que determinan si x pertenece a Λ o no son congruencias lineales en x_1, x_2, x_3. Entonces las condiciones de ser subgrupo se cumplen trivialmente. Es decir $(\Lambda, +)$ tiene estructura de subgrupo de $(\mathbb{Z}^3, +)$. □

Y para terminar con este capítulo, vamos a calcular el índice del subgrupo Λ, que luego nos será necesario. Solo vamos a calcular el caso $2 \not| f_1 f_2 f_3$. Para ello vamos a utilizar el Primer Teorema de Isomorfía:

Teorema 3.8. *(Primer teorema de Isomorfía) Si F, G son grupos y $f : G \to F$ es un homomorfismo, con* $\mathrm{Ker}(f) = K$ *entonces* $G/K \cong \mathrm{Im}(f)$.

Definimos la aplicación

$$\begin{array}{rccc} f: & \mathbb{Z}^3 & \to & \left(\prod_{p|f_1f_2f_3,primo} \mathbb{Z}/p\mathbb{Z}\right) \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ & (x_1,x_2,x_3) & \mapsto & (x_3 - r_p x_2, x_1, x_2 - x_3), \end{array}$$

la cual es un homomorfismo de grupos, y además es sobreyectiva. Tenemos que $\Lambda = \mathrm{Ker}(f)$. Aplicando (3.8) tenemos que $\mathbb{Z}^3/\Lambda \cong \mathrm{Im}(f)$. Luego el índice de Λ en $\mathbb{Z}^3$ es $m = |\mathbb{Z}^3/\Lambda| = 4|f_1f_2f_3|$.

3.2.4. Conclusión de la demostración

Para esta sección final del capítulo, hemos tomado como referencia [2, cap.4].

La última parte de esta demostración, es sabiendo que la ecuación tiene soluciones módulo p para todo p primo, concluir que en particular la tiene para algún (x_1,x_2,x_3) en ese subgrupo Λ que hemos definido.

Recordamos que el índice de Λ en $\mathbb{Z}^3$ es $m = 4|f_1f_2f_3|$. Aplicando el Teorema Chino de los Restos tenemos que

$$f(x_1,x_2,x_3) \equiv 0 (\,\mathrm{mód}\, 4|f_1f_2f_3|), \quad \forall x \in \Lambda.$$

Para terminar la demostración necesitamos un teorema que vamos a demostrar más adelante para no romper el hilo de la demostración, pero que enunciamos ahora:

Teorema 3.9. *Sea Λ un subgrupo de $\mathbb{Z}^n$ de índice m. Sea $\mathscr{C} \subset \mathbb{R}^n$ un conjunto simétrico y convexo de volumen $V(\mathscr{C}) > 2^n m$. Entonces $\mathscr{C}$ y Λ tienen algún punto común distinto del* 0.

Ahora definimos el conjunto convexo y simétrico dado por:

$$\mathscr{C} = \left\{(x_1,x_2,x_3) \in \mathbb{Z}^3 \,||f_1|x_1^2 + |f_2|x_2^2 + |f_3|x_3^2 < 4|f_1f_2f_3|\right\},$$

$\mathscr{C}$ define un elipsoide, luego su volumen es

$$V(\mathscr{C}) = \frac{\pi}{3} 2^3 4|f_1f_2f_3| > 2^3 4|f_1f_2f_3|.$$

Luego aplicando (3.9) tenemos que $\exists\, x \in \Lambda \cap \mathscr{C}$ con $x \neq 0$ tal que

1. $F(x_1,x_2,x_3) \equiv 0 (\,\mathrm{mód}\, 4|f_1f_2f_3|)$, ya que $x \in \Lambda$;
2. $|F(x_1,x_2,x_3)| = |f_1x_1^2 + f_2x_2^2 + f_3x_3^2| \leq |f_1|x_1^2 + |f_2|x_2^2 + |f_3|x_3^2 < 4|f_1f_2f_3|$, ya que $x \in \mathscr{C}$.

Entonces tenemos que la única opción es que:

$$F(x_1,x_2,x_3) = 0$$

tal y como queríamos demostrar.

Ahora que ya hemos terminado con la demostración del Teorema, vamos a proceder a demostrar (3.9). Para ello, vamos a enunciar un lema necesario:

Lema 3.10. *Sea $m > 0$ un entero y $\mathscr{S} \subset \mathbb{R}^n$ con $V(\mathscr{S}) > m$. Entonces hay $m+1$ puntos distintos $s_0, \ldots, s_m$ de $\mathscr{S}$ tales que $s_i - s_j \in \mathbb{Z}^n, (0 \leq j \leq m)$.*

Demostración. Definimos $\mathscr{W} \subset \mathbf{R}^n$ como el cubo de lado 1 cuyos puntos $(w_1, \ldots, w_n)$ cumplen:

$$0 \leq w_j < 1 \quad (1 \leq j \leq n).$$

Luego todo $\mathbf{x} \in \mathbf{R^n}$ se escribe de manera única como

$$\mathbf{x} = \mathbf{w} + \mathbf{z}, \text{ con } \mathbf{w} \in \mathscr{W}, \mathbf{z} \in \mathbb{Z}^n.$$

Sea $\psi(\mathbf{x})$ la función característica de $\mathscr{S}$, entonces

$$\begin{aligned} m < V(\mathscr{S}) &= \int_{\mathbf{R}^n} \psi(\mathbf{x}) d\mathbf{x} \\ &= \int_W \left(\sum_{\mathbf{z} \in \mathbf{Z}^n} \psi(\mathbf{w}+\mathbf{z}) \right) d\mathbf{w}. \end{aligned}$$

Como $V(\mathscr{W}) = 1$, existe algún $\mathbf{w}_0 \in \mathscr{W}$ tal que

$$\sum_{\mathbf{x} \in \mathbf{Z}^n} \psi(\mathbf{w}_0 + \mathbf{z}) > m \geq m+1.$$

□

Entonces ahora ya podemos demostrar (3.9)

Demostración. Definimos $S = \frac{1}{2}\mathscr{C}$ como el conjunto de puntos de $\mathscr{C}$ de la forma $\frac{1}{2}c, c \in \mathscr{C}$. El volumen de este subconjunto es:

$$V\left(\frac{1}{2}\mathscr{C}\right) = 2^{-n} V(\mathscr{C}) > m.$$

Por el lema anterior tenemos que van a existir $\mathbf{c}_0, \ldots, \mathbf{c}_m \in \mathscr{C}$ todos ellos diferentes, tales que:

$$\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_j \in \mathbf{Z}^n \quad (0 \leq i, j \leq m).$$

Luego hay $m+1$ puntos

$$\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_0 \quad (0 \leq i \leq m)$$

y m clases de $\mathbf{Z}^n$ modulo Λ.

Luego por el Principio del Palomar, al menos dos tienen que estar en la misma clase, es decir existen i, j con $i \neq j$ tales que

$$\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_j \in \Lambda$$

y como hemos dicho que el subconjunto es simétrico $-\mathbf{c}_j \in \mathscr{C}$, y como también es convexo tenemos que:

$$\frac{1}{2}\mathbf{c}_i - \frac{1}{2}\mathbf{c}_j = \frac{1}{2}\mathbf{c}_i + \frac{1}{2}(-\mathbf{c}_j) \in \mathscr{C}.$$

□

Capítulo 4

Ecuaciones de grado superior

En este último capítulo del trabajo, nuestra principal referencia ha sido [2, cap.18]. En este capítulo vamos a presentar dos ejemplos de ecuaciones de grado mayor que 2 para las cuales el principio local-global del que nos habla el Teorema de Hasse-Minkowski no se cumple. Esto muestra que el teorema no vale para ecuaciones de grado superior a 2.

El primer caso se trata de una forma cúbica:

$$3x^3 + 4y^3 + 5z^3 = 0. \tag{4.1}$$

Vamos a enunciar y demostrar un lema, que nos va a ser necesario para demostrar que esta ecuación no tiene soluciones racionales.

Lema 4.1. *Sean $a,b,c > 1$ con $a \neq b \neq c$. Suponemos que $d = abc$ es libre de cuadrados y que $\exists u,v,w \in \mathbb{Z}$ con al menos uno no nulo tales que cumplen la ecuación $au^3 + bv^3 + cw^3 = 0$. Entonces existen $x,y,z \in \mathbb{Z}$ con $z \neq 0$ tales que $x^3 + y^3 + dz^3 = 0$.*

Demostración. Se $\rho^3 = 1, \rho \neq 1$, y definimos también

$$\xi = au^3 + b\rho v^3 + \rho^2 cw^3,$$

$$\eta = au^3 + \rho^2 bv^3 + \rho cw^3.$$

Entonces sumando estos términos obtenemos

$$\xi + \eta = 3au^3$$

y

$$\rho\xi + \rho^2\eta = 3cw^3,$$

$$\rho^2\xi + \rho\eta = 3bw^3.$$

Luego

$$\xi^3 + \eta^3 + d\zeta = 0, \quad \zeta = -3uvw.$$

Entonces los puntos $(\xi, \rho\eta, \zeta)$ y $\left(\eta, \rho^2\xi, \zeta\right)$ son conjugados sobre $\mathbb{Q}$. Entonces la línea que los une coincide con

$$x^3 + y^3 + dz^3 = 0$$

en un punto sobre $\mathbb{R}$ distinto de $(1,-1,0)$. □

Luego con este lema, sabemos que si (4.1) tuviese soluciones, entonces la ecuación:

$$x^3 + y^3 + 60z^3 = 0, \tag{4.2}$$

tendría solución con $z \neq 0$. Pero en [2, p.86], se dan argumentos para ver que las únicas soluciones de (4.2) son de la forma $(a,-a,0)$. Es decir con $z = 0$, lo que contradice lo que habíamos demostrado en

(4.1). Por lo que tenemos que (4.1) no tiene ninguna solución racional.

Nuestro segundo ejemplo se trata de una ecuación de grado 4:

$$x^4 - 17 = 2y^2 \tag{4.3}$$

Supongamos que tiene solución, (x,y). Escribimos $x = \frac{a}{c}$ fracción irreducible. Entonces

$$a^4 = 17c^4 = 2b^2, \quad \text{mcd}(a,c) = \text{mcd}(b,c) = \text{mcd}(a,b) = 1.$$

Ponemos

$$A = a^2, \quad C = c^2,$$

la ecuación nos queda:

$$A^2 - 17C^2 = 2b^2.$$

Se trata de una forma cuadrática como las que hemos tratado a lo largo de todo el trabajo, luego es soluble localmente en todo primo si y solo si es soluble globalmente. De hecho $(5,1,2)$ es solución.

Por otro lado,

$$(5A + 17C + 4b)(5A + 17C - 4b) = 17(A + 5C)^2.$$

Si nos fijamos en la parte derecha de esta igualdad, si los dos múltiplos tuviesen algún divisor primo par común, entonces este divide a $(5A + 17C)$ y a $(A + 5C)$, luego divide a $8A$ y a $8C$, lo que es una contradicción ya que a y c son coprimos.

En función de dos enteros u y v vamos a ver cuales son las posibilidades:

- En el primer caso, si $A + 5C = uv \Rightarrow 5a^2 + 17c^2 \pm 4b = 17u^2, 5a^2 + 17c^2 \mp 4b = v^2$. Entonces

  $$10a^2 + 34c^2 = 17u^2 + v^2,$$

  $$a^2 + 5c^2 = uv.$$

  Pero si buscamos a esto solución módulo 17,

  $$10a^2 \equiv v^2 (\text{ mód } 17),$$

  luego

  $$\left(\frac{a}{v}\right)^2 \equiv 10 (\text{mod}).$$

  Pero en el cuerpo $\mathbb{F}_{17}$, se puede comprobar que 10 no es un cuadrado, luego esto es imposible. Entonces esta ecuación no tiene solución módulo 17, por lo tanto no tiene solución racional.

- En el segundo caso, si $A + 5C = 2uv \Rightarrow 5a^2 + 17c^2 \pm 4b = 34u^2, 5a^2 + 17c^2 \mp 4b = 2v^2$. Que con un razonamiento análogo al primer caso, puedo demostrar que tampoco hay solución racional.

En conclusión hemos demostrado que tanto (4.1) y (4.3) no tienen solución en $\mathbb{Q}$. Sin embargo se puede demostrar que sí tienen soluciones en todas sus completaciones (véase [2, cap.18]). Luego esto muestra que el Teorema de Hasse-Minkowski no se cumple para ecuaciones de grado superior a 2.

Bibliografía

[1] N. KOBLITZ, *p-adic numbers, p-adic analysis, and zeta functions.* Graduate Texts in Mathematics, Vol. 58, Springer (1977).

[2] J. W. S. CASSELS, *Lectures on elliptic curves.* London Mathematical Society Student Texts, Vol. 24, Cambridge University Press (1991).

[3] J.-P. SERRE, *A course in arithmetic.* Graduate Texts in Mathematics, Vol. 7, Springer (1973).

[4] K. IRELAND Y M. ROSEN, *A Classical Introduction to Modern Number Theory.* Graduate Texts in Mathematics, Vol. 84, Springer (1982).