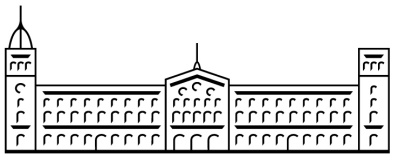

**Trabajo final de Grado**

**GRAU DE MATEMÀTIQUES**

**Facultat de Matemàtiques**
**Universitat de Barcelona**

# El problema de Erdös y Ulam

**Autor: Borja Sánchez López**

**Director:** Dr. Vicenç Navarro Aznar
**Realitzat a:** Departament d'Àlgebra i Geometria

**Barcelona,** 30 de junio de 2015

# Abstract

Paul Erdös, in the first half of last century, asked about finite integer sets in the plane in general position. This means, finite many points sets of the plane, with no 3 points on a line, nor 4 on a circle, with integer distances between any 2 points of the set. One can easily find a 3 points set where all distances between those points are integers. However, the problem becomes harder to solve when we try to find greater finite integer sets in general position. We will see some constructions of these sets of $n$ points, being $n < 8$. Nowadays, we know some 7 points integer sets in general position, but we have not found an example of an 8 points set that satisfies the conditions.

Stanislaw Ulam studied the infinite version of the problem and conjectured that there is no everywhere dense rational set in the plane. Till today, this problem has been addressed by studying the set of rational points on algebraic curves, achieving the main results from the Mordell's Theorem and the Faltings' Theorem.



# Resumen

Paul Erdös preguntó, en la primera mitad del siglo pasado, acerca de la existencia de conjuntos del plano, finitos y enteros, en posición general. Es decir, conjuntos con un número finito de puntos del plano, sin haber 3 en una recta ni 4 en una circunferencia, con distancias enteras entre 2 puntos cualquiera del conjunto. Se pueden hallar fácilmente conjuntos de 3 puntos que restan a distancias enteras, sin embargo, el problema se complica en cuanto aumentamos la cantidad de puntos. Veremos construcciones de este tipo de conjuntos de $n$ puntos, para $n < 8$. Hoy en día se conocen conjuntos enteros de 7 puntos del plano en posición general, pero el problema sigue abierto para conjuntos con 8 o más puntos.

Stanislaw Ulam estudió el caso infinito del problema y conjeturó que no existe ningún conjunto racional denso en el plano. Hasta hoy, se ha avanzado en el problema gracias al estudio de los puntos racionales sobre las curvas algebraicas, obteniendo resultados intereseantes a partir de profundos teoremas como son el Teorema de Mordell y el Teorema de Faltings.

# Agradecimientos

Como siempre, y en todo lo que logre, doy las gracias a la madre que me parió y a mi hermana. Por escuchar mis divagaciones a menudo cargantes sobre temas de este trabajo, por sus ánimos y por su apoyo incondicional. Gracias mamá, y gracias bichito.

A Vicenç Navarro, tutor de este trabajo, le debo la gran idea del tema escogido. He disfrutado aprendiendo. Agradezco sus consejos y guía, con los que he podido volver al camino cuando me perdía.

Quiero valorar también la ayuda de Jordi y Patrícia, haciendo lecturas previas del trabajo y aportando un ejemplo al anexo B., gracias.

# Sumario

# Presentación

## El Problema de Erdös

Representar dos puntos en el plano con distancia racional es una tarea trivial. Al dibujar tres puntos en el plano, con distancias racionales entre ellos y sin estar alineados, tampoco nos encontramos con demasiados problemas, pues no es nada que un compás no nos permita lograr. El nivel de dificultad aumenta cuando queremos añadir un cuarto punto, sin que caiga en la única circunferencia generada por los 3 puntos anteriores, ni esté alineado con 2 de los puntos dibujados previamente. Nos es de gran ayuda, darnos cuenta de que cualquier conjunto con un número finito de puntos y con distancias racionales entre los puntos del conjunto puede aumentarse hasta que dichas distancias sean enteras. Claramente, el aumento comentado corresponde a una homotecia que especificaremos en otro momento. Por ello, nuestra búsqueda puede simplificarse a buscar conjuntos con distancias enteras entre los puntos del conjunto. Si todas las distancias entre los puntos de un conjunto finito son enteras, y además, no hay 3 puntos alineados ni 4 en una circunferencia, diremos simplemente que es un conjunto entero.

*El Problema de Erdös* pregunta sobre la existencia de conjuntos enteros de $n$ puntos del plano. Hasta el día de hoy, se ha mostrado ejemplos de conjuntos enteros de $n$ puntos del plano hasta llegar a 7 puntos hace apenas una década. Incluso se han llegado a dar miles de ejemplos distintos de estos conjuntos para $n = 7$, pero sin embargo, el problema sigue resistiéndose para valores de $n$ superiores.

Cualquier conjunto entero de $n$ puntos contiene trivialmente conjuntos enteros de $m$ puntos con $m < n$. Es más, cualquier conjunto entero de $n$ puntos puede considerarse como la adhesión unívoca por almenos tres puntos, de dos conjuntos enteros de $m_1$ y $m_2$ puntos con $m_1, m_2 < n$. Por ello, si nos es posible, es interesante estudiar la cantidad de conjuntos enteros de $m$ puntos con $m < n$, sin conformarnos simplemente con su existencia. Está a nuestro alcance caracterizar todos los triángulos con lados enteros según, por ejemplo, uno de sus ángulos, o también por su diámetro, concepto que veremos más adelante. Veremos también un modo de dar infinitos conjuntos enteros de 4 puntos, y la importancia de este método para la construcción de los $n$-clusters, que también definiremos.

## El Problema de Ulam

Supongamos lo siguiente: partimos de un conjunto que tiene un solo punto del plano $(x_0, y_0)$. Decidimos añadir otro punto cualquiera $(x_1, y_1)$ que esté a distancia racional de $(x_0, y_0)$. Ahora otro punto $(x_2, y_2)$ que esté a distancia racional de los dos anteriores. Siguiendo el proceso, seguimos sumándole más puntos del plano $(x_n, y_n)$ de manera que su distancia a $(x_i, y_i)$ para todo $i < n$ sea racional, y si es posible, seguimos hasta tener infinitos puntos en nuestro conjunto. Llamaremos conjunto racional a un subconjunto del plano con distancias racionales entre los puntos del conjunto. ¿Qué formas puede llegar a tomar un conjunto racional infinito?

*El Problema de Ulam*, concretamente, niega la existencia de un conjunto racional denso en el plano. Lo cierto es que ni siquiera es sencillo proponer ejemplos de conjuntos racionales infinitos que no caigan casi enteramente sobre rectas o circunferencias.

Los puntos racionales sobre las curvas algebraicas, que estudiaremos en este trabajo, nos permitirán responder a ciertas preguntas relacionadas con la distribución en el plano de los puntos de un conjunto racional infinito. Aunque todavía no estemos preparados para dar una solución a este problema, se ha llegado a restringir considerablemente la forma que debiera tomar un conjunto racional denso en el plano, en el caso que existiese uno.

Vamos a necesitar algunos conceptos básicos de las curvas algebraicas, que podemos encontrar en el capítulo 1 con una breve introducción a las curvas algebraicas.

En el capítulo 2 hacemos una búsqueda de los puntos racionales sobre las curvas algebraicas, empezando por las curvas racionales o cónicas (de género 0), continuando con las curvas cúbicas (de género 1) y terminando con las curvas de género $g > 1$. En especial, remarcamos los teoremas de Mordell y Faltings.

Afrontamos *El Problema de Erdös* en el capítulo 3, donde vemos herramientas y métodos usados hoy en día para encontrar conjuntos enteros con la ayuda de ordenadores. Definimos el diámetro de un conjunto entero, nos familiarizamos con los triángulos Heronianos y tratamos de generar los $n$-clusters.

El capítulo 4 está dedicado a *El Problema de Ulam*. Comenzamos viendo los subconjuntos racionales densos de la recta y la circunferencia. Después, vemos varios potentes teoremas que relacionan los puntos racionales sobre curvas algebraicas y los conjuntos racionales, que demostramos gracias a los teoremas de Mordell y Faltings vistos en el capítulo 2.

# 1. Introducción a las curvas algebraicas

En este capítulo, empezaremos dando varias definiciones, propiedades y herramientas relacionadas con las curvas algebraicas que nos van a ser de utilidad durante las secciones posteriores. Si bien se puede decir que daremos una introducción a las curvas algebraicas, puesto que tan solo vamos a dar los conceptos que nos interesan para este trabajo, se podrían echar en falta algunos aspectos básicos de las curvas algebraicas de las que haremos omisión, y asimismo, se podrían considerar no adecuados algunos otros un tanto más específicos. Conceptos básicos de curvas algebraicas y geometría algebraica pueden encontrarse en [2] o [12].

**Definición 1.0.0.1.** Una *variedad algebraica* sobre $\mathbb{Q}$ del espacio proyectivo $\mathbb{P}^n_{\mathbb{C}}$ es el conjunto de puntos $V \subset \mathbb{P}^n_{\mathbb{C}}$ tal que todo punto de $V$ anula un conjunto $S$ de funciones polinómicas homogéneas sobre $\mathbb{Q}$ en $n+1$ variables. Es decir;

$$V = \{p = [x_0, ..., x_n] \in \mathbb{P}^n_{\mathbb{C}} \mid F(p) = 0 \ \forall F \in S \subset \mathbb{Q}[x_0, ..., x_n]\}$$

**Definición 1.0.0.2.** Una *variedad algebraica* sobre $\mathbb{Q}$ del espacio afín $\mathbb{A}^n_{\mathbb{C}}$ es el conjunto de puntos $U \subset \mathbb{A}^n_{\mathbb{C}}$ tal que todo punto de $U$ anula un conjunto $T$ de funciones polinómicas sobre $\mathbb{Q}$ en $n$ variables. Es decir;

$$U = \{p = (x_1, ..., x_n) \in \mathbb{A}^n_{\mathbb{C}} \mid f(p) = 0 \ \forall f \in T \subset \mathbb{Q}[x_1, ..., x_n]\}$$

**Definición 1.0.0.3.** Sea $V$ una variedad algebraica proyectiva definida a partir del conjunto de funciones polinómicas homogéneas $S = \{F_1(x_0, ...x_n), ..., F_m(x_0, ..., x_n)\}$. Definimos la *dimensión* $d$ de la variedad $V$ en el espacio proyectivo $P^n_{\mathbb{C}}$ como $d = n - m$ donde $m$ es el número de funciones independientes de $S$.

**Definición 1.0.0.4.** Sea $U$ una variedad algebraica afín definida a partir del conjunto de funciones polinómicas $T = \{f_1(x_1, ...x_n), ..., f_m(x_1, ..., x_n)\}$. Definimos la *dimensión* $d$ de la variedad $U$ en el espacio afín $A^n_{\mathbb{C}}$ como $d = n - m$ donde $m$ es el número de funciones independientes de $T$.

**Definición 1.0.0.5.** Una *curva algebraica* es una variedad algebraica de dimensión 1.

Por lo tanto, una curva algebraica $C$ del espacio proyectivo $\mathbb{P}^n_{\mathbb{C}}$ es el conjunto de puntos $[x_0, ..., x_n] \in \mathbb{P}^n_{\mathbb{C}}$ que anulan $n-1$ funciones polinómicas homogéneas independientes en $n+1$ variables. Puesto que nos interesan las curvas algebraicas de $\mathbb{P}^2_{\mathbb{C}}$, éstas están definidas por una sola ecuación $F(x, y, z) = 0$ donde $F(x, y, z)$ es una función polinómica homogénea de 3 variables complejas.

**Notación.** Notaremos simplemente $\mathbb{P}^2$ al espacio $\mathbb{P}^2_{\mathbb{C}}$.

También podemos hablar de las curvas algebraicas en $\mathbb{A}^2_{\mathbb{C}}$. Éstas, en consecuencia, vienen definidas por una ecuación $f(x, y) = 0$ donde $f$ es una función polinómica de 2 variables complejas.

**Notación.** Notaremos simplemente $\mathbb{A}^2$ al espacio $\mathbb{A}^2_{\mathbb{C}}$.

La dimensión de una curva algebraica, por definición, es 1 sobre los complejos. No obstante, puesto que $\dim_{\mathbb{R}} \mathbb{C} = 2$, la misma curva puede considerarse una superficie ( dimensión 2 ) como variedad real. De hecho, a las curvas algebraicas de $\mathbb{A}^n_{\mathbb{C}}$ se las conoce comúnmente como superficies de Riemann. Por lo general, estas superficies están sumergidas en $\mathbb{R}^{2n}$, $n \geq 2$, por lo que resulta complicado o imposible dibujarlas.

Por otro lado, a nosotros nos van a interesar en particular los puntos con coordenadas racionales sobre las curvas alebraicas, que reciben el nombre de puntos racionales. Debido a ello, nos las podemos arreglar para representar gráficamente la parte que nos interesa de la curva. A continuación explicaremos cómo.

**Observación.** Todo punto $p \in \mathbb{P}^2$ racional, puede ser expresado con coordenadas enteras, multiplicando $p$ por el denominador común de sus coordenadas racionales.

## 1.1. Curvas en el Espacio Proyectivo y Afín

Supongamos ahora, que tenemos una curva algebraica $C$ en $\mathbb{P}^2$ de ecuación $F(x, y, z) = 0$ de grado $d$. Sea $f(x, y) := F(x, y, 1)$, entonces $f(x, y) = 0$ define una curva algebraica $C^*$ en $\mathbb{A}^2$. Además, todo punto entero $p = [a, b, c]$ con $c \neq 0$ que anule a $F$, tomando coordenadas homogéneas, determina un punto racional $p^* = (\frac{a}{c}, \frac{b}{c})$ de la curva algebraica $C^*$ en $\mathbb{A}^2$, pues $0 = F(\frac{a}{c}, \frac{b}{c}, 1) = f(\frac{a}{c}, \frac{b}{c})$. De la misma manera, si hallamos un punto racional $p^* = (\frac{a}{c}, \frac{b}{c})$ de $C^*$, entonces, se comprueva que $c^d f(\frac{a}{c}, \frac{b}{c}) = F(a, b, c) = 0$ donde $F(x, y, z) = 0$ era la ecuación de $C$, por lo que deducimos que $p = [a, b, c]$ es un punto entero de $C$.

En numerosas ocasiones, haremos estas traducciones entre curvas algebraicas de distintos espacios, con la intención de hallar los puntos racionales solución de $f(x, y) = 0$ en $\mathbb{A}^2$, a partir de los puntos enteros solución de $F(x, y, z) := z^d f(\frac{x}{z}, \frac{y}{z})$ en $\mathbb{P}^2$, y viceversa, es decir, encontrar las soluciones enteras de $F(x, y, z)$ (con $z \neq 0$) a partir de las soluciones racionales de $f(x, y) := F(x, y, 1)$.

Las curvas algebraicas de $\mathbb{P}^2$, en ocasiones las interpretaremos sobre $\mathbb{A}^2 \cup \mathbb{P}^1$, es decir, el espacio de los puntos del plano complejo unión con el punto en el infinito para cada dirección. Se puede comprovar que tan solo es una manera distinta de definir el mismo espacio, teniendo en cuenta la siguiente función con inversa;

$$\begin{array}{rcl} \mathbb{P}^2 & \longrightarrow & \mathbb{A}^2 \cup \mathbb{P}^1 \\ \\ [x, y, z] & \longmapsto & \begin{cases} (\frac{x}{z}, \frac{y}{z}) \in \mathbb{A}^2 & si\ z \neq 0 \\ [x, y] \in \mathbb{P}^1 & si\ z = 0 \end{cases} \\ [x, y, 1] & \longmapsto & (x, y) \in \mathbb{A}^2 \\ [x, y, 0] & \longmapsto & [x, y] \in \mathbb{P}^1 \end{array}$$

De hecho, puesto que queremos encontrar los puntos racionales de las curvas algebraicas, podemos restringir el espacio, por lo que nos bastará considerar la

curva en $\mathbb{A}^2_{\mathbb{R}} \cup \mathbb{P}^1$. De este modo, obviando el infinito, incluso podremos dibujar las curvas en el plano real, que en particular contiene todos los puntos racionales.

**Ejemplo.** Sea $C$ una curva algebraica de $\mathbb{P}^2$, con ecuación $F(x, y, z) = 2x^2 - 3yz + 3xy + 3y^2 - 5z^2 = 0$, de la cual queremos conocer, si tiene, sus puntos enteros. Recordemos que la curva puede ser vista en $\mathbb{A}^2 \cup \mathbb{P}^1$. Entonces, primero obviamos los puntos del infinito y hallamos $f(x, y) := F(x, y, 1) = 2x^2 - 3y + 3xy + 3y^2 - 5 = 0$. Los puntos racionales de la nueva curva $C^*$ del plano complejo afín, obtenida a partir de la ecuación $f(x, y) = 0$, nos determina también los puntos enteros en $C$, menos aquellos con $z = 0$. Intersecando ahora con $\mathbb{A}^2_{\mathbb{R}}$, es decir, teniendo en cuenta que $x$ e $y$ son reales, representamos la curva;

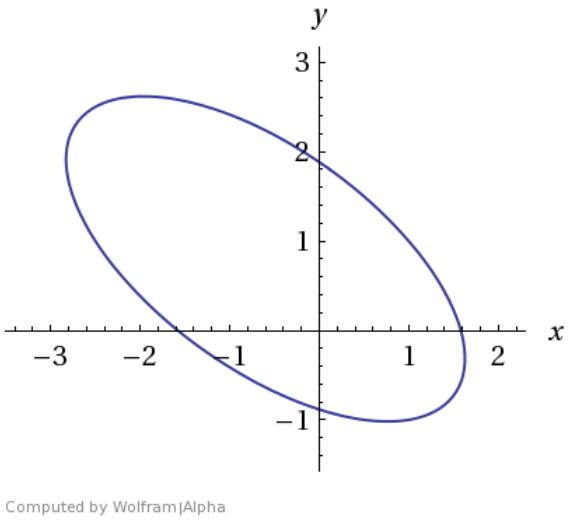


Figura 1: Elipse

que es una elipse. Se comprueva facilmente que el punto $(1, -1)$ pertenece a $C^*$, y por lo tanto $(1, -1, 1)$ es de $C$. Más adelante, veremos un método para determinar con un procedimiento geométrico, todos los puntos racionales de la elipse $C^*$ a partir de uno dado, y de ese modo, todos los puntos enteros de $C$ con $z \neq 0$.

## 1.2. Singularidad

Podemos clasificar los puntos de una curva algebraica entre singulares y no singulares.

**Definición 1.2.0.6.** Dada la funcion polinómica $F(x, y, z)$ que define una curva algebraica $C$ en $\mathbb{P}^2$ ( analogamente para $\mathbb{A}^2$ ), los *puntos singulares* de $C$ son aquellos

puntos $p \in C$ que anulan la Matriz Jacobiana ( matriz de derivadas parciales ). Es decir, $p$ es singular si;

$$DC(p) = \left( \frac{\partial F(x,y,z)}{\partial x}(p), \frac{\partial F(x,y,z)}{\partial y}(p), \frac{\partial F(x,y,z)}{\partial z}(p) \right) = (0,0,0)$$

De lo contrario diremos que el punto $p$ es no singular.

**Definición 1.2.0.7.** Una curva algebraica se dice que es *singular* si existe un punto $p$ singular de la curva. De lo contrario decimos que la curva es no singular.

## 1.3. Género

El género es una propiedad intrínseca de la curva. Esta propiedad se puede dar desde varios puntos de vista (geométrico, topológico, aritmético), cada uno con su propia definición y fórmulas. Como no vamos a hacer un uso práctico de su definición y fórmulas, nos será suficiente saber que el género contribuye a darnos una idea de cuán 'complicada' es una curva. Nos interesa destacar las curvas de género 0 no singulares, resultantes de las ecuaciones $F(x,y,z) = 0$ con $F$ polinomio homogéneo lineal (rectas) o cuadrático (cónicas) y las curvas de género 1 no singulares (curvas elípticas), obtenidas a partir de funciones cúbicas homogéneas. Para dar una idea de la información proporcionada por el género, podemos dar la visión topológica del concepto, ilustrada en las siguientes superficies topológicas;

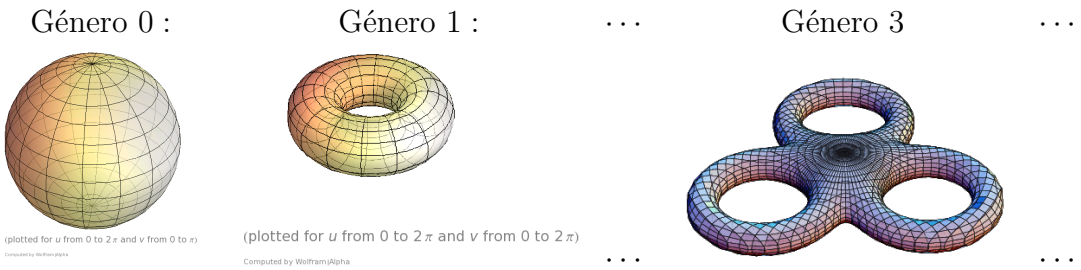


Figura 2: género de superficies topológicas

# 2. Puntos racionales sobre curvas

En esta sección nos disponemos a encontrar los puntos racionales sobre curvas algebraicas, es decir, aquellos puntos de la curva, con coordenadas racionales. Partiremos este trabajo según el género de la curva; empezaremos con las curvas cónicas, seguiremos con las cúbicas, y más concretamente con las curvas elípticas, para terminar con las curvas de género $g > 1$. Para las curvas elítpicas, nos valdremos de *El Teorema de Mordell* [13], del que intentaremos dar algunas herramientas para atisbar una idea de la demostración. Para las curvas de género $g > 1$, formularemos un potente teorema demostrado recientemente en 1983, merecedor de la medalla *Fields*, conocido como *El Teorema de Faltings* [16].

## 2.1. Sobre cónicas

Las cónicas, de manera informal, son el resultado de la intersección entre un cono y un plano que no pase por el vértice del cono. Estas curvas se expresan siempre mediante una ecuación cuadrática, y tenemos 4 tipos: la circunferencia, la elipse, la hipérbola y la parábola. Por lo general, trabajaremos las cónicas y sus puntos racionales en $\mathbb{A}^2$, para después sacar conslusiones sobre los puntos enteros sobre cónicas en $\mathbb{P}^2$.

**Propiedad.** Toda recta de $\mathbb{A}^2$ que interseque a una cónica $C$, interseca 2 veces a $C$ contando multiplicidades.

Esta propiedad nos va a ser fundamental para situar los puntos racionales sobre las cónicas. Sea la cónica $C$ y un punto $P \in C$. Si una recta por $P$ es tangente a la cónica $C$, entonces diremos que interseca dos veces a $C$ en $P$ ( multiplicidad 2).

La técnica que usaremos para hallar los puntos racionales para todas las cónicas es la siguiente: en $\mathbb{A}^2$, dado un punto racional $P = (a, b)$ sobre la cónica, trazáremos una recta de pendiente $t$ por ese punto, que cortará de nuevo nuestra cónica en un único punto $(a_t, b_t)$. Este nuevo punto será racional si y solo si $t$ es racional. Se cumple además, que dado otro punto racional $Q = (c, d)$ sobre la cónica diferente a $P$, existe un único racional $t_Q$ de manera que $Q = (a_{t_Q}, b_{t_Q})$. Es decir, tenemos una correspondencia entre los puntos racionales sobre la cónica y los posibles valores racionales $t$ de la pendiente de la recta. En conclusión, nuestra cónica posee una infinidad de puntos racionales.

Agudamente, uno podría señalar que la construcción anterior solo tiene sentido cuando tenemos de antemano un punto racional $P = (a, b)$ que sea solución de la ecuación de la cónica. En efecto, por eso discutiremos antes la existencia de puntos racionales sobre las cónicas (al menos uno), para concluir que habrán infinitos. De hecho, hay cónicas sin ningún punto racional.

### 2.1.1. Existencia de puntos racionales y el Teorema de Legendre

En general, no es fácil encontrar a ojo una solución racional para la ecuación de una cónica. Es más, no tiene porqué existir una. Demos dos ejemplos, de los cuales el segundo, junto con un estudio más detallado del tema, puede hallarse en [13]:

**Ejemplo.**

$$x^2 - y^2 = 2,$$

que representa una hipérbola. Claramente, no podremos hallar una solución con $x$ e $y$ enteros, puesto que, en el caso en que ni $x$ ni $y$ son nulos, ni $x = y$, la resta de dos cuadrados es siempre superior o igual a 3, y en el resto de casos, se puede comprovar de forma trivial que tampoco hay soluciones.

Supongamos que en cambio, sí que existe una solución racional no trivial $x = \frac{n}{k}$ e $y = \frac{m}{k}$, entonces tenemos que $n^2 - m^2 = 2k^2$ con $n, m, k \in \mathbb{Z}$. Este último argumento, es equivalente al que decíamos, de que para encontrar soluciones racionales a una curva algebraica de $\mathbb{A}^2$, nos es suficiente encontrar las soluciones enteras, con $k \neq 0$, a la ecuación correspondiente en el espacio proyectivo $\mathbb{P}^2$. Es decir, hemos convertido el problema a hallar soluciones enteras para $n^2 - m^2 = 2k^2$.

Podemos suponer que $n \neq 0 \neq m$ y que $n \neq m$ ya que buscamos soluciones no triviales y con $k \neq 0$. Podemos suponer también, que $n, m, k$ son todos coprimos dos a dos, pues, por ejemplo, si hubiese un $t$ tal que $t|n, m$ entonces $t|k$ y podemos dividir la ecuación por $t$ (de hecho, por $t^2$) y cancelar. En especial, $n$ y $m$ no pueden ser los dos pares.

Reduciendo la ecuación módulo 2 , nos damos cuenta de que $n^2 \equiv m^2 \pmod 2$, que por ser 2 un número primo deducimos que $n \equiv m \pmod 2$. Es decir, $n$ y $m$ tienen la misma paridad, y como no podían ser los dos pares, deben ser ambos impares. Podemos reescribir $n^2 - m^2 = (n + m)(n - m)$, y puesto que $2|(n + m), (n - m)$, pues $n$ y $m$ son impares distintos, tenemos $4|(n^2 - m^2) = 2k^2$. Esto nos dice que $2|k$. Reescribimos la ecuación como $(n + m)(n - m) = 2(2k')^2$ donde $2k' = k$. Hemos determinado que tanto $n + m$ como $n - m$ son divisibles por 2. Ahora bien, imponiendo que $4|n - m$ ( respectivamente $n + m$ ), demostramos que $4 \nmid n + m$ ( respectivamente $n - m$ ).

- Si $4|n - m$ entonces $n \equiv m \pmod 4 \Rightarrow n + m \equiv 2m \pmod 4$. Pero dado que $m$ es impar, $2m \equiv 2 \not\equiv 0 \pmod 4$. Por lo tanto, $4 \nmid n + m$.

Sea un primo $p \neq 2$ que divide a $k'$. Claramente, $p|(n+m)(n-m)$ pero vamos a ver, con argumentos muy similares a los de antes, que si $p|n - m$ ( respectivamente $n + m$ ), entonces $p \nmid n + m$ ( respectivamente $n - m$ );

- Si $p|n - m$ entonces $n \equiv m \pmod p \Rightarrow n + m \equiv 2m \pmod p$. Acabamos observando que $n + m \equiv 0 \pmod p$ solo si $m \equiv 0 \pmod p$, pero esto no puede ser porque $m$ y $k$ son coprimos. Por lo tanto, $p \nmid n + m$.

Para terminar, expresamos $k$ como producto único de sus factores primos $k = 2^r p_1^{r_1} \cdots p_i^{r_i}$, con $r > 0$, pues $2|k$, y $p_j \neq 2\ \forall j$. Es decir, que tenemos;

$$(n+m)(n-m) = 2(2^{2r} p_1^{2r_1} \cdots p_i^{2r_i}),$$

y considerando los dos puntos anteriores, cada factor $p_j^{2r_j}$ divide o bien a $n+m$ o bien a $n-m$. Reordenando $p_1, ...p_i$ si hiciera falta, es necesario y suficiente hallar una solución al siguiente sistema;

$$\begin{cases} n \pm m &= 2p_1^{2r_1} \cdots p_j^{2r_j} \\ n \mp m &= 2^{2r} p_{j+1}^{2r_{j+1}} \cdots p_i^{2r_i} \end{cases} \text{ para un cierto } 0 \leq j \leq i.$$

Que siempre tiene solución entera, ya que si sumamos ambas ecuaciones, nos da;

$$2n = 2p_1^{2r_1} \cdots p_j^{2r_j} + 2^{2r} p_{j+1}^{2r_{j+1}} \cdots p_i^{2r_i} \Rightarrow$$
$$n = p_1^{2r_1} \cdots p_j^{2r_j} + 2^{2r-1} p_{j+1}^{2r_{j+1}} \cdots p_i^{2r_i}$$

A partir de aquí, podemos encontrar $m$. Entonces, existen enteros $n$ y $m$ tales que $n^2 - m^2 = 2k^2$ si y solo si $k$ es par, lo que implica que existen infinitas soluciones. Una solución, por ejemplo, viene dada para $k = 4$ cumpliendo que $9^2 - 7^2 = 2(4)^2$, que nos da el punto racional $(\frac{9}{4}, \frac{7}{4})$ sobre la hipérbola.

**Observación.** Hemos encontrado todos los puntos racionales sin usar la técnica geométrica que habíamos dicho, pero es con este método de reducción de módulo que podremos determinar la existencia de puntos racionales.

**Observación.** Hemos obtenido los puntos racionales de la hipérbola en $\mathbb{A}^2$, a partir de los puntos enteros sobre la cónica correspondiente de $\mathbb{P}^2$, como habíamos advertido.

**Ejemplo.**

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

Si existe alguna solución a esta ecuación deberá ser racional, así que, como en el ejemplo anterior, consideramos la versión proyectiva de la ecuación $n^2 + m^2 = 3k^2$. Si $n, m, k \in \mathbb{Z}$ satisfacen la ecuación, podemos suponer que son coprimos dos a dos. Además, ni $n$ ni $m$ son divisibles por 3, o de lo contrario, si $3|n$ entonces $3|3k^2 - n^2 = m^2$ y 3 dividiría a $n, m$ contrariamente a lo que habíamos dicho. Esto equivale a decir que $n \equiv \pm 1 \equiv m \pmod 3 \Rightarrow n^2 \equiv 1 \equiv m^2 \pmod 3$. Por otro lado, si reducimos módulo 3 la ecuación $n^2 + m^2 = 3z^2$ obtenemos;

$$0 \equiv n^2 + m^2 \equiv 1 + 1 = 2 \pmod 3,$$

lo cual es una contradicción. Podemos asegurar entonces que no hay puntos racionales sobre la cónica de ecuación $x^2 + y^2 = 3$.

Como hemos podido entrever, la existencia de puntos racionales sobre una cónica se reduce al estudio de soluciones enteras para una ecuación del tipo $an^2 + bm^2 + ck^2 = 0$. Podremos discutir dicha existencia después de ver el siguiente teorema, ver [18] para más información al respecto.

**Teorema 2.1.1.1** (Legendre)**.** La ecuación diofantina $ax^2 + by^2 + cz^2 = 0$ con $a, b, c$ coprimos dos a dos, libres de cuadrados y no todos del mismo signo, tiene una solución no trivial racional ( y por lo tanto, entera ) si y solo si, $-ab$ es un cuadrado módulo $|c|$, $-bc$ es un cuadrado módulo $|a|$ y $-ca$ es un cuadrado módulo $|b|$.

A continuación veremos unos ejemplos concretos de cónicas y sus puntos racionales. Además, daremos una caracterización de los conjuntos racionales de tres puntos no alineados ( triángulos enteros ).

### 2.1.2. La circunferencia unidad y ternas pitagóricas

Existe una correspondencia directa entre los puntos racionales de la circunferencia unidad $C$ y las ternas pitagóricas. Esto es, porque si consideramos la ecuación $x^2 + y^2 = 1$ de la circunferencia unidad $C$, su versión proyectiva es $x^2 + y^2 = z^2$, que caracteriza las ternas pitagóricas.

De este argumento, deducimos que si hallamos todos los puntos racionales en $C$, obtendremos también las soluciones enteras de la versión proyectiva de la curva con $z \neq 0$, y por lo tanto, las ternas pitagóricas. Una forma de determinar todos los puntos racionales $p = (x, y)$ de $C$, es lograr una parametrización $x(t), y(t)$ siendo $x(t), y(t)$ funciones racionales.

Para ello, partimos de una solución racional trivial de la ecuación de la circunferencia como es $(-1, 0)$. A continuación, trazamos la recta con pendiente $t$ que pasa por $(-1, 0)$, esta es, la recta $y = t(x + 1)$.

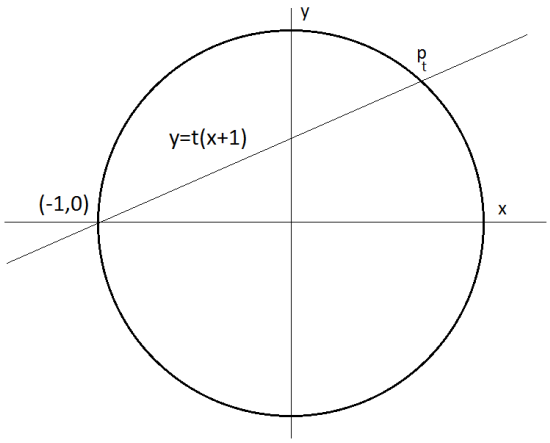


Figura 3: recta por $(-1, 0)$ y $p_t$ de pendiente $t$

Queremos la parametrización del punto $p_t = (x(t), y(t))$ de la *figura 4*. Sustituyendo un punto genérico $(x, t(x+1))$ de la recta en la ecuación de la circunferencia, llegamos a que $x^2 + (t(x+1))^2 - 1 = 0$. Las soluciones de la ecuación, son los valores que toma la coordenada $x$ en las intersecciones entre la recta y la circunferencia de la figura 4. Podemos factorizar $(x+1)$ en la ecuación, pues es la solución trivial que corresponde al punto de intersección $(-1, 0)$, y obtenemos $(x+1)(x(1+t^2)+t^2-1) = 0$. La otra solución para $x$, cuando $x(1+t^2)+t^2-1 = 0$, corresponde a la coordenada $x(t)$. Una tenemos esto, somos capaces de parametrizar el punto $p_t$;

$$\begin{aligned} x(t) &= \tfrac{1-t^2}{t^2+1} \\ y(t) &= t(x+1) = \tfrac{2t}{t^2+1} \end{aligned}$$

El punto $p_t = (x(t), y(t))$ es racional si y solo si $t$ lo es, por lo que determinamos todos los puntos racionales sobre la circunferencia unidad. Es decir, si $t = \frac{n}{m}$ con $n, m \in \mathbb{Z}$, entonces $p_t = p_{n,m} = (\frac{m^2-n^2}{n^2+m^2}, \frac{2nm}{n^2+m^2})$ representa todos los puntos racionales de $C$.

Por lo tanto, hallamos todas las ternas pitagóricas $a, b, c$ solución de $x^2+y^2 = z^2$, pues son $a = m^2 - n^2$, $b = 2nm$, $c = n^2 + m^2$ $\forall n, m \in \mathbb{Z}$

### 2.1.3. La elipse $x^2 - 2qxy + y^2 = 1$ y triángulos enteros

Primero, recordaremos un teorema muy conocido;

**Teorema** (Coseno)**.** Dado un triángulo de lados $a, b, c$ y ángulos $\alpha, \beta, \gamma$ opuestos a dichos lados, entonces;

$$a^2 - 2ab\cos(\gamma) + b^2 = c^2$$

Consideremos la elipse $C$ de ecuación $x^2 - 2qxy + y^2 = 1$. Así como ocurre en el caso de la circunferencia unidad, obtenemos una solución racional para la elipse si y solo si obtenemos una solución entera para $x^2 - 2xyq + y^2 = z^2$ con $z \neq 0$. Gracias al Teorema del Coseno, esto nos dice que un punto de $C$ es racional, digamos $(\frac{a}{c}, \frac{b}{c})$, si y solo si existe un triángulo de lados enteros $a, b, c$ y $\cos(\gamma) = q$, donde $\gamma$ es el ángulo opuesto al lado $c$. Por lo tanto, nos basta con hallar todos los puntos racionales de $C$ para obtener los triángulos enteros con $\cos(\gamma) = q$.

**Observación.** Se deduce que $q = \cos(\gamma)$ debe ser racional o de lo contrario, si $q \notin \mathbb{Q}$, no existen $x$ e $y$ racionales que puedan satisfacer la ecuación de $C$. También nos damos cuenta de que queremos que $q^2 < 1$, pues el coseno de cualquier ángulo de un triángulo se halla en el intervalo $(-1, 1)$.

De nuevo, trazamos la recta de pendiente $t \in \mathbb{R}$ que pasa por el punto (-1,0) de $C$. La recta corta con $C$, además de en (-1,0), en un punto $p_t = (x(t), y(t))$.

Procedemos como en el caso de la circunferencia, para encontrar la parametrización de $p_t$.

$$x(t) = \frac{1-t^2}{1-2qt+t^2}$$
$$y(t) = t(x+1) = \frac{2t-2qt^2}{1-2qt+t^2}$$

**Observación.** $x(t)$ e $y(t)$ no están definidos si $1-2qt+t^2=0$. Pero eso solo puede suceder si $q^2 \geq 1$ para $t \in \mathbb{R}$.

Para terminar, escribiendo $t = \frac{n}{m}$, $q = \frac{q_1}{q_2}$ y simplificando $p_t$ obtenemos:

$$x(n,m) = \frac{(m^2-n^2)q_2}{q_2(m^2+n^2)-2q_1nm}$$
$$y(n,m) = \frac{q_2 2nm - 2n^2q_1}{q_2(m^2+n^2)-2q_1nm}$$

Concluimos pues, que dado $q = \frac{q_1}{q_2}$, los triángulos enteros de lados $a, b, c$ con $\cos(\gamma) = q = \frac{q_1}{q_2}$ son aquellos con;

$$a = (m^2-n^2)q_2,$$
$$b = 2q_2nm - 2n^2q_1,$$
$$c = q_2(m^2+n^2) - 2q_1nm$$

$\forall n, m \in \mathbb{Z}$

**Observación.** El caso de la circunferencia visto anteriormente, no es más que un caso particular de la elipse para $q = \cos(\gamma) = 0$, es decir, triángulos con un ángulo recto.

### 2.1.4. La hipérbola unidad

Una vez hemos encontrado los puntos racionales sobre la circunferencia unidad, obtenemos una biyección que nos determina los puntos racionales sobre la hipérbola unidad.

Dado un punto racional $(\frac{a}{c}, \frac{b}{c})$ con $a, b, c \in \mathbb{Z}$, está sobre la circunferencia unidad si y solo si $(\frac{c}{a}, \frac{b}{a})$ cae sobre la hipérbola unidad, ya que $(\frac{a}{c})^2 + (\frac{b}{c})^2 = 1 \iff (\frac{c}{a})^2 - (\frac{b}{a})^2 = 1$

## 2.2. Sobre cúbicas. Curvas de género 1

Ahora dejamos las curvas de género 0 y nos fijamos en las cúbicas. Valga decir, que las cúbicas podemos distinguirlas, como cualquier conjunto de curvas, en curvas singulares y curvas no singulares. Las del primer tipo no guardan más misterio que las cónicas, en cuanto al conjunto de puntos racionales se refiere, pues es suficiente reproducir el mismo proceso de parametrización de la curva a partir de un punto distinguido, el punto singular.

**Definición 2.2.0.1.** Una *curva elíptica* sobre un cuerpo $K$ es una curva proyectiva no singular sobre $K$ de género 1.

Sin embargo, las cúbicas no singulares son otra historia. Como acabamos de definir, una curva de género 1 no singular, en el espacio proyectivo, se conoce como curva elíptica. El problema por el que no podemos parametrizar una curva elíptica, es que una recta en el plano cualquiera que corte a nuestra curva, intersecará dos veces más con ella, contando multiplicidades. Para determinar los puntos racionales sobre una curva elíptica, usaremos *El Teorema de Mordell* [13] y [21]. Pero antes, repasemos algunas herramientas y propiedades de las curvas elípticas que son fundamentales para la demostración del teorema, de la que tan solo daremos una idea por ser una demostración demasiado compleja para incluir con rigurosidad en este trabajo. Para conocer con más detalle las curvas elípticas, mirar [12] y [13].

Las curvas elípticas las expresamos con una ecuación cúbica homogénea. Es decir, sea $E$ la curva de ecuación cúbica homogénea $ax^3 + bx^2y + cxy^2 + dy^3 + ex^2z + fxz^2 + gz^3 + hy^2z + iyz^2 + jxyz = 0$, diremos que es una curva elíptica si es no singular de género 1. Primero nos interesa reducir la complejidad de la ecuación a una mucho más simple, conocida como la *ecuación (o forma) de Weierstrass* de curvas elípticas. Para ello, antes tendremos en cuenta la siguiente propiedad que hemos comentado antes.

**Propiedad.** Toda recta del plano proyectivo que interseque a una curva elíptica $E$, interseca exactamente 3 veces con $E$ contando multiplicidades.

Es decir, consideremos una recta cualquiera del plano proyectivo que interseque con $E$ en el punto $P$. Entonces, tal recta interseca dos veces más con $E$, contando multiplicidades. Diremos que la recta interseca a $E$ en $P$ dos veces (multiplicidad 2) si y solo si la recta es tangente a $E$ en $P$ y $P$ no es un punto de inflexión. En el caso que $P$ sea punto de inflexión de $E$ y la recta sea tangente a $E$ en $P$, diremos que la recta interseca 3 veces a $E$ en $P$ ( multiplicidad 3 ).

### 2.2.1. La ecuación de Weierstrass

Toda ecuación cúbica homogénea que descrive una curva elíptica $E$ con un punto racional $O \in E$, puede reescribirse en la forma;

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

nombrada la *ecuación de Weierstrass*. Además, la condición de no singularidad que caracteriza las curvas elípticas, se expresa de modo más sencillo, imponiendo que $4a^3 + 27b^2 \neq 0$.

Primero realizaremos un cambio de referencia que transformará nuestra ecuación. Para transformarla, consideramos $O$ el punto racional sobre $E$, y tomamos la siguiente referencia en el plano proyectivo; situamos el eje $Z = 0$ pasando por $O$ y tangente (con multiplicidad 2) a $E$. Por ser $Z = 0$ tangente a $E$, estas dos se cortan en otro único punto $P$ aparte de $O$. Como recta $X = 0$ tomamos la recta tangente a $E$ por $P$. Para terminar, el eje $Y = 0$ será cualquier recta linealmente independiente a las anteriores que pase por $O$.

Este cambio reescribe la ecuación anterior de la siguiente forma;

$$xy^2 + (ax + bz)yz = cx^2z + dxz^2 + ez^3$$

Si multiplicamos la ecuación por $\frac{xz}{z^2}$ y renombramos $\frac{xy}{z}$ como simplemente la variable $y$, obtenemos;

$$y^2z + (ax + bz)yz = cx^3 + dx^2z + exz^2$$

A continuación, realizamos el cambio de $y$ por $y - \frac{1}{2}(ax + bz)$ para lograr la ecuación

$$y^2z = ax^3 + bx^2z + cxz^2 + dz^3$$

Para conseguir que el coeficiente de $x^3$ sea 1, nos basta con realizar las sustituciones de $x$ e $y$ por $ax$ y $a^2y$ respectivamente;

$$y^2z = x^3 + ax^2z + bxz^2 + cz^3$$

Para terminar, buscamos la forma reducida de la cúbica en $x$ de Cardano, sustituyendo $x$ por $x - \frac{az}{3}$ y consiguiendo;

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

Una vez hemos hallado la forma reducida, imponemos que sea una curva regular. Es decir, queremos que la matriz diferencial de la equación de $E$, tenga rango máximo ( rango 1 ). Si la curva fuese singular, entonces existirían $x, y, z$ tal que;

$$DC(x, y, z) = \left( \begin{array}{ccc} 3x^2 + az^2, & -2yz, & -y^2 + 2axz + 3bz^2 \end{array} \right) = (0, 0, 0)$$

De la segunda ecuación $-2yz = 0$, deducimos que $y = 0$ o $z = 0$. Si es $z = 0$, entonces tenemos que;

$$\left\{ \begin{array}{rcl} 3x^2 & = & 0 \\ -y^2 & = & 0 \end{array} \right. \Leftrightarrow x = 0 \text{ e } y = 0$$

En el caso que $y = 0$, obtenemos que;

$$\begin{cases} 3x^2 + az^2 = 0 \\ 2axz + 3bz^2 = 0 \Rightarrow x = \frac{-3bz}{2a} \end{cases} \Rightarrow 3(\tfrac{-3bz}{2a})^2 + az^2 = 0 \Rightarrow \begin{cases} z = 0 \\ \text{ó} \\ 3(\tfrac{-3b}{2a})^2 + a = 0 \Rightarrow \end{cases}$$

$$27b^2 + 4a^3 = 0$$

Por lo tanto, la condición de no singularidad la obtenemos imponiendo que $27b^2 + 4a^3 \neq 0$.

### 2.2.2. El grupo $E(\mathbb{Q})$

**Definición 2.2.2.1.** Sea $E$ una curva elíptica de ecuación $y^2z = x^3 + axz^2 + bz^3$, definimos $E(\mathbb{Q})$ como el conjunto de puntos racionales sobre $E$.

Mediante una operación que veremos, dotaremos a $E$ de una estructura de grupo. Pero antes, veamos un par de detalles;

Sea $E$ la curva elíptica de ecuación $y^2z = x^3 + axz^2 + bz^3$. Observamos que la recta $z = 0$ del infinito corta a $E$ en las soluciones de la ecuación $0 = x^3$, y por lo tanto, corta el punto $(0, 1, 0) = O$ de $E$ con multiplicidad 3. Es decir, $O$ es punto de inflexión y además, es el único punto de $E$ en tal recta.

**Observación.** El punto $O = (0, 1, 0)$, interpretado en $A^2 \cup \mathbb{P}^1$, más concretamente en $\mathbb{P}^1$, es el punto de intersección de todas las rectas paralelas al eje $y$. Por lo tanto, la recta que pasa por un punto $P$ y por $O$ en $A^2_{\mathbb{R}} \cup \mathbb{P}^1$, es la recta por $P$ paralela al eje $y$.

**Notación.** Sea $E$ una curva elíptica con dos puntos $P, Q \in E$. Sea $r$ la recta por $P$ y $Q$. Claramente $r$ interseca a $E$ en los puntos $P$ y $Q$. Notaremos $P * Q$ al tercer punto de intersección de $r$ y $E$.

Una vez tenemos en cuenta lo anterior, definimos la operación sobre $E$, que notaremos con $'+'$, de la siguiente manera: Sean $P, Q \in E$, y sea la recta que pasa por ellos dos, podemos encontrar un tercer punto $P * Q$, que pertenece también a la recta y a la curva. Definimos $P + Q$ como el punto $S = O * (P * Q)$, es decir, el punto $S$ que resulta de construir la recta por $O$ y $P * Q$, y hallar el tercer punto en $E$ sobre esta recta. Esclarezcamos esta definición geométrica con un dibujo;

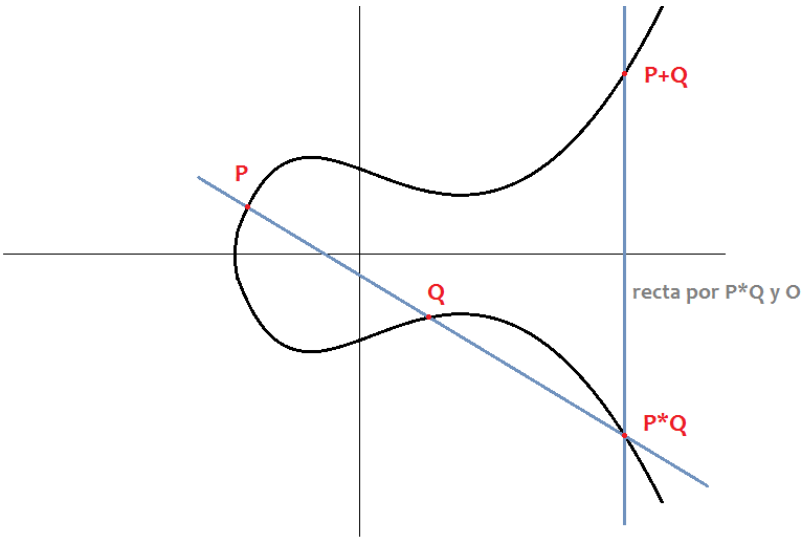


Figura 4: Suma de $P$ y $Q$ en el grupo de $E$

Esta operación nos permite entender $E$ como un grupo abeliano con elemento neutro $O$. No profundizaremos más en las propiedades de grupo, aunque geométricamente resulta sencillo comprovar la comutatividad y, con algo más de dificultad, la asociatividad. Además, es cierto que si $P$ y $Q$ de $E$ son racionales, entonces $P+Q$ también es racional, por lo que $E(\mathbb{Q})$ resulta ser un subgrupo.

### 2.2.3. Altura

La siguiente definición nos servirá para determinar la 'complejidad' de un punto racional sobre nuestra curva, desde el punto de vista de la teoría de números.

**Definición 2.2.3.1.** Definimos la *altura de un número racional* $x = \frac{n}{m}$ con mcd$(n,m)$= 1 como $H(x) = \text{máx}\{|m|, |n|\}$

Nos servimos de la anterior definición para dar la altura de un punto racional $P = (x, y, 1)$ de la curva elíptica. Recordemos que nuestra curva viene dada por la ecuación $y^2z = x^3 + axz^2 + bz^3$.

**Definición 2.2.3.2.** Definimos la *altura de un punto racional* $P = (x, y, 1) \in \mathbb{P}^2$ como la altura de la primera coordenada, es decir, $H(P) = H(x)$. El único punto racional impropio $O = (0, 1, 0)$ tiene altura $H(O) = 1$.

Es fundamental tener en cuenta la siguiente propiedad de las alturas, con la que trataremos de dar una cota al conjunto de generadores del grupo $E(\mathbb{Q})$.

**Propiedad.** El conjunto de números racionales con una altura inferior a un número positivo dado es un conjunto finito.

**Propiedad.** El conjunto de puntos racionales de $E(\mathbb{Q})$ con una altura inferior a un número positivo dado es un conjunto finito.

La primera propiedad está clara, pues si $H(x) < k$, entonces el numerador y denominador de $x$ deben ser inferiores a $k$, lo que nos da una cantidad finita de combinaciones. Para la segunda propiedad, basta observar que por la primera propiedad, tenemos una finitud de valores para $x$, y entonces, una vez escogido un valor para $x$, $y$ tan solo puede tomar dos valores, pues $y^2 = x^3 + ax + c$. Nos interesa considerar el logaritmo de las alturas, por la propiedad aditiva de los logaritmos.

**Definición 2.2.3.3.** Sea $P \in E(\mathbb{Q})$, definimos $h(P) = log(H(P))$, que también nombraremos altura.

A continuación, veremos 4 lemas que serán nuestra guía para la demostración de *El Teorema de Mordell*. Para todos ellos, supondremos que tenemos una curva elíptica concreta $E$, y por lo tanto, un grupo $E(\mathbb{Q})$ concreto.

**Lema** (1)**.** Para cada $M$, el conjunto $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ es finito.

**Lema** (2)**.** Sea $Q \in E(\mathbb{Q})$, existe $k_Q$ tal que $h(P + Q) \leq 2h(P) + k_Q$, $\forall P \in E(\mathbb{Q})$.

**Lema** (3)**.** Existe una $k$ tal que $h(2P) \geq 4h(P) - k$, $\forall P \in E(\mathbb{Q})$.

**Lema** (4)**.** El índice $(E(\mathbb{Q}) : 2E(\mathbb{Q}))$ es finito.

Con $2E(\mathbb{Q})$ nos referimos al subgrupo de $E(\mathbb{Q})$ formado por los puntos racionales $P$ que son punto doble para algún otro $Q \in E(\mathbb{Q})$, es decir, los puntos $P$ para los que existe un $Q$ donde se cumple $P = Q + Q$.

### 2.2.4. Teorema del Descenso

**Teorema 2.2.4.1** (del Descenso)**.** Sea $G$ un grupo abeliano. Supongamos que existe una función altura $h : A \to \mathbb{R}$ para la que se cumplen los Lemas 1, 2, 3 y 4. Entonces $G$ está finítamente generado.

*Demostración.* Nuestra intención, es hallar un subconjunto finito de $G$ a partir del cual podamos generar todo $G$. Para ello, comenzamos considerando el lema 4, que nos dice que $(G : 2G)$ es finito. Para simplificar notación, diremos $H = 2G$. En particular, sabemos que tenemos un número finito $n$ de clases laterales. Recordemos que una clase lateral de $H$ en $G$ es $g + H = \{g + h \mid h \in H\}$. Así que, consideremos $b_1, \cdots, b_n$ los representantes de las $n$ clases laterales.

Por lo tanto, para cualquier elemento $g \in G$, existe un $i_1$ tal que $g - b_{i_1} \in H$, pues $g$ debe pertenecer a alguna clase lateral. Es decir, que $g - b_{i_1} = h_1$ para un cierto $h_1 \in H$. Como $h \in H = 2G$, tenemos que existe un $g_1 \in G$ tal que $h = 2g_1$ así que;

$$g - b_{i_1} = 2g_1$$

Repetimos el proceso para $g_1$, por el que deberá existir un $i_2$ y un $g_2$ tal que $g_1 - b_{i_2} = 2g_2$. Lo mismo para $g_2$ y demás, hasta tener;

$$\begin{aligned} g - b_{i_1} &= 2g_1 \\ g_1 - b_{i_2} &= 2g_2 \\ &\vdots \\ g_{m-1} - b_{i_m} &= 2g_m \end{aligned}$$

o equivalentemente;

$$\begin{aligned} g &= b_{i_1} + 2g_1 \\ g_1 &= b_{i_2} + 2g_2 \\ &\vdots \\ g_{m-1} &= b_{i_m} + 2g_m \end{aligned}$$

Nuestra intención es expresar $g$, que era un elemento cualquiera de $G$, como la suma de los elementos de un subconjunto finito de $G$. En la primera ecuación, podemos sustituir $g_1$ según la igualdad de la segunda ecuación, y en la segunda ecuación, podemos cambiar $g_2$ obedeciendo a la tercera ecuación. Realizando estas sustituciones hasta $g_{m-1}$ expresamos;

$$g = b_{i_1} + 2b_{i_2} + \cdots + 2^{m-1}b_{i_m} + 2^m g_m$$

Esto quiere decir, que $g$ se puede generar a partir del conjunto $\{b_1, \dots b_n\}$ y el elemento $g_m$, ya que los $b_{i_j}$ pertenecen a ese conjunto. Si podemos probar, que para un $m$ suficientemente grande, $g_m$ tiene altura inferior a un entero $k$, habremos acabado, pues el conjunto $\{f \in G | h(f) < k\}$ es finito por el lema 1 y el conjunto finito generador de $G$ que buscamos sería $\{b_1, \dots b_n\} \cup \{f \in G | h(f) \leq k\}$.

Para ello, compararemos la altura de $g_{j-1}$ con la de $g_j$. Por el lema 2, tenemos que;

$$h(g - b_i) \leq 2h(g) + k_i,$$

para un cierto $k_i$ que depende de $b_i$ y para todo $g \in G$. Sea $k' = \text{máx}_i\, k_i$, entonces;

$$h(g - b_i) \leq 2h(g) + k',\ \forall g \in G,\ \forall i \in \{1, \dots, n\}$$

Del Lema 3, sabemos que hay una $k''$ tal que $h(2g) \geq 4h(g) + k''$ para cualquier $g$, por lo tanto;

$$4h(g_j) \leq h(2g_j) + k'' = h(g_{j-1} - b_{i_j}) + k'' \leq 2h(g_{j-1}) + k' + k'' \Longleftrightarrow$$

$$h(g_j) \leq \frac{1}{2}h(g_{j-1}) + \frac{k' + k''}{4} = \frac{3}{4}h(g_{j-1}) - \frac{1}{4}(h(g_{j-1}) - (k' + k''))$$

Por lo tanto, si definimos $k = k' + k''$ y suponemos que $h(g_{j-1}) \geq k$ entonces;

$$h(g_j) \leq \frac{3}{4}h(g_{j-1})$$

Como decíamos, queríamos ver que para una $m$ suficientemente grande $h(g_m) \leq k$. Si la condición para un $g_j$ ya se cumple, hacemos $j = m$, pues es suficientemente

grande. Si no, hallamos el punto $g_{j+1}$ que hemos probado que cumple $h(g_{j+1}) \leq \frac{3}{4}h(g_j)$, por lo que su altura es, como mucho, tres cuartas partes de la altura de $h(g_j)$. Repetimos este último paso, hasta encontrar un $g_{j+i}$ que satisfaga lo que queremos, y seguro que lo encontraremos, porque la sucesión $\{(\frac{3}{4})^i\}_i$ tiende a cero cuando $i$ tiende al infinito. Así pues, $g$ se puede generar a partir del conjunto finito $\{b_1, \dots b_n\} \cup \{f \in G | h(f) \leq k\}$ como queríamos probar.

□

### 2.2.5. Teorema de Mordell

**Teorema 2.2.5.1** (de Mordell)**.** Sea $E$ una curva elíptica. El grupo $E(\mathbb{Q})$ está finitamente generado.

Aquí concluye el estudio para curvas cúbicas no singulares. Recordemos el inicio de sección: los puntos racionales sobre una cúbica singular $C$, se hallaban repitiendo la técnica de parametrización de la curva según un racional $t$, tomando el punto singular $S$ ( que siempre es único ) como referencia. Si bien es cierto, es necesario especificar, que también existe un grupo para $C$, si excluímos del conjunto al punto $S$. Habiendo elegido un punto $O \in C - \{S\}$ como elemento neutro, el grupo tiene la misma operación geométrica descrita anteriormente. Y si $O \in C(\mathbb{Q})$ entonces $C(\mathbb{Q}) - \{S\}$ resulta ser un subgrupo. Sin embargo, el comportamiento de este subgrupo es bien distinto. O bien es isomorfo al grupo $(\mathbb{Q}, +)$ o bien es isomorfo al grupo $(\mathbb{Q}^*, \times)$, que en ninguno de los dos casos es finitamente generado, al contrario que en el caso de las curvas elípticas.

La demostración del *Teorema de Mordell* utiliza de manera directa el *Teorema del Descenso*. Pero antes de engañarnos demasiado, hay que recordar que no hemos visto las demostraciones de los Lemas 2, 3 y 4. Podríamos probar sin demasiadas complicaciones los Lemas 2 y 3, sin embargo, el Lema 4 nos podría dar varios dolores de cabeza. Por ello, seguiremos con nuestra búsqueda de puntos racionales sobre curvas. El siguiente nivel pasaría por las curvas de género $g > 1$.

## 2.3. Sobre curvas de género $g > 1$

Para este tipo de curvas, no indagaremos en el tema, simplemente daremos buen uso al siguiente potente resultado.

### 2.3.1. Teorema de Faltings

**Teorema 2.3.1.1** (Faltings)**.** Una curva algebraica $C$ de género $g > 1$ definida sobre un cuerpo de números algebraicos contiene una cantidad finita de puntos racionales.

# 3. El Problema de Erdös

Nos adentramos en el problema de Erdös. Constatemos dos cosas. La primera, un conjunto en posición general es un conjunto que no tiene 3 puntos sobre una recta ni 4 puntos sobre una circunferencia. Y la segunda, un conjunto con distancias racionales entre los puntos del conjunto, puede dilatarse con una homotecia para que las distancias sean enteras. Antes de ver algunas construcciones de conjuntos finitos en posición general y distancias enteras, nos preguntamos: ¿Qué conjuntos son infinitos y con todas las distancias enteras? Tras unos segundos de meditación, uno rápidamente piensa en posibles conjuntos sobre la recta. ¿Y fuera de ella? A continuación, el *Teorema de Anning-Erdös* despejará cualquier tipo de duda sobre esta cuestión. La demostración que seguimos puede encontrarse en [5] y la primera demostración por Norman H. Anning y Paul Erdös se halla en [1].

## 3.1. El Teorema de Anning-Erdös

**Teorema 3.1.0.2** (Anning-Erdös)**.** Sea $S$ un subconjunto infinito del plano. Si la distancia entre todos los puntos de $S$ es entera, entonces $S$ está contenido en una recta.

*Demostración.* Para provar el resultado, demostraremos que si existen 3 puntos de $S$ que no están sobre una recta, entonces la cardinalidad de $S$ está acotada. Sean $A, B$ y $C$ dichos puntos de $S$ no alineados. Consideramos las distancias entre estos puntos como marca la figura 5;

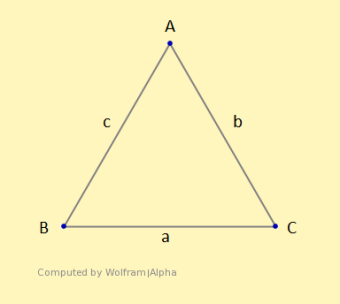


Figura 5: triángulo ABC

Por hipótesis, $a, b, c \in \mathbb{N}$. Consideramos un entero $d \geq a, b, c$. Sea $X$ otro punto de $S$, es decir, que $d(X, A), d(X, B), d(X, C) \in \mathbb{N}$. De la desigualdad triangular tenemos que;

$$|d(X, A) - d(X, B)| \leq c \leq d$$

Por ser la resta de dos naturales, será;

$$|d(X,A) - d(X,B)| = i, \tag{3.1}$$

para un cierto natural $i \leq d$. La ecuación 3.1, tras fijar la $i$, es una hipérbola con $A$ y $B$ como focos. Es decir, que $X$ pertenece a alguna de las $d+1$ hipérbolas.

El mismo razonamiento podemos repetirlo ahora con $B$ y $C$: si $X$ es de $S$ entonces;

$$|d(X,C) - d(X,B)| \leq a \leq d$$

Por lo tanto, $X$ satisface la ecuación de la hipérbola;

$$|d(X,A) - d(X,B)| = j, \tag{3.2}$$

para un cierto natural $j \leq d$. Entonces, $X$ pertenece también a una de las $d+1$ hipérbolas con $B$ y $C$ como focos;

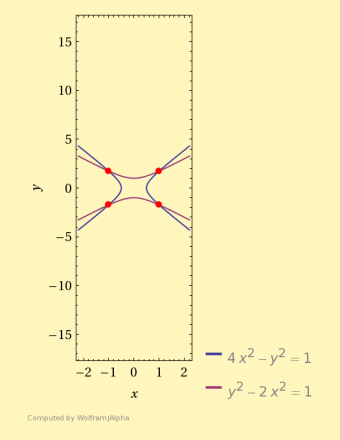


Figura 6: Intersección de 2 hipérbolas

Por lo tanto, $X$ es una de las 4 soluciones del sistema formado por 3.1 y 3.2 (intersección de dos hipérbolas, ver figura 6). Dado que disponíamos de $d+1$ posibles hipérbolas con focos $A$ y $B$, y la misma cantidad de hipérbolas con focos $B$ y $C$, nos da un total de $(d+1)^2$ sistemas distintos con 4 soluciones cada uno. Es decir, $X$ solo puede ser uno de esos $4(d+1)^2$ puntos solución, y por lo tanto, la cardinalidad de $S$ está acotada.

□

## 3.2. Conjuntos finitos con distancias enteras

Ahora sí, nuestro conjunto con distancias enteras va a ser finito. Antes de imponer que el conjunto debe estar en posición general, nos preguntamos la existencia de estos conjuntos sin más condición. Claramente, queremos obviar el caso en que el conjunto está sobre una recta. Demos la construcción de un conjunto con un número de puntos $n \in \mathbb{N}$ arbitrariamente grande y distancias enteras, presente en [1] donde se pueden encontrar dos ejemplos más. Para ello, haremos uso del siguiente *Teorema de Fermat* y del *Teorema de Ptolomeo.*

**Teorema 3.2.0.3** (Fermat)**.** Un número primo $p$ es suma de dos cuadrados si y solo si $p \equiv 1 \pmod 4$

**Teorema 3.2.0.4** (Ptolomeo)**.** Dado un cuadrilátero $ABCD$ con vértices en una circunferencia, entonces se cumple: $d(A,C)d(B,D) = d(A,B)d(C,D)+d(B,C)d(D,A)$.

**Teorema 3.2.0.5.** Para cualquier $n \geq 0$, existe un subconjunto $S$ del plano con $card(S) = n$ y con distancias enteras, tal que $S$ está contenido en una circunferencia.

*Demostración.* Consideremos la circunferencia de diámetro 1 en el origen, $x^2+y^2 = \frac{1}{4}$. Sean $p_1, p_2, p_3, \ldots$ números primos tales que $p_k \equiv 1 \pmod 4$ $\forall k \in \mathbb{N}$. Entonces, por el *Teorema de Fermat*, existen números naturales $a_k, b_k$ que satisfacen;

$$(1) \quad p_k^2 = a_k^2 + b_k^2,$$

para todo k natural.

Ahora, sea el punto sobre la mitad superior de la circunferencia que está a distancia $\frac{b_k}{p_k} < 1$ del punto $(-\frac{1}{2}, 0)$, que denotaremos por $(x_k, y_k)$. Definimos nuestro conjunto como;

$$S = \{(-\frac{1}{2}, 0), (0, \frac{1}{2}), (x_k, y_k); 1 \leq k \leq n-2\}$$

Veremos que la distancia entre cualquier par de puntos es racional. Por inducción sobre $k$, para el caso base $k = 1$ tenemos;

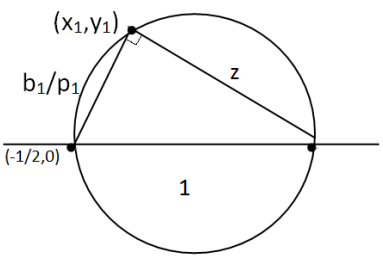


Figura 7: Punto $(x_1, y_1)$ de $S$

Por lo que solo debemos ver si $z$ es racional. En efecto pues el triángulo inscrito es un triángulo rectángulo y al cumplirse (1), nos queda que $z = \frac{a_1}{p_1}$.

Supongamos que lo hemos demostrado para todo $k < i$. Debemos ver que la distancia de $(x_k, y_k)$ a $(x_i, y_i)$ es racional. Si tomamos los 4 puntos $(-\frac{1}{2}, 0), (0, \frac{1}{2}), (x_k, y_k)$ y $(x_i, y_i)$, por construcción tenemos que 5 de las 6 distancias entre dichos puntos es racional. Tan solo queda comprobar la distancia de $(x_k, y_k)$ a $(x_i, y_i)$, que por el teorema de Ptolomeo, debe ser racional.

Para terminar, aumentando el radio de la circunferencia lo suficiente (dilatándolo por el mínimo común denominador de todas las distancias del conjunto), obtenemos un conjunto, sobre la circunferencia, de $n$ puntos con todas las distancias enteras.

□

## 3.3. Conjuntos Enteros

Al fin atenderemos al Problema de Erdös con todas sus condiciones. Repetimos: nos preguntamos sobre la existencia de conjuntos de $n$ puntos del plano en posición general, es decir, sin 3 puntos en una misma recta ni 4 en una circunferencia, tales que la distancia entre dos puntos cualquiera sea entera. Para abreviar, los llamaremos simplemente conjuntos enteros. Un problema a la hora de buscar estos conjuntos, cuanto más grande es la $n$, viene dada por la creciente separación entre los puntos del conjunto. Otro, es por ejemplo, es la complejidad de las coordenadas de sus puntos. Es por eso, que antes de ponernos a buscar conjuntos enteros, necesitaremos los conceptos que a continuación vamos a ver. Dejaremos las contrucciones y ejemplos de conjuntos enteros para el anexo A.

### 3.3.1. Diámetro y cantidad de triángulos enteros

**Definición 3.3.1.1.** El *diámetro* de un conjunto entero $S$ es la distancia máxima $d$ asumible entre los puntos del conjunto. Es decir $d = \text{máx}_{p,q \in S}\, d(p, q)$.

Es comprensible que cuantos más puntos queramos que tenga nuestro conjunto entero, más elevado deberá ser el diámetro. Démonos cuenta, de que si fijamos el diámetro $d$, existen un número finito de posibles conjuntos enteros de $n$ puntos y diámetro $d$, pues cada una de las distancias entre dos puntos del conjunto, es entera y menor o igual a $d$, por lo que hay una finitud de posibilidades. En el capítulo anterior hemos hallado todos los triángulos enteros. Puesto que los conocemos todos, veamos cuantos triángulos enteros distintos de diámetro exáctamente $d$ hay, tras ver la siguiente definición;

**Definición 3.3.1.2.** Definimos $\phi(n, d)$ como la cantidad de conjuntos enteros no isométricos de $n$ puntos y diámetro $d$.

Con no isométricos nos referimos a que no exista una transformación isométrica entre dos de los conjuntos, es decir, que no se reproduzcan todas las mismas distancias entre todos los puntos.

**Proposición 3.3.1.1.**

$$\phi(3,d) = \begin{cases} \frac{d(d+2)}{4} & \text{si } d \text{ es par} \\ \\ \frac{(d+1)^2}{4} & \text{si } d \text{ es impar} \end{cases}$$

*Demostración.* Queremos contar la cantidad de triángulos de lados $(a,b,c)$ no isométricos con diámetro $d$ y $a,b,c,d \in \mathbb{N}$. Puesto que el triángulo debe tener diámetro $d$, consideramos $c = d$ el lado más largo. Luego, $b$ puede tener cualquier valor tal que $1 \leq b \leq d$ (que son $d$ posibilidades). Para acabar de construir el triángulo, debemos cumplir la desigualdad triangular (estrictamente), por lo que nos bastará imponer que $a + b \geq c + 1 = d + 1$. Entonces, $a$ tiene cualquier valor en esa desigualdad, sin ser mayor que $d$, es decir $(d+1) - b \leq a \leq d$ (que son $b$ posibilidades). Por lo tanto, el número total de triángulos es;

$$\sum_{b=1}^{d} b = \frac{d(d+1)}{2}$$

En este cálculo, no hemos hecho ninguna distinción entre triángulos. Es decir, hemos contado el triángulo de lados $(a,b,d)$ y también el de lados $(b,a,d)$ que son isométricos, pues el segundo es el resuldado de una simetría axial del primero. Esto nos ha ocurrido para todos los triángulos menos aquellos con $a = b$. Por ello, vamos a contar la cantidad de triángulos isóceles con $a = b$ y con base $d$.

La desigualdad triángular nos dice que $a + b = 2b \geq d + 1$ y por lo tanto $\left[\frac{d+2}{2}\right] \leq b \leq d$. Entonces, hay $\frac{d}{2}$ triángulos isóceles con $a = b$ si $d$ es par y $\frac{d+1}{2}$ si $d$ es impar. En este cálculo entra también el triángulo equilátero de lado $d$.

Nuestra solución es; la mitad de los triángulos no isóceles con $a = b$, más los triángulos isóceles con $a = b$;

$$\phi(3,d) = \begin{cases} \frac{\frac{d(d+1)}{2} - \frac{d}{2}}{2} + \frac{d}{2} & \text{si } d \text{ es par} \quad = \quad \frac{d(d+2)}{4} \text{ si d es par} \\ \frac{\frac{d(d+1)}{2} - \frac{d+1}{2}}{2} + \frac{d+1}{2} & \text{si } d \text{ es impar} \quad = \quad \frac{(d+1)^2}{4} \text{ si d es impar} \end{cases}$$

□

Existen otras maneras de clasificar los triángulos enteros, por ejemplo, por su perímetro. En [4], se contabilizan los triángulos enteros de perímetro igual o inferior a $p$, a partir del *Teorema de Pick*, ver [20].

Hemos visto que la cantidad de triángulos distintos de diámetro $d$ es del orden de $d^2$. También es cierto que $\phi(n,d)$ será finito para cualquier $n$ y $d$, puesto que hay una finitud de posibles valores que puede tomar cada una de las distancias entre dos puntos. Esto nos permite usar el cálculo con ordenadores para generar todos los posibles conjuntos enteros no isométricos de $n$ puntos y diámetro inferior o igual a $d$. A partir de una búsqueda exhaustiva, e incrementando sucesivamente el diámetro $d$, en [6], se determina el mínimo diámetro $\dot{d}(2,n)$ necesario para construir un conjunto entero de $n$ puntos en el plano con $n \leq 7$. Estos son;

$$\begin{aligned}\dot{d}(2,3) &= 1\\ \dot{d}(2,4) &= 8\\ \dot{d}(2,5) &= 73\\ \dot{d}(2,6) &= 174\\ \dot{d}(2,7) &= 22270\end{aligned}$$

Para $n = 3$, el triángulo de diámetro 1 es claramente el triángulo equilátero de lado 1. En breve, veremos un conjunto entero de 4 puntos con diámetro mínimo 8. Mostraremos el conjunto entero asociado para $n = 7$ en el anexo, como habíamos dicho. Como se puede apreciar, el diámetro mínimo crece muy deprisa según añadimos un punto más. Debido a ello, y a la alta cuantía de cálculos que se precisan, todavía no se ha podido determinar con este método el diámetro mínimo para un conjunto entero de 8 puntos. Aunque primero habría que demostrar la existencia de un tal conjunto.

Esta búsqueda, exhaustiva y realmente costosa en tiempo y cálculos, no es la única que nos permite hallar conjuntos enteros. Otro método, menos ambicioso por no ser exhaustivo pero más astuto por responder a una intuición, recientemente ha generado 25 nuevos conjuntos enteros de 7 puntos ( más concretamente son 7-clusters, para definición ver 3.3.3 ), encontrados y representados gráficamente en [15]. La idea del método parte de la construcción de conjuntos enteros de 4 puntos a partir de un tipo concreto de triángulos. A continuación veremos cómo hallar tantos conjuntos de estos como queramos.

### 3.3.2. Triángulos Heronianos y conjuntos enteros de 4 puntos

Existe un tipo de triángulos, conocidos como triángulos Heronianos, que nos pueden servir para generar infinitos conjuntos enteros de 4 puntos en el plano . Los triángulos Heronianos son triángulos de lados y área enteros. Puesto que el área de un triángulo es base por altura entre 2, entonces las alturas de estos triángulos son racionales (o enteras). Por supuesto, aumentando el triángulo con una homotecia de razón el mínimo denominador común de las alturas, hallamos un triángulo con alturas y lados enteros. En particular, los triángulos Pitagóricos son triángulos Heronianos. Su nombre, se explica por ser triángulos que satisfacen la ecuación diofantina;

$$\Delta^2 = s(s-a)(s-b)(s-c)$$

obtenida a partir de la fórmula de Herón para calcular el área $\Delta$ de un triángulo de lados $a, b$ y $c$ donde $s = \frac{a+b+c}{2}$. Se conocen soluciónes a dicha ecuación diofantina, que son;

$$\begin{aligned} a &= n(m^2+k^2) \\ b &= m(n^2+k^2) \\ c &= (m+n)(mn-k^2) \end{aligned}$$

con $n, m$ y $k$ enteros tal que $\text{mcd}(n,m,k)=1$, $\frac{m^2n}{2m+n} \leq k^2 < mn$ y $1 \leq n \leq m$ ( para obtener lados positivos y triángulos no repetidos ). Veamos un par de ejemplos;

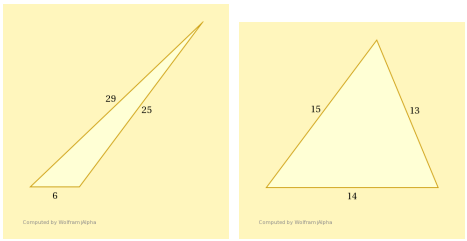


Figura 8: Triángulos Heronianos

El triángulo de la izquierda de la figura 8 tiene área 60 y el otro 84. El primero lo hemos obtenido escogiendo $n=1$, $m=5$, $k=2$, y no es complicado comprovar que el segundo no puede generarse. Sin embargo, puede obtenerse un triángulo múltiplo a éste, para unos ciertos valores de $n, m, k$. El método empleado para obtener el de la derecha, ha sido el de adherir dos triángulos Pitagóricos, así como vemos en la figura 9;

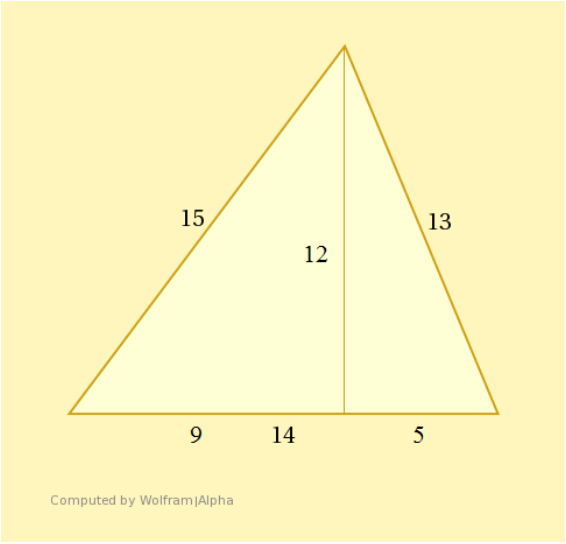


Figura 9: Triángulo Heroniano obtenido a partir de dos triángulos Pitagóricos

**Teorema.** Todo triángulo Heroniano o un múltiplo de éste, puede obtenerse uniendo dos triángulos Pitagóricos.

La demostración de este teorema junto con más resultados referentes a los triángulos Heronianos pueden encontrarse en [3]. Para el tema que nos ocupa, cesaremos el

estudio de estos triángulos y aprovecharemos sus propiedades para generar infinitos conjuntos enteros de 4 puntos.

Sea $ABC$ un triángulo Heroniano no rectángulo de lados $a, b, c \in \mathbb{Z}$ y sea $h$ la altura asociada al vértice $A$ y perpendicular al lado $a$ ( ver figura 10 ). Podemos suponer que $h$ es entero ( sino, aumentamos el triángulo para que dicha altura sea un entero ). Sea el triángulo $A'B'C'$ una copia ( simétrica ) del anterior, lo adherimos al primero identificando $B$ con $B'$ y $C$ con $C'$. Entonces $S = \{A, B, C, A'\}$ es un conjunto entero.

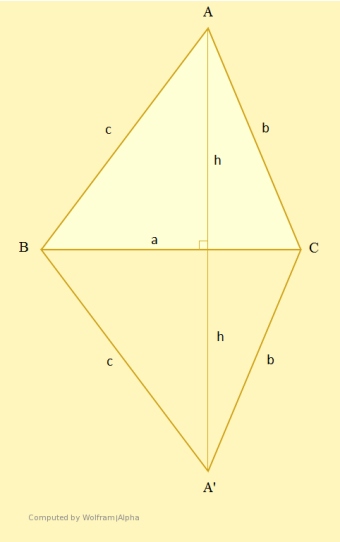


Figura 10: Conjunto entero de 4 puntos A,B,C y A'

No daremos una demostración, pues está claro que las distancias son enteras. Es más, puesto que el triángulo $ABC$ es no rectángulo, se comprueba que en $S$ no hay 3 puntos en una recta (claramente) ni 4 en una circunferencia. Si hubiesen 4 en una circunferencia, el lado $a$ resultaría ser el diámetro de la circunferencia, por lo que el ángulo $\widehat{CAB}$ sería un ángulo recto.

Utilizando este método podemos obtener un conjunto entero de 4 puntos con diámetro mínimo, que recordemos que era 8. Primero, tomamos dos copias (simétricas) del famoso triángulo de Pitágoras de lados $3, 4$ y $5$, y los adherimos a ambos por el lado que mide 4 para obtener un triángulo Heroniano de altura 4, base 6 y dos lados iguales de 5. Con el mismo procedimiento de antes, unimos por la base 2 copias (simétricas) del triángulo Heroniano, siendo la base un eje de simetría. Por el razonamiento anterior, obtenemos un conjunto entero de 4 puntos donde el diámetro viene dado por la suma de las alturas $4 + 4 = 8$.

Visto lo anterior, uno se pregunta qué pasa si adherimos dos triángulos Heronianos que no sean copias. En [14], ponen a prueba computacionalmente esta idea. Para todos los triángulos Pitagóricos generados a partir de $n, m \leq 128$ en las fórmulas aportadas en 2.1.2 para generar Ternas Pitagóricas, realizan las posibles adhesiones de dos de estos triángulos para así generar Triángulos Heronianos. Una vez han conseguido esto, realizan todas las combinaciones de dos triángulos Heronianos

uniéndolos por un lado y comprobando si el resultado es un conjunto entero de 4 puntos. Realizando una unión similar de conjuntos enteros hasta de 6 puntos, se han obtenido 25 nuevos conjuntos enteros de 7 puntos. No obstante, en el último documento al que hemos hecho referencia [14], los conjuntos tienen un requisito añadido. Deben ser $n$-clusters, una propiedad que veremos inmediatamente.

### 3.3.3. $n$-Clusters

**Definición 3.3.3.1.** Un $n$-cluster, con $n > 1$, es un conjunto de $n$ puntos del plano con coordenadas enteras, distancias enteras entre todos los puntos del conjunto y sin haber 3 puntos alineados ni 4 en una circunferencia.

Por lo tanto, los $n$-cluster son el resultado de imponer la condición de coordenadas enteras a los puntos de un conjunto entero. Esto facilita notablemente nuestro recuento y búsqueda de estos conjuntos, aunque ( como posiblemente cabría esperar ) parece aumentar drásticamente el diámetro mínimo entre los $n$-clusters, que notaremos $\dot{d}_c(2, n)$;

$$\begin{aligned} \dot{d}_c(2,3) &= 5 \\ \dot{d}_c(2,4) &= 8 \\ \dot{d}_c(2,5) &= 78 \\ \dot{d}_c(2,6) &= 1886 \\ \dot{d}_c(2,7) &= 2262000 \end{aligned}$$

Por otro lado, tan solo vemos ese fuerte incremento del diámetro mínimo para $n = 6$ y $n = 7$ en comparación con los conjuntos enteros. Esta información junto con mucha más referente a los $n$-clusters y $n_m$-clusters ( con definiciones ) viene facilitada en [9].

Hay una diferencia fundamental a la hora de buscar $n$-clusters y conjuntos enteros. Los $n$-clusters, están formados por la unión de triángulos Heronianos. Es decir, todos tres puntos de un $n$-cluster, son los vértices de un triángulo Heroniano. La razón, se halla en que los puntos de los $n$-clusters tienen coordenadas enteras, y por el *Teorema de Pick* [20], un tal triángulo tiene área racional ( o entera aumentando el $n$-cluster si es necesario ). Por lo tanto, a partir del método descrito anteriormente, de unir triángulos Heronianos para generar $n$-clusters, podemos obtener cualquier $n$-cluster. De esta forma, se han podido encontrar más de 1000 7-clusters en 2013 [7].

### 3.3.4. Conjuntos enteros de $\mathbb{Z}_m^2$

Explicaremos una última estrategia usada con el fin de determinar la no existencia de $n$-clusters, o alentar la búsqueda de éstos. Se trata de 'relajar' el problema de encontrar subconjuntos finitos de $\mathbb{Z}^2$ con distancias enteras y en posición general, al problema de encontrar estos subconjuntos pero en $\mathbb{Z}_m^2$ para un $1 < m \in \mathbb{N}$ [6]. Antes de buscar este tipo de conjuntos, debemos dar unas definiciones;

**Definición 3.3.4.1.** Dos puntos $(a, b), (c, d) \in \mathbb{Z}_m^2$ están a distancia entera si existe un número $d \in \mathbb{Z}_m$ tal que $(a - c)^2 + (b - d)^2 = d^2$

**Definición 3.3.4.2.** Tres puntos $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in \mathbb{Z}_m^2$ están alineados si existen $a, b, t_1, t_2, w_i \in \mathbb{Z}_m$ tal que $a + w_i t_1 = a_i$ y $b + w_i t_2 = b_i$ para $1 \leq i \leq 3$.

**Definición 3.3.4.3.** Quatro puntos $(a_1, b_1), ..., (a_4, b_4) \in \mathbb{Z}_m^2$ están sobre una circunferencia si existen $a, b \in \mathbb{Z}_m, r \in \mathbb{Z}_m \backslash \{\bar{0}\}$ tal que $(a_i - a)^2 + (b_i - b)^2 = r^2 \ \forall i$.

Es decir, queremos subconjuntos de $\mathbb{Z}_m^2$ con cada par de puntos a distancia entera y sin haber 3 puntos alineados ni 4 sobre una circunferencia, que llamaremos también conjuntos enteros ( de $\mathbb{Z}_m^2$ ). Denotamos $I(m, 2)$ al máximo número de puntos que forman un conjunto entero de $\mathbb{Z}_m^2$. La búsqueda de estos conjuntos es menos costosa por la reducción de módulo, lo que permite simular muchos más conjuntos. Por ejemplo, se ha llegado a demostrar que $I(50, 2) \geq 12$ y $I(61, 2) \geq 9$ a partir de conjuntos explícitos. Esto no tiene por qué implicar que exista, por ejemplo, un 9-cluster, pero nos deja la posibilidad de que así sea.

# 4. El Problema de Ulam

Nos toca hablar del Problema de Ulam. Ahora, nuestros conjuntos no tienen por qué estar en posición general. Además, las distancias entre los puntos del conjunto serán racionales. Nos referiremos a estos conjuntos como conjuntos racionales. Y por supuesto, tendremos una infinidad de puntos. Por otro lado, el problema pregunta sobre la existencia de un conjunto racional denso en el plano. Después de las ataduras en los conjuntos del anterior capítulo, puede parecer que numerosos conjuntos racionales deberían aparecer frente a nuestros ojos. Sin embargo, otras restricciones se nos presentarán. Por ejemplo, recordemos que al inicio del capítulo anterior, hemos visto que un conjunto infinito con todas las distancias enteras, debe caer sobre una recta. Para empezar este capítulo, nos contentaremos con estudiar conjuntos racionales sobre la recta que sean densos en ésta. Posteriormente, trataremos de ampliar el horizonte.

## 4.1. El caso de las rectas

Nos disponemos a dar conjuntos racionales sobre una recta y denso en ésta. O mejor, dado un conjunto $S$ con un solo punto $p$ y una recta $r$ con $p \in r$, trataremos de añadir a $S$ tantos puntos de la recta como nos sea posible, consiguiendo que $S$ sea un conjunto racional y denso en la recta. El caso básico por el que empezar, podría ser la recta $y = 0$ del plano, y supondremos que $(0, 0) = O$ pertenece a $S$. Los puntos que decidamos añadir serán $(a, 0) \in \mathbb{R}^2$, que por lo tanto restarán a distancia $a$ del punto inicial $O$. En otras palabras, $a$ debe ser racional. Claramente, la implicación contraria es también cierta, pues sea $(b, 0)$ con $b \in \mathbb{Q}$, este punto puede ser añadido a $S$ ya que la distancia a otro punto $(a, 0) \in S$ será $|b - a| \in Q$. Estamos listos para definir nuestro conjunto racional, pues es;

$$S = \{(a, 0) \in \mathbb{R}^2 \mid a \in \mathbb{Q}\}$$

$S$ es denso en la recta $y = 0$, puesto que los racionales son densos en la recta real. Además, sea $S'$ un conjunto racional sobre la recta $y = 0$ y denso en ésta que contenga el punto $O$. Por construcción de $S$, se cumple $S' \subseteq S$. Por supuesto, no es necesario que $S'$ sea igual a $S$, pues $S'$ puede ser por ejemplo $S' = S \backslash \{O\}$ o $S' = \{(\frac{n}{m}, 0) \in \mathbb{Q}^2 \mid mcd(n, m) = 1,\ m \neq 2\}$. Podemos seguir quitando puntos al conjunto, muchos, mientras siga siendo denso. Digamos $S' = \{(\frac{n}{m}, 0) \in \mathbb{Q}^2 \mid mcd(n, m) = 1,\ 2 \nmid m\}$. Este último conjunto, al que le hemos quitado todos los racionales con denominador par en la primera coordenada, es denso en la recta $y = 0$, pues una manera de verlo consiste en ver que entre dos racionales cualesquiera con denominador par ( con numerador y denominador coprimos ), siempre existe un racional con denominador impar.

Supongamos ahora, que tenemos un conjunto racional $T$ sobre una recta cualquiera $r$ del plano y denso en $r$. Razonablemente, podemos rotar el plano hasta que $r$ sea paralela al eje $x$, y después, podemos transportar $r$ para que un punto cualquiera de $T$ se identifique con $O$. Por supuesto, ni rotar ni transportar modifica las distancias entre los puntos de $T$, ya que son isometrías. Llamaremos $T'$ al conjunto

$T$ después de realizar las isometrías descritas. Claramente, tras llevar a cabo las isometrías, la recta $r$ pasa a ser la recta $y = 0$ y el punto $O$ pertenece a $T'$. De esta manera, nos damos cuenta de que $T' \subseteq S$. Así que tenemos una idea clara de la distribución de los puntos en $T$.

Un conjunto racional denso en una recta, no tiene por qué estar fromado únicamente por puntos sobre la recta. En la sección 4.3, veremos que si un conjunto racional descansa sobre una recta en una infinidad de puntos, entonces todos los puntos del conjunto, excepto posiblemente un máximo de 4 puntos, pertenecen a la recta. Por lo tanto, si queremos dar un conjunto racional denso en la recta $y = 0$ distinto a los que hemos dado antes, debe tener una finitud de puntos que caigan sobre la recta.

## 4.2. El caso de las circunferencias. La inversión

Si recordamos la sección 3.2, habíamos dado un conjunto de $n$ puntos sobre la circunferencia con distancias enteras entre los $n$ puntos. Entonces, permitiendo que las distancias sean racionales, se puede seguir el mismo ejemplo para dar infinitos puntos sobre la circunferencia de diámetro 1 que forman un conjunto racional. Quedaría discutir si el conjunto es denso en la propia circunferencia.

Es muy importante, ya que haremos uso de ello a menudo sin dar muchas explicaciones, darse cuenta de que podemos aplicar isometrías a cualquier conjunto racional $S$, como por ejemplo, rotar alrededor de un punto o transportar, sin afectar a la racionalidad de las distancias. Además de las isometrías, podemos también realizar homotecias de factor $\lambda$ racional, ya que en consecuencia las distancias obtenidas serán las anteriores multiplicadas por $\lambda$. Aplicando estas transformaciones, podemos desplazar cualquier conjunto racional y obligar a su imagen a contener dos puntos cualquiera a distancia racional, siendo el conjunto imagen un conjunto racional.

Las anteriores transformaciones, no son las únicas que preservan la racionalidad de las distancias entre los puntos de un conjunto racional. A continuación, veremos qué es una inversión [19], recurso que nos permitirá dar conjuntos racionales densos sobre la recta a partir de uno denso sobre la circunferencia, y lo opuesto, conjuntos racionales densos sobre la circunferencia a partir de uno denso sobre la recta.

**Definición 4.2.0.4.** Una *inversión* de radio $k$ y centro de inversión $O = (x_0, y_0) \in \mathbb{R}^2$, es una transformación continua y biyectiva de $\mathbb{R}^2$ en $\mathbb{R}^2$, que envía un punto $P = (x, y)$ al punto $P' = (x', y')$ tal que;

$$\begin{cases} x' &= x_0 + \frac{k^2(x-x_0)}{(x-x_0)^2+(y-y_0)^2} \\ y' &= y_0 - \frac{k^2(y-y_0)}{(x-x_0)^2+(y-y_0)^2} \end{cases}$$

Puede parecer una definición complicada, pero geométricamente cobra sencillez. Consideramos la circunferencia de centro $O$ y radio $k$, conocida como circunferencia

de inversión. Sea un punto $P$, su imagen $P'$ por la inversión de centro de inversión $O$ y radio $k$, viene representada en la figura 11;

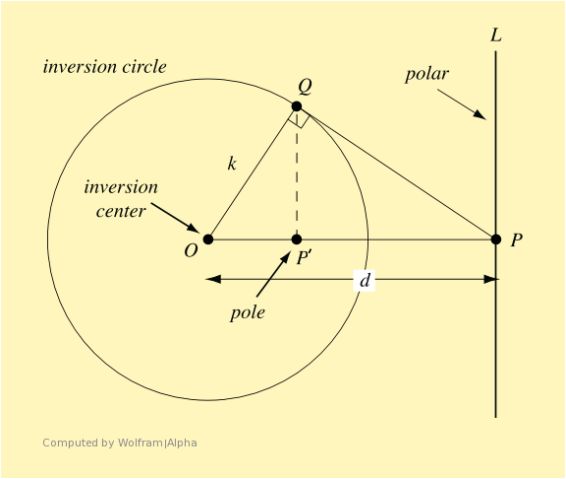


Figura 11: Inversión del punto $P$

Dejaremos a un lado el estudio de esta función, pues únicamente aprovecharemos algunas de sus propiedades.

**Propiedad.** La inversión de una recta que no pasa por el centro de inversión es una circunferencia que pasa por el centro de inversión sin contenerlo.

**Propiedad.** La inversión de una circunferencia que pasa por el centro de inversión es una recta que no pasa por el centro de inversión.

**Lema.** Sea $S$ un conjuntos racional y $x \in S$. La inversión de $S\backslash\{x\}$ de radio racional $k$ y de centro de inversión $x$ es un conjunto racional.

*Demostración.* Para verlo, nos será suficiente demostrarlo para $k = 1$ y centro de inversión $x = (0, 0) \in S$. En este caso, es más sencillo tomar la notación compleja, pues la inversión envía un punto $z$ al punto $\frac{1}{z}$. Sean $z_1, z_2 \in S$, se cumple que $|z_1|, |z_2|, |z_1 - z_2| \in \mathbb{Q}$. Por lo tanto, nos damos cuenta de que;

$$\left|\frac{1}{z_1} - \frac{1}{z_2}\right| = \left|\frac{z_2 - z_1}{z_1 z_2}\right| = \frac{|z_2 - z_1|}{|z_1||z_2|} \in \mathbb{Q}$$

□

Por lo tanto, esto último nos asegura la preservación de la racionalidad de las distancias al realizar una inversión. Utilizaremos este lema en las próximas secciones. También nos traduce la propiedad de ser denso en una circunferencia, a ser denso en una recta. Poniendo en común las propiedades y el lema, decimos.

Un conjunto racional $S$ sobre la circunferencia es denso en ésta, si y solo si la imagen de $S$ por la inversión de radio racional $k$ con centro de inversión $x \in S$ es un conjunto racional denso en una recta.

## 4.3. El Teorema de Solymosi-de Zeeuw

En esta sección, queremos destapar propiedades de los conjuntos racionales densos en el plano, si existe alguno. La primera de estas sorprendentes propiedades, nos revelará que un conjunto racional denso en el plano, no puede coincidir en una infinidad de puntos con cualquier curva algebraica del plano, con la excepción de las rectas y circunferencias. De la segunda, deduciremos que un conjunto racional denso en el plano no puede tener infinitos puntos sobre una circunferencia o una recta, pues de lo contrario estarían todos sobre ésta ( menos posiblemente una finitud de puntos ). La llave maestra que utilizaremos para demostrar los siguientes teoremas, será un potente resultado que hemos enunciado en el capítulo 2.3.1: *El Teorema de Faltings*. Seguiremos fielmente la demostración de [16], aunque antes, observemos el siguiente lema [11].

**Lema.** Para todo conjunto racional $S$ existe un entero $k$ libre de cuadrados de manera que si una transformación envía dos puntos de $S$ a $(0,0)$ y $(1,0)$, entonces todo punto de la imagen de $S$ por la transformación es de la forma;

$$(r_1, r_2\sqrt{k}),\ r_1, r_2 \in \mathbb{Q}$$

Notar que si una curva contiene infinitos puntos de esa forma, entonces está definida sobre $\mathbb{Q}(\sqrt{k})$

*Demostración.* Sea $T$ el conjunto racional imagen de $S$ por las transformaciones que envían dos puntos de $S$ a $(0,0)$ y $(1,0)$. Queremos ver que existe un $k$ libre de cuadrados tal que todo punto de $T$ es de la forma $(r_1, r_2\sqrt{k})$ con $r_1, r_2 \in \mathbb{Q}$. Sea $P = (x_1, y_1)$ un punto cualquiera de $T$.

Sea $Q = (x_2, y_2)$ otro punto de $T$. Entonces los puntos $(0,0), P, Q$ forman un triángulo con lados racionales y por el *Teorema del Coseno* (que hemos enunciado en 2.1.3), el coseno de cualquier ángulo interno del triángulo es racional. Sean $\vec{P} = \overrightarrow{(x_1, y_1)}$ y $\vec{Q} = \overrightarrow{(x_2, y_2)}$. Recordemos la definición geométrica del producto escalar;

$$\vec{P} \cdot \vec{Q} = |\vec{P}||\vec{Q}|cos(\alpha),$$

donde $\alpha$ es el ángulo entre $\vec{P}$ y $\vec{Q}$. Pero $|\vec{P}|$ y $|\vec{Q}|$ son los lados del triángulo y $\alpha$ uno de sus ángulos internos, y por lo tanto $|\vec{P}|, |\vec{Q}|, \cos\alpha \in \mathbb{Q}$. Esto implica que $\vec{P} \cdot \vec{Q}$ es también racional. Dado que $(1,0) \in T$, podemos tomar $Q = (1,0)$ y por la definición algebraica del producto escalar;

$$\vec{P} \cdot \vec{Q} = x_1x_2 + y_1y_2 = x_1 + y_10 = x_1 \in \mathbb{Q}$$

Y entonces $x_1 = r_1$ con $r_1$ racional. Además, si $Q = (x_2, y_2) \in T$ y sabemos que debe ser $x_2 \in \mathbb{Q}$, entonces;

$$\vec{P} \cdot \vec{Q} = x_1x_2 + y_1y_2 \Longrightarrow y_1y_2 = \vec{P} \cdot \vec{Q} - x_1x_2 \in \mathbb{Q}$$

Es decir, que el producto de las coordenadas $y$ de dos puntos cualquiera $P, Q \in T$ es racional. Esto equivale a decir que existe un $k$ libre de cuadrados tal que $y_1 = r_2\sqrt{k}$ con $r_2$ racional. □

**Teorema 4.3.0.1.** Todo conjunto racional del plano coincide con una curva algebraica cualquiera únicamente en un subconjunto finito de puntos, excepto el caso en que la curva es una recta o una circunferencia

No daremos la demostración completa a este teorema, en su lugar, mostraremos el caso de las curvas de género $g \geq 2$ y daremos las ideas principales que se suceden, e invitamos a mirar [16] para una rigurosa demostración.

Supongamos que $S$ es un conjunto racional infinito y contenido en una curva $C$ de género $g \geq 2$. Mediante las transformaciones comentadas anteriormente, como el transporte y la homotecia, podemos mover dos puntos de $S$ a $(0,0)$ y $(0,1)$. Por el lema en 4.3, los puntos de $S$ son de la forma $(r_1, r_2\sqrt{k}),\ r_1, r_2 \in \mathbb{Q}$ para un cierto $k$. Por lo tanto, por haver infinitos puntos de esa forma sobre $C$, la curva está definida sobre $\mathbb{Q}(\sqrt{k})$. Podemos dilatar el eje $y$ con razón $\sqrt{k}$, lo cual implicaría que la infinidad de puntos de $S$, ahora racionales, pues son $(r_1, r_2)$ con $r_1, r_2 \in \mathbb{Q}$, pertenecen a la curva $C$ de género $g \geq 2$, en contradicción con el *Teorema de Faltings.* Es decir, $S$ no puede tener infinitos puntos sobre la curva $C$.

Supongamos ahora que $S$ es un conjunto racional infinito y contenido en una curva $C_1$ de género $g_1 = 1$ definida por la ecuación $f(x,y)$ de grado $d \geq 3$. Podemos suponer de nuevo, que los puntos $(0,0)$ y $(0,1)$ pertenecen a $C_1$ y $S$, donde $(0,0)$ no es un punto singular de $C_1$. La prueba en este caso, terminará cuando se demuestre que la curva $C_2$ de $\mathbb{R}^3$;

$$\begin{cases} f(x,y) &= 0 \\ x^2 + y^2 &= z^2 \end{cases}$$

es de género $g_2 \geq 2$. Esto implicaría que $S$ no puede ser infinito porque aplicando primero el lema, cada punto $(r_1, r_2\sqrt{k}),\ r_1, r_2 \in \mathbb{Q}$ de $S$ ( y por lo tanto de $C_1$ ) determina un punto de $C_2$ que es $(r_1, r_2\sqrt{k}, r_3)$, que dilatando el eje $y$ como antes, nos daría una infinidad de puntos racionales $(r_1, r_2, r_3)$ sobre una curva de género $g_2 \geq 2$ contradiciendo de nuevo el *Teorema de Faltings.*

La prueba de que el género $g_2 \geq 2$, se vale de la *Fórmula de Riemman-Hurwitz* recordando que $g_1 = 1$ y $d = 2$, y de la posterior demostración de la existencia de algún punto de ramificación.

Prosigue la demostración con las curvas de género 0, siguiendo la misma estrategia pero acrecentando la longitud y complejidad de los pasos.

**Teorema 4.3.0.2.** Si un conjunto racional $S$ tiene infinitos puntos sobre una recta ( respect. circunferencia ), entonces todos los puntos de $S$ excepto un máximo de 4 ( respect. 3) están sobre la recta (respect. circunferencia)

*Demostración.* Para la demostración, usaremos de nuevo el *Teorema de Faltings* sobre una curva hiperelíptica;

$$y^2 = \prod_{i=1}^{6}(x - \alpha_i),$$

que es de género 2 si y solo si las raíces $\alpha_i$ del polinomio de la parte derecha de la ecuación son diferentes.

Queremos ver, que si un conjunto $S$ tiene infinitos puntos sobre una recta, entonces todos los puntos de $S$ a excepción de un máximo de 4 puntos, descansan sobre la recta. Para ello, supongamos que el conjunto $S$ tiene infinitos puntos sobre una recta y 5 puntos fuera de ella. Sin perder generalidad, podemos decir que la recta es $y = 0$. Podemos suponer entonces, que en el semiplano superior ( por encima de la recta $y = 0$ ) hay 3 de esos 5 puntos, que podemos suponer que son $(0, 1), (a_1, b_1), (a_2, b_2)$. Sea $(x, 0) \in S$ un punto de la recta $y = 0$, con $x \neq 0, a_1, a_2$, entonces, por ser puntos de un conjunto racional y por el *Teorema de Pitágoras* se cumple;

$$\begin{aligned} d((x,0),(0,1))^2 &= x^2 + 1 \\ d((x,0),(a_1,b_1))^2 &= (x-a_1)^2 + b_1^2 \\ d((x,0),(a_2,b_2))^2 &= (x-a_2)^2 + b_2^2, \end{aligned}$$

con $d((x, 0), (0, 1)), d((x, 0), (a_1, b_1))$ y $d((x, 0), (a_2, b_2))$ racionales. Por lo tanto, para cada punto $(x, 0) \in S$, hallamos un punto racional $(x, y)$ solución de la curva algebraica;

$$y^2 = (x^2 + 1)((x - a_1)^2 + b_1^2)((x - a_2)^2 + b_2^2)$$

Si se demuestra que el género $g$ de la curva es 2, habremos acabado, pues por el *Teorema de Faltings*, es imposible que podamos hallar infinitos puntos racionales sobre la curva. Como hemos comentado al inicio de la demostración, es suficiente comprovar que las 6 raíces del polinomio $f(x) = (x^2+1)((x-a_1)^2+b_1^2)((x-a_2)^2+b_2^2)$ son diferentes. Observamos que, por ejemplo, $(x - a_1)^2 + b_1^2$ no tiene raíces reales, pues por ser $b_1 \neq 0$ la suma de dos reales positivos no puede anularse. Así, deducimos que cada uno de los factores de $f(x)$ tiene 2 raíces complejas conjugadas no reales. Puesto que cada factor tiene coeficiente 1 frente el término $x^2$, dos de los factores tendrán las mismas raíces si y solo si son idénticos. Expandiendo los tres factores, nos damos cuenta de que dos factores son idénticos si y solo si;

$$\begin{cases} & a_1 = a_2 \quad \text{y} \quad b_1 = b_2 \\ \text{o bien,} & \\ & a_i = 0 \quad \text{y} \quad b_i = \pm 1, \quad \text{donde } i \in \{1, 2\} \end{cases}$$

Pero como los tres puntos $(0, 1), (a_1, b_1), (a_2, b_2)$ son distintos y los tres están en el semiplano superior ( y fuera de la recta $y = 0$ ), podemos asegurar que las 6 raíces son distintas y que la recta tiene género 2.

Como habíamos dicho, esto contradice el *Teorema de Faltings*, y por lo tanto, solo un máximo de 2 puntos del conjunto racional $S$ puede caer en el semiplano superior. Con un argumento análogo, solo dos puntos de $S$ pueden pertenecer al semiplano inferior. Es decir, el conjunto $S$ tiene todos los puntos sobre la recta $y = 0$, exceptuando posiblemente un máximo de 4 puntos.

El caso de la circunferencia, se sigue de las propiedades de la inversión enunciadas en la anterior sección: Sea $S$ un conjunto racional con infinitos puntos sobre una

circunferencia y con 4 puntos o más fuera de ésta. Podemos suponer que el $(0,0)$ pertenece a la circunferencia y a $S$. Considereemos la inversión de centro $(0,0)$ y radio $k$ racional. Por las propiedades de la inversión, el conjunto imagen $T$ de $S\backslash\{(0,0)\}$ es un conjunto racional sobre una recta $r$, con infinitos puntos sobre la recta y almenos 4 puntos fuera de ella. Para acabar, podemos añadir el punto $(0,0)$, que no pertenece ni a $r$ ni a $T$, al conjunto racional $T$. $T \cup \{(0,0)\}$ resulta ser un conjunto racional con infinitos puntos sobre una recta y almenos 5 puntos fuera de ella, en contradicción a lo que hemos visto antes. Para ver que el conjunto $T \cup \{(0,0)\}$ es racional, recordemos que $z \in S$ tenía distancia racional a $(0,0)$, y entonces, la distancia de la imagen de $z$ por la inversión al punto $(0,0)$, es $\frac{1}{|z|} \in \mathbb{Q}$. Es decir, la distancia de cualquier punto de $T$ a $(0,0)$ es racional.

□

Hagamos una conclusión de la sección; si existiese un conjunto racional $S$ denso en el plano, aún teniendo que contener una seria cantidad de puntos del plano para lograr la propiedad de densidad, no puede coincidir con una curva algebraica en una infinidad de puntos. El conjunto $S$ tiene una forma bastante concisa y especial, pues debe evitar caer en una infinidad de puntos sobre cualquier recta, circunferencia o curva algebraica en general existente en el plano.

## 4.4. El teorema de Huff

En esta sección responderemos a una duda que ha podido surgir al comprovar los teoremas de 4.3. ¿Existe realmente un conjunto racional con infinitos puntos sobre una recta y exactamente 4 puntos fuera de ella? Por extraño que pueda parecer, 4 es el límite de puntos que pueden caer fuera de la recta, y en efecto, por los teoremas en [10], existen infinitos ejemplos que lo demuestran. Para ello, además de algunos lemas, definiciones y teoremas que nos disponemos a dar, vamos a necesitar algunas propiedades y resultados sobre curvas elípticas, proporcionados en 2.2 y 2.2.5, como el grupo geométrico existente en las curvas elípticas o el *Teorema de Mordell*.

Antes de nada, damos la ecuación de una curva elíptica $C$ con la que trabajaremos toda la sección, que ilustramos con la figura 12. La ecuación de $C$ es;

$$ax(y^2-1) - by(x^2-1) = 0 \quad [1]$$

Como hemos visto en 2.2, una recta tangente a $C$ por un punto $(x,y) \in C$, interseca con $C$ en un ( posiblemente nuevo ) punto $(x_1, y_1)$. Huff realizó los cálculos y nos proporciona las ecuaciones;

$$\begin{cases} x_1 = \frac{2x(y^2+1)}{(x^2+1)(y^2-1)} \\ y_1 = \frac{2y(x^2+1)}{(y^2+1)(x^2-1)} \end{cases}$$

para localizar el punto $(x_1, y_1)$ a partir de $(x,y) \in C$. Claramente, y como ya sabíamos, si $(x,y)$ es racional, entonces $(x_1, y_1)$ también los es. Al punto $(x_1, y_1)$ lo

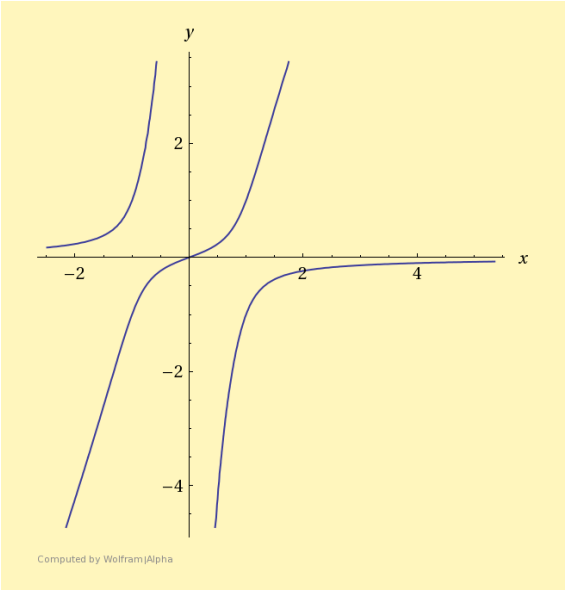


Figura 12: Curva de ecuación [1] con $a = 3$,$b = 8$

llamaremos tangencial de $(x, y)$ sobre la curva $C$. Demos más herramientas de las que posteriormente haremos buen uso;

**Definición 4.4.0.5.** Una valoración $v$ es una aplicación de un cuerpo $(K, +, \cdot)$ en un cuerpo totalmente ordenado $M \cup \{\infty\}$ que cumple las siguientes propiedades;

- $v(a) = \infty \iff a = 0$.
- $v(ab) = v(a) + v(b)$.
- $v(a + b) \geq \text{mín}\{v(a), v(b)\}$ con igualdad si $v(a) \neq v(b)$.

Vamos a necesitar la valoración 2-ádica, que notaremos simplemente $v$ y se define;

$$\begin{array}{rccl} v: & \mathbb{Q} & \longrightarrow & \mathbb{Z} \cup \{\infty\} \\ & x \neq 0 & \longmapsto & t \\ & 0 & \longmapsto & \infty, \end{array}$$

donde $x = \left(\frac{n}{m}\right) 2^t$ con $n, m, p \in \mathbb{Z}$, y $mcd(n, 2) = 1 = mcd(m, 2)$. Se comprueba que $v$ es una valoración. Podemos ver que $v(x) = 0$ solo si $x = \frac{n}{m}$ con $n$ y $m$ enteros impares. Además, de la definición, se observa que ;

**Lema.** Sean $a, b \in \mathbb{Z}\backslash\{0\}$. Si $v(a) = v(b)$ entonces $v(a + b) > v(a)$

*Demostración.* Como $v(a) = v(b) = t$, tenemos $a = \frac{n_1}{m_1} 2^t$ y $b = \frac{n_2}{m_2} 2^t$ con $n_1, m_1, n_2, m_2 \in \mathbb{Z}$ todos impares. Por lo tanto;

$$v(a + b) = v(2^t(\tfrac{n_1 m_2 + n_2 m_1}{m_1 m_2})) = v(2^t) + v(\tfrac{n_1 m_2 + n_2 m_1}{m_1 m_2}) = t + v(\tfrac{n_1 m_2 + n_2 m_1}{m_1 m_2})$$

Solo tenemos que ver que $v(\frac{n_1m_2+n_2m_1}{m_1m_2}) > 0$. Basta observar que el numerador es suma de dos números impares y el denominador es impar, y entonces;

$$v(\tfrac{n_1m_2+n_2m_1}{m_1m_2}) = v(2(\tfrac{k}{m_1m_2})) = v(2) + v(\tfrac{k}{m_1m_2}) = 1 + v(\tfrac{k}{m_1m_2}) > 0$$

□

**Teorema** (1)**.** Sea $(x, y)$ un punto racional de $C$. Entonces los puntos $(-x, -y)$, $(\pm x, \mp\frac{1}{y})$, $(\pm\frac{1}{x}, \mp y)$ y $(\pm\frac{1}{x}, \pm\frac{1}{y})$ son también racionales de $C$.

**Teorema** (2)**.** Los puntos $(x, y), (-x, \frac{1}{y}), (\frac{1}{x}, -y)$ y $(-\frac{1}{x}, -\frac{1}{y})$ tienen la misma tangencial $(x_1, y_1)$.

No probaremos estos dos teoremas, aunque uno podría entretenerse en sustituir los puntos del teorema 1 en la ecuación de $C$, y los puntos del teorema 2 en las ecuaciones de Huff de la tangencial para corroborar la veracidad de los dos resultados. De la misma manera, se puede comprobar, que los puntos mencionados en el teorema 1 que no aparecen en el teorema 2, tienen también la misma tangencial entre ellos y la tangencial opuesta en signo respecto a los del teorema 2.

**Observación.** Las valoraciones por medio de $v$ de las coordenadas de las tangenciales de los puntos del Teorema 1 coinciden.

**Teorema 4.4.0.3.** Si $(x, y)$ es un punto racional de $C$ con $v(x) \neq 0 \neq v(y)$, entonces hay infinitos puntos racionales sobre la curva $C$.

*Demostración.* Para empezar, podemos considerar que $v(x) > 0$ y $v(y) > 0$, pues si por ejemplo fuese $v(x) < 0$ y $v(y) > 0$, de los teoremas 1 y 2 deducimos que el punto $(\frac{1}{x}, -y)$ es también un punto racional de $C$ con $v(\frac{1}{x}) \neq 0 \neq v(-y)$. Pero además es $v(\frac{1}{x}) = -v(x) > 0$, y $v(-y) = v(y) > 0$ por lo que tomaríamos éste como punto de partida.

De las ecuaciones de Huff para la tangencial, sabemos que;

$$x_1 = \frac{2x(y^2+1)}{(x^2+1)(y^2-1)}$$

Aplicando la valoración $v$ a la ecuación obtenemos;

$$\begin{aligned} v(x_1) &= v(\tfrac{2x(y^2+1)}{(x^2+1)(y^2-1)}) \\ &= v(2x(y^2+1)) - v(x^2+1) - v(y^2-1) \\ &= v(2) + v(x) + v(y^2+1) - v(x^2+1) - v(y^2-1) \quad = 1 + v(x) \\ &> v(x). \end{aligned}$$

Aclaramos que es por la propiedad de la valoración de la suma, y de que $v(1) = 0$, que decimos que $v(y^2+1) = v(x^2+1) = v(y^2-1) = 0$. De la misma manera, $v(y_1) > v(y)$. Por lo tanto, $(x, y) \neq (x_1, y_1)$ pero además, $v(x_1) > v(x) > 0$ y $v(y_1) > v(y) > 0$, por lo que el punto $(x_1, y_1)$ cumple las condiciones del teorema. Podemos repetir el proceso para $(x_1, y_1)$ encontrando un punto racional distinto

$(x_2, y_2)$ de la curva $C$. Puesto que podemos repetir este proceso infinitas veces, obtenemos infinitos puntos racionales $(x_i, y_i)$ $\forall i \in \mathbb{N}$ sobre la curva $C$.

□

El siguiente teorema pretende lo mismo que el anterior: asegurar la existencia de infinitos puntos racionales sobre $C$ a partir de un punto racional $(x, y) \in C$ que cumple unas ciertas condiciones.

**Teorema 4.4.0.4.** Si $(x, y)$ es un punto racional de la curva $C$ con $v(x) = v(y) = 0$ y $(x, y) \neq (\pm 1, \pm 1)$, entonces existen infinitos puntos racionales sobre la curva $C$.

*Demostración.* Podemos reescribir las coordenadas de la siguiente manera;

$$\begin{cases} x &= 2k_1 + \frac{1}{2k2} + 1 \\ y &= 2k_3 + \frac{1}{2k4} + 1 \end{cases}$$

con $k_i \in \mathbb{Z}$ $\forall i$. De lo anterior, se comprueba que $v(x^2+1) = v(y^2+1) = 1$ y que $v(x^2-1) \geq 2$ $v(y^2-1) \geq 2$. De la misma manera que en la demostración del teorema anterior, vemos;

$$\begin{aligned} v(x_1) &= v(2) + v(x) + v(y^2+1) - v(x^2+1) - v(y^2-1) \\ &< 0. \end{aligned}$$

□

En la referencia citada anteriormente en este capítulo [10] hay además otro teorema junto con un lema, con el que encontramos más situaciones en las que $C$ tiene infinitos puntos racionales, cumplidas unas condiciones.

Tan solo queda dar un último resultado que nos aclarará la importancia de hallar infinitos puntos racionales sobre $C$.

**Teorema 4.4.0.5.** Si $(x, y)$ es un punto racional de $C$, entonces las distancias entre el punto $\left(\frac{2by}{y^2-1}, 0\right)$ y los puntos $(0, \pm a)$ y $(0, \pm b)$ son racionales.

*Demostración.* Recordemos que el punto $(x, y)$ es un punto racional de $C$, y en consecuencia satisface la ecuación de la curva;

$$ax(y^2-1) - by(x^2-1) = 0$$

por lo que deducimos que;

$$by(x^2-1) = ax(y^2-1)\,[1]$$

Queremos comprovar, que la distancia $d$ de $\left(\frac{2by}{y^2-1}, 0\right)$ a $(0, a)$ es racional, es decir, que;

$$\left(\frac{2by}{y^2-1}\right)^2 + a^2 = d^2,$$

para algún racional $d$. Primero, hacemos lo siguiente;

$$\left(\frac{(x^2-1)2by}{(x^2-1)(y^2-1)}\right)^2 + a^2 = d^2,$$

y sustituimos [1] en la ecuación;

$$\frac{4a^2x^2}{(x^2-1)^2} + a^2 = d^2,$$

Extraemos factor común de $a^2$ y sumamos las fracciones usando el denominador común.

$$a^2\left(\frac{4x^2+(x^2-1)^2}{(x^2-1)^2}\right) = d^2$$

Observamos que $4x^2 + (x^2-1)^2 = 4x^2 + x^4 - 2x^2 + 1 = x^4 + 2x^2 + 1 = (x^2+1)^2$.

$$\left(a\frac{(x^2+1)}{(x^2-1)}\right)^2 = d^2$$

Lo que demuestra que la distancia $d$ es racional. De forma muy similar, se demuestra que la distancia de $\left(\frac{2by}{y^2-1}, 0\right)$ a $(0, b)$ también es racional. No es necesario probarlo para los puntos $(0, -a)$ y $(0, -b)$, pues por simetría son puntos situados a la misma distancia que $(0, a)$ y $(0, b)$ respectivamente.

□

Es decir, que si la curva elíptica $C$ posee una infinidad de puntos racionales distintos $(x_i, y_i)$ $\forall i \in \mathbb{N}$, podemos construir el conjunto racional

$$S = \left\{\left(\frac{2by_i}{y_i^2-1}, 0\right) \in \mathbb{Q}^2 \mid (x_i, y_i) \in C(\mathbb{Q})\right\} \cup \{(0, \pm a)\} \cup \{(0, \pm b)\},$$

que tiene infinitos puntos sobre la recta $y = 0$ y 4 puntos fuera de ella.

# Conclusión

Los puntos racionales sobre curvas algebraicas nos han proporcionado numerosos resultados relacionados con los conjuntos enteros y racionales, aunque en un principio pudiesen parecer dos estudios sin demasiado en común. Para *El Problema de Erdös*, hemos visto la puesta en práctica computacional de métodos exhaustivos que nos daban conjuntos enteros, y otros métodos más efectivos que construyen sucesivamente los $n$-clusters a partir de la adhesión de triángulos Heronianos. Incluso hemos visto que todo $n$-cluster puede ser obtenido con ese método. Y en cuanto a *El Problema de Ulam*, se ha logrado descartar que un conjunto racional denso en el plano, pueda intersecar en una infinidad de puntos con cualquier curva algebraica imaginable. Curiosamente, mientras que los conjuntos enteros infinitos caen sobre una recta, los conjuntos racionales con infinitos puntos sobre una recta permiten un máximo de 4 puntos fuera de ella.

No quisiera acabar, sin decir que hay más temas interesantes relacionados de los que se podían haber hablado, pero que excedían los límites del trabajo, ya sea por el número de páginas, ya sea por el nivel de dificultad. Por ejemplo, el artículo [11] del profesor Jafar Shaffaf o independientemente el trabajo del profesor Terence Tao [17], donde se demuestra *El Problema de Ulam* asumiendo *La Conjetura de Bomberi-Lang*. Otro ejemplo, sería el referente a *La Conjetura de Harborth*, que asegura que todo grafo plano puede dibujarse con todas las aristas enteras y sin intersecciones entre éstas. Esta conjetura resulta ser cierta asumiendo como falso *El Problema de Ulam*. Reservamos los capítulos de un posible trabajo posterior para incluir estos resultados.

Tras finalizar el trabajo, he conseguido respuestas a muchas preguntas que a un ignorante del tema como yo le abordan sin compasión en un inicio. Aunque saciar este hambre trae consigo más hambre: ¿Qué tipo de conjuntos enteros de $n$ puntos perdemos de vista al reducir nuestra busqueda a los $n$-clusters? ¿Qué métodos se han llevado a cabo para encontrar un conjunto entero de 8 puntos? ¿Pueden algunos conjuntos enteros ser la proyección en $\mathbb{R}^2$ de ciertos conjuntos de $\mathbb{R}^3$ mucho más simétricos o comprensibles?

En resumen, no nos faltan preguntas, capítulos ni motivos para un futuro trabajo.

# Anexo

## A. Ejemplos de Conjuntos Enteros

En esta sección, damos algunos conjuntos enteros y $n$-clusters, encontrados a partir de búsquedas con ordenadores usando las técnicas y métodos explicados antes: la búsqueda por diámetros, la unión de triángulos Pitagóricos y Heronianos y los $n$-clusters de $\mathbb{Z}_m^2$, mirar [7, 9, 14, 15]. En ocasiones, estimular la intuición visualizando ejemplos, es un buen primer paso antes de ponerse a buscar conjuntos enteros. Para empezar, demos el conjunto entero de 7 puntos con diámetro mínimo.

$$(0,0),(22270,0),(\tfrac{26127018}{2227},\tfrac{932064}{2227}\sqrt{2002}),(\tfrac{245363}{17},\tfrac{3144}{17}\sqrt{2002}),(\tfrac{17615968}{2227},\tfrac{238464}{2227}\sqrt{2002}),$$

$$(\tfrac{56068}{17},\tfrac{3144}{17}\sqrt{2002}),(\tfrac{19079044}{2227},\tfrac{-54168}{2227}\sqrt{2002})$$

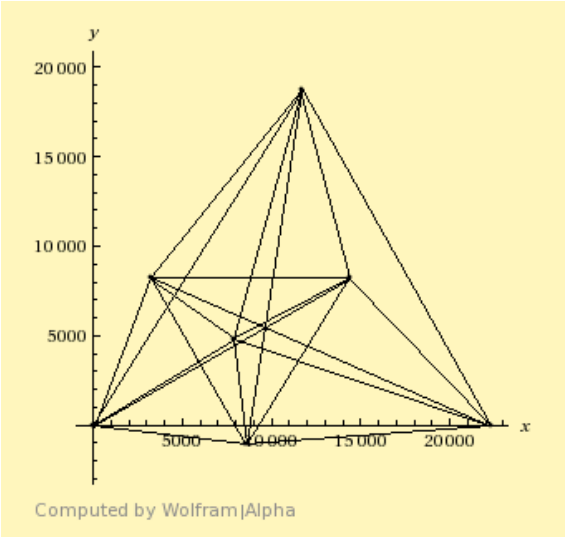


Figura 13: conjunto entero de 7 puntos con diámetro mínimo ( $\dot{d}(2,7) = 22270$ )

A continuación, vemos los $n$-clusters con diámetro más pequeño encontrados.

(0,0) (3,4) (3,-4) (6,0)

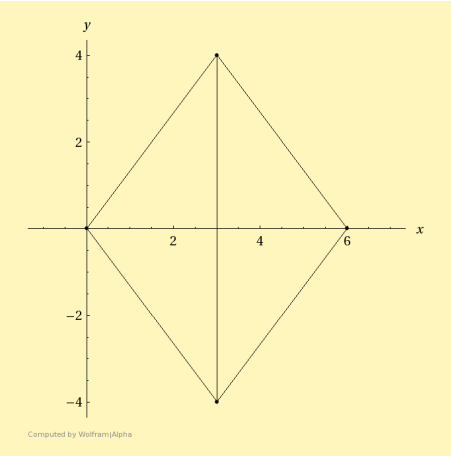


Figura 14: 4-cluster con diámetro mínimo ( $\dot{d}_c(2,4) = 8$ )

(0,0) (16,30) (-16,30) (0,-33) (56,0)

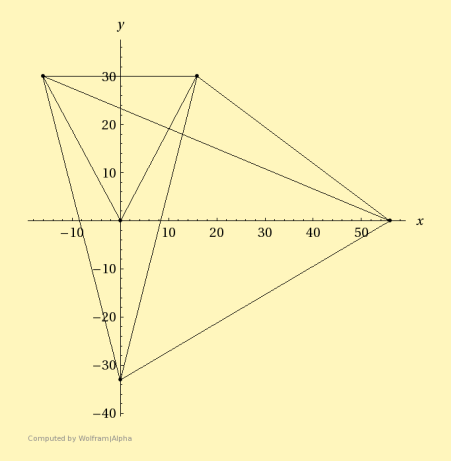


Figura 15: 5-cluster con diámetro mínimo ( $\dot{d}_c(2,5) = 78$ )

$(0,0), (132,-720), (546,-272), (960,-720), (1155,540), (546,1120)$

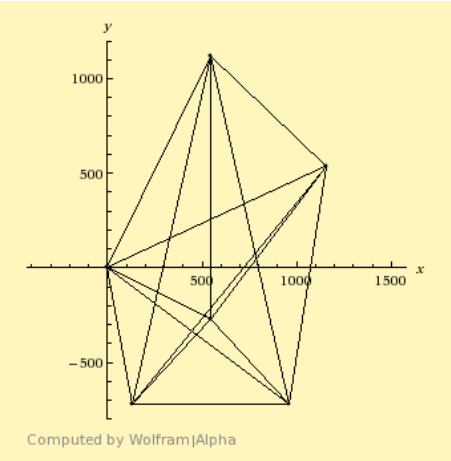


Figura 16: 6-cluster con diámetro mínimo ( $\dot{d}_c(2,6) = 1886$ )

(0,0) (374400,-2230800) (1081600,-1488240) (-453024,-1630200) (426725,-1630200) (569088,-1291680) (-439040,-1308720)

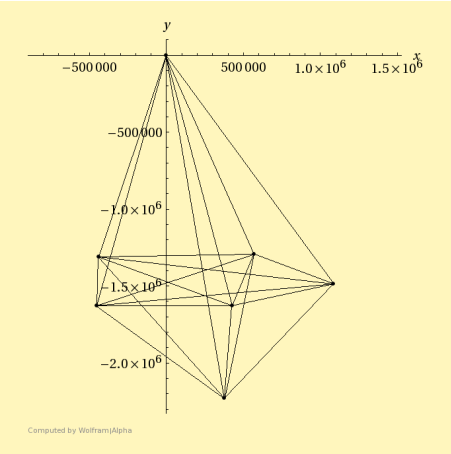


Figura 17: 7-cluster con diámetro mínimo ( $\dot{d}_c(2,7) = 2262000$ )

Sigamos con unos cuantos ejemplos de 7-clusters:

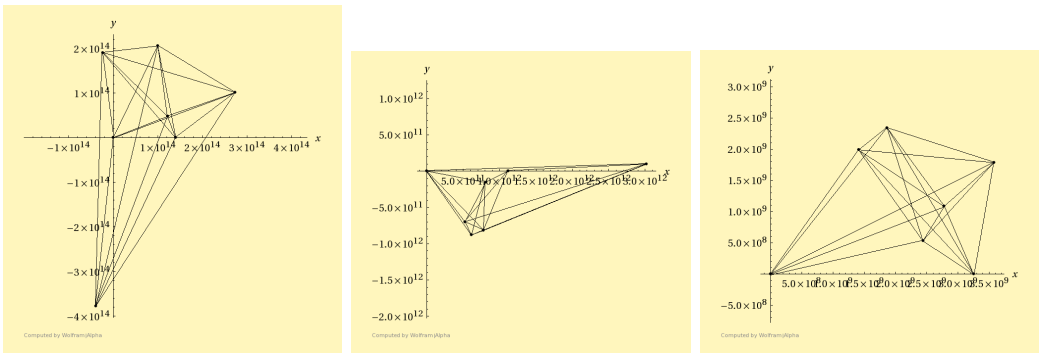

Figura 18: 7-clusters

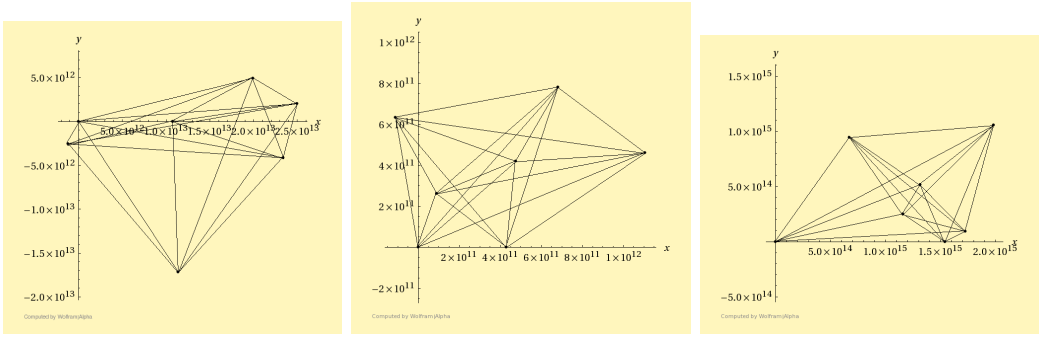

Figura 19: 7-clusters

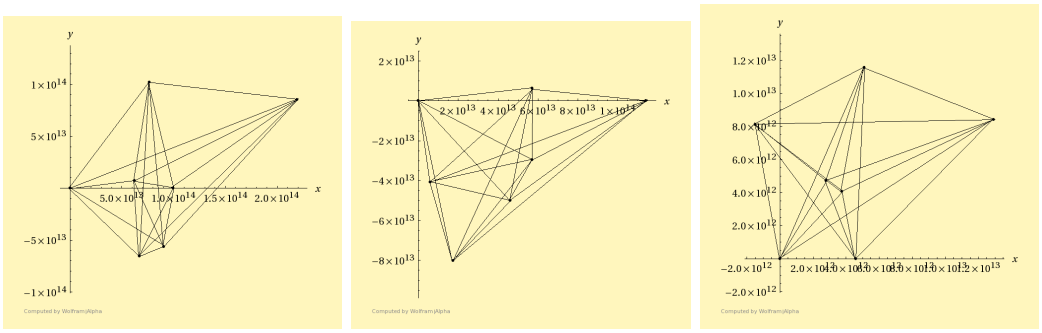

Figura 20: 7-clusters

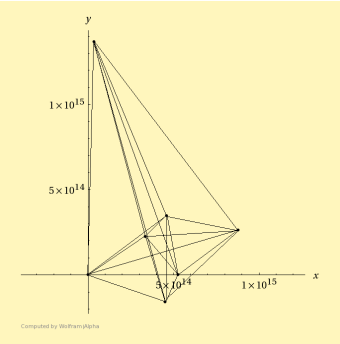


Figura 21: 7-clusters

Recomiendo ojear más conjuntos en las referencias especificadas antes [15].

## B. Aplicaciones

Hemos hablado de subconjuntos de puntos de $\mathbb{R}^2$, distancias enteras, linealidad y más conceptos presentes en nuestro universo, desde en la situación de los planetas en el espacio hasta en un tablero de ajedrez. Por ello, decidí plantear algún caso hipotético en el que el estudio realizado supuestamente pudiese tener alguna aplicación práctica.

Pensemos en antenas emisoras de alguna onda, que hay que distribuir por algún terreno. Con tal de ampliar el radio de la señal con el mínimo número de antenas, evitaremos alinear 3 antenas. Además, cada antena funciona como un repetidor de señal, que recibe y rebota la onda a las demás antenas, y por ello, la distancia entre antenas debe ser un cierto número múltiplo acorde con la longitud de onda, para así una mejor recepción de la señal y aumentar su calidad. Este problema requiere de un conjunto entero para su solución, aunque permitimos que 4 antenas estén en una misma circunferencia.

Cuando vi este ejemplo planteado en uno de los artículos que ojeé [8], me envalentoné para pensar en otros ejemplos inventados:

Visualizamos el monitor de un controlador aéreo, en el que los puntos de la pantalla representan aviones en movimiento en un plano. Puede ser que en ese momento los aviones estén yendo en línea recta o puede que estén girando con una curvatura de curva concreta (que suelen mantener largamente en el tiempo). No sabemos la dirección que toman porque son puntos, aún así nos gustaría minimizar la probabilidad de choque frontal entre dos de los aviones visibles. Por ello, queremos evitar a toda costa que se alineen demasiados aviones o que hayan más de 3 en una misma circunferencia, para reducir así el número de caravanas, y por lo tanto, de posibles choques frontales. Sea $d$ la distancia mínima necesaria para que dos aviones que se acercan de frente puedan modificar su trayectoria y así evitar la colisión. Siempre que podamos situaremos los aviones a distancia $kd$ entre ellos para algún $k \in \mathbb{Z}$, para así saber el número de maniobras que pueden hacer los aviones antes de colisionar. Por ejemplo, dos aviones a distancia $3d$ tienen 3 oportunidades de modificar su trayectoria antes de que sea demasiado tarde. Nuestro controlador aéreo, sin saberlo, busca una distribución de los puntos lo más parecida a un conjunto entero, y además, calcula los conjuntos enteros (o casi) más similares al presente, para guiar los aviones a esa nueva distribución y mantener la probabilidad de choque frontal lo mas baja a lo largo del tiempo. Este ejemplo puede extenderse a $\mathbb{R}^3$ y la búsqueda de conjuntos enteros en tres dimensiones.

Sin tener suficiente, reté a unos amigos que me han acompañado estos años en la carrera de matemàticas. Lo prometido es deuda, y con mucha honra, aquí viene el ejemplo de Jordi y Patrícia con sus propias palabras:

"Imaginem que volem fer un teixit a partir d'un conjunt de molècules. Suposem que volem que el teixit tingui una propietat específica que depèn en gran part de les distàncies entre enllaços moleculars. De manera que com més quantitat de molècules situades a distància racional hi hagi, més eficaç serà el teixit. Observem que donada la quantitat de molècules necessària per fer un teixit, el nombre de molècules que

s'ha de tenir en compte és molt gran i es pot considerar infinit. Així doncs, l'estudi del problema d'Ulam pot aportar possibles distribucions de les molècules per tal d'aconseguir la propietat que volíem."

# Referencias


[1] ANNING, Norman H. y ERDÖS, Paul , *Integral distances*, 1945, Bulletin of the American Mathematical Society 51 (8), pp. 598–600, DOI 10.1090/S0002-9904-1945-08407-9.

[2] CADAVID, Carlos, *Una Primera Lección de Geometría Algebraica*, Medellín, Colombia: Universidad EAFIT,2005, pp. 67-81, Ingeniería y Ciencia, ISSN 1794-9165.

[3] CARLSON, John R., *Determination of Heronian Triangles,* San Diego State College, San Diego, California, Fibonacci Quarterly, Vol.8, 1970, p.499-506.

[4] GUERRERO R.,Eugenio; A. MARMOLEJO L., Miguel y MESA P., Héber, *Triángulos de lados enteros, particiones y el Teorema de Pick,* Barcelona: Universitat Autónoma de Barcelona, 20 de octubre del 2011 [consulta: 3 de Mayo del 2015], MATerials MATemàtics Volum 2011, treball no. 5, ISSN: 1887-1097. Disponible en: http://www.mat.uab.cat/matmat/PDFv2011/v2011n05.pdf

[5] KLEE, Victor y WAGON, Stan, *Problem 10 Does the plane contain a dense rational set?*, 1991, Old and New Unsolved Problems in Plane Geometry and Number Theory, Dolciani mathematical expositions 11, Cambridge University Press, pp. 132–135, ISBN 978-0-88385-315-3.

[6] KREISEL, Tobias y KURZ, Sascha, *There are integral heptagons, no three points on a line, no 4 on a circle*, Bayreuth: University of Bayreuth, 2008, Discrete and Computational Geometry 39, pp. 786-790.

[7] KURZ, Sascha and NOLL; Landon C. ; RATHBUN, Randall and SIMMONS Chuck, *Constructing 7-Clusters,* [en línea (pdf)], 9 de diciembre de 2013, [consulta: 27 de mayo del 2015], Disponible en: http://arxiv.org/pdf/1312.2318.pdf, Identificador: arXiv:1312.2318v1 [math.CO]

[8] KURZ Sascha and WASSERMANN Alfred, *On the Minimum Diameter of Plane Integral Point Sets*, [en línea (pdf)], 8 de abril del 2008, [consulta: 13 de mayo del 2015], Disponible en: http://arxiv.org/pdf/0804.1307.pdf, Identificador: arXiv:0804.1307 [math.CO]

[9] NOLL, Landon Curt, *N-clusters,* [Blog], 21 de diciembre del 2013, [consulta: 2 de abril del 2015], Disponible en: http://www.isthe.com/chongo/tech/math/n-cluster/

[10] PEEPLES,W.D. jr., *Eliptic Curves and Rational Distance Sets*, febrero del 1954, Proceedings of the American Mathematical Society, Vol. 5, No. 1, pp. 29-33

[11] SHAFFAF, Jafar, *A Proof for the Erdós-Ulam Problem assuming Bombieri-Lang Conjecture*, [en línea (pdf)], 7 de enero del 2015, [consulta: 27 de junio del 2015], Disponible en: http://es.arxiv.org/pdf/1501.00159v2, Identificador: arXiv:1501.00159v2 [math.NT]

[12] SILVERMAN, Joseph H. , *The Arithmetic of Elliptic Curves*, Second Edition, Springer Science+Business Media, LLC 2009, Graduate Texts in Mathematics 106, DOI 10.1007/978-0-387-09494-6 I.

[13] SILVERMAN, Joseph H. y TATE, John, *Rational Points on Elliptic Curves,* New York and Berlin: Springer-Verlag New York, Inc., 1992, Undergraduate Texts in Mathematics, ISBN 3-540-97825-9.

[14] SIMMONS, Chuck y NOLL, Landon Curt, *N-Cluster Search: Progress Update*, [en línea (pdf)], agosto 2010, [consulta: 27 de marzo del 2015], Disponible en: http://www.isthe.com/chongo/tech/math/n-cluster/7-clustersearchresults.pdf.

[15] SIMMONS, Chuck y NOLL, Landon Curt, *Pictures and coordinates of twenty-five recently found 7-clusters*, [Blog], 22 de Octubre 2010, [consulta: 27 de marzo del 2015], Disponible en: http://cesium062.blogspot.com.es/2010/10/pictures-and-coordinates-of-twenty-five.html

[16] SOLYMOSI Jozsef and DE ZEEUW, Frank, *On a question of Erdös and Ulam,* [en línea (pdf)] 14 de enero del 2009, [consulta: 2 de marzo del 2015], Disponible enhttp://arxiv.org/pdf/0806.3095v2.pdf, Identificador: arXiv:0806.3095 [math.CO]

[17] TAO, Terence, *The Erdos-Ulam problem, varieties of general type, and the Bombieri-Lang conjecture* [Blog], 22 de diciembre del 2014, [consulta: 27 de marzo], Disponible en:https://terrytao.wordpress.com/2014/12/20/the-erdos-ulam-problem-varieties-of-general-type-and-the-bombieri-lang-conjecture/

[18] WAYNE, Aitken, *Legendre's theorem, Legrange's descent,* [en linea (pdf)], [consulta: 27 de abril del 2015], Supplement for math 370: Number Theory. Disponible en: http://public.csusm.edu/aitken_html/notes/legendre.pdf

[19] WEISSTEIN, Eric W., *Inversion*, [en linea], MathWorld–A Wolfram Web Resource. Disponible en: http://mathworld.wolfram.com/Inversion.html.

[20] WIKIPEDIA, *Teorema de Pick,* Wikipedia, la enciclopedia libre, 20 de marzo del 2015, [consulta: 2 de junio del 2015] Disponible en: https://es.wikipedia.org/w/index.php?title=Teorema_de_Pick&oldid=80891415, código de versión: 80891415.

[21] ZUMALACÁRREGUI, Ana, *Teorema de Mordell-Weil,* Tutor: A. Quirós Gracián, Madrid: Universidad Autónoma de Madrid, 2010.