Departamento de Matemáticas, Facultad de Ciencias
Universidad Autónoma de Madrid

Introducción a la geometría algebraica a través de la Aritmética de Diofanto

Trabajo de fin de grado

Grado en Matemáticas

Autor: Martín de las Heras Moreno
Tutor: Enrique González Jiménez

Curso 2021-2022

Resumen

Diofanto de Alejandría fue un matemático de la antigüedad, autor de la Aritmética, una compendio de libros donde se plantean problemas matemáticos. Estos problemas, a priori simples, generan estructuras estudiadas en geometría algebraica. También se aportan soluciones, pero de manera única y numérica, por lo que no se suele tener el conjunto total de las soluciones de cada problema.
En este trabajo, inspirados por encontrar todas las soluciones a estos problemas de la Aritmética, o por observar hasta qué punto son resolubles de manera completa, se explican tanto la Aritmética, como nociones básicas de este campo. De esta manera, se usa la obra como elemento introductorio al campo de la geometría algebraica.

El trabajo comienza por una introducción sobre la Aritmética, su historia, su estructura y su influencia en las matemáticas. A continuación, se presentan conceptos básicos de la geometría algebraica en los espacios afín y proyectivo. El siguiente tema a tratar es el mundo de las curvas elípticas, tomando un papel central la estructura de grupo de sus puntos y concluyendo con el Teorema de Mordell.
Una vez visto los conceptos, se retorna a la Aritmética, utilizando sus problemas para ejemplificar una clasificación de las variedades algebraicas en función de la dimensión (y el género en el caso de dimensión 1), y viendo los tipos de variedades y sus puntos racionales. Finalmente, se exponen los resultados del cálculo de los diferentes problemas de la Aritmética con el software de cálculo simbólico `Magma`.

Abstract

Diophantus of Alexandria, was an ancient mathematician who authored the series of books called Arithmetica. This work, consists of several books of mathematical problems that at first sight seem simple, but they generate structures studied in algebraic geometry. A single numerical solution is given for each problem, but never the complete set.
In this work, inspired by finding all solutions to each problem, or at least to know to which degree are they fully solvable, we explain both the Arithmetica and basic notions of this field of mathematics. Thus, we use Diophantus' work as an introduction to the field of algebraic geometry.

The project starts with an introduction to the Arithmetica, its history, structure and influence on mathematics. then, we dive into basic concepts of algebraic geometry, both in affine and projective space. The next topic to study will be elliptic curves, where the main point of focus will be the group structure of its points and concluding with Mordell's Theorem.
Once the concepts have been explained, we go back to the Arithmetica, using its problems to exemplify a classification of algebraic varieties in terms of their dimension (and for those with dimension 1, also their genus), and naming the types of varieties and their rational points. Finally, we present the results of our own calculations of the different problems of the Arithmetica with the symbolic calculus software `Magma`.

Índice general

Introducción VII

1 Aritmética de Diofanto 1
- 1.1 Diofanto . . . 1
- 1.2 Aritmética . . . 1
  - 1.2.1 Libros *griegos* . . . 2
  - 1.2.2 Libros *árabes* . . . 2
  - 1.2.3 Estructura de los problemas . . . 2
  - 1.2.4 Influencias . . . 3
- 1.3 Fermat . . . 3

2 Geometría algebraica 5
- 2.1 Espacio afín . . . 5
- 2.2 Espacio proyectivo . . . 7
- 2.3 Variedades algebraicas . . . 9
  - 2.3.1 Aplicaciones entre variedades . . . 12
- 2.4 Puntos singulares . . . 15
- 2.5 Curvas algebraicas . . . 17
  - 2.5.1 Aplicaciones entre curvas . . . 17
  - 2.5.2 Género de una curva . . . 18

3 Curvas elípticas 19
- 3.1 Forma normal de Weierstrass . . . 19
- 3.2 Ley de las tangentes y las secantes . . . 20
- 3.3 Ley de grupo . . . 22
- 3.4 Teorema de Mordell . . . 24

4 Puntos racionales en variedades algebraicas 25
- 4.1 Introducción . . . 25
- 4.2 Clasificación . . . 25

5 Cálculo con MAGMA de los problemas de la Aritmética 31
- 5.1 Funcionamiento del código . . . 31
- 5.2 Tablas de resultados . . . 32

A Problemas de Diofanto 35

B Código MAGMA 45

Introducción

La Aritmética es una antigua colección de problemas algebraicos. Fue escrita por el matemático Diofanto en el siglo III d.C. y es un trabajo que mantiene una gran influencia en el desarrollo del álgebra.
Esta serie de 13 libros, de los cuales se conservan 10 actualmente, establecen problemas de polinomios y soluciones numéricas para cada uno. La complejidad de los mismos va en aumento a medida que se va avanzando y en algunos casos se conoce el método utilizado por Diofanto para resolverlos. Uno de los problemas más famosos, fue el problema 8 del libro II, el cual inspiró el conocido *Último Teorema de Fermat*, el cual escribió en el margen de su copia de la Aritmética.

Una vez explicado en el primer capítulo el origen y pérdida parcial de esta obra, se procede a explicar diversos conceptos de geometría algebraica; elementos que se pueden extraer de estos problemas.

La geometría algebraica, se dedica al estudio de los conjuntos de soluciones de ecuaciones polinómicas. Es un campo extenso y cuyo desarrollo es relativamente moderno, pero en lo que concierne a este trabajo, se tratarán solamente las bases.
Se comienza explicando los conceptos relativos al espacio afín, tanto el espacio en sí como sus conjuntos algebraicos. De la misma manera se explican conceptos relativos al espacio proyectivo. A continuación, se llega al campo de las variedades algebraicas, afines y proyectivas, así como las aplicaciones entre variedades y la regularidad de las mismas. Para ello hacemos uso de conceptos como el anillo local de una variedad, y explicamos conceptos como el de variedades isomorfas. El siguiente punto de interés en el capítulo son los puntos singulares. Para concluir se realiza una breve introducción a las curvas algebraicas y al concepto de género de una curva. En este capítulo se estudia la curva de ecuación $y^2 = x^3 + Ax + B$, la cual se utilizará regularmente en el siguiente capítulo.

Proseguimos con el estudio de las curvas elípticas, las cuales utilizaremos siempre bajo la ecuación $y^2 = x^3 + Ax + B$ ya mencionada. En ellas se definirá una operación de suma, la cual genera a su vez una estructura de grupo en los puntos que la componen. Esto nos lleva al llamado *Teorema de Mordell*, el cual nos desvela que la estructura de grupo generada sobre la curva elíptica es concretamente de grupo abeliano finitamente generado.

En el penúltimo capítulo, se vuelve a conectar con Diofanto, mediante una clasificación de variedades algebraicas en función de su dimensión. De la misma manera,

se explicará el estado del problema de obtención de puntos racionales en variedades algebraicas. Esta clasificación será ejemplificada con problemas reales propuestos por Diofanto, pero está limitada a partir de un punto debido a la dificultad de los conceptos necesarios para poder desarrollarla adecuadamente.

Por último, se presenta un cálculo de las dimensiones de todas las variedades generadas por los problemas de la aritmética. En el caso de las curvas algebraicas, también se aporta el género de cada una. Para ello, se hizo uso del software de cálculo simbólico `Magma`. En primer lugar se explica el funcionamiento del código, el cual fue ejecutado de manera local, para a continuación, en forma de tabla, presentar los resultados de los cálculos, primero en general, y más tarde agrupando para cada libro los problemas.

CAPÍTULO 1
Aritmética de Diofanto

1.1. Diofanto

Matemático griego alejandrino conocido como el padre del álgebra. Nacido entre 201 y 215 d.C y fallecido entre 285 y 299 d.C, la exactitud de su edad viene dada por el acertijo presente en su epitafio, el cual decía:

«Caminante, esta es la tumba de Diofanto: es él quien con esta sorprendente distribución te dice el número de años que vivió. Su niñez ocupó la sexta parte de su vida; después, durante la doceava parte su mejilla se cubrió con el primer bozo. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo un precioso niño que, una vez alcanzada la mitad de la edad de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años. De todo esto se deduce su edad».

Este acertijo, reflejo de lo que es su obra se resuelve de manera fácil, sea x la edad de Diofanto tenemos:

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x$$

De esa manera pese a no saber el año exacto de su nacimiento y de su muerte, sabemos que su vida duró 84 años gracias a su propio epitafio.

Entre sus obras se le atribuyen cuatro contribuciones principales: la Aritmética, Moriástica, Sobre los números poligonales y Porismas, el cual está perdido y se sabe de su existencia por numerosas referencias en la Aritmética.

1.2. Aritmética

La Aritmética no se trata de solo un libro, sino de una serie de 13 libros de problemas aritméticos escritos por Diofanto. De todos estos, sin embargo solo han llegado a la actualidad 10 y debido a dos *renacimientos*, como explica Norbert Schappacher en [11]. A raíz de ese artículo dividiremos los orígenes de los libros en dos secciones.

1.2.1. Libros *griegos*

Estos libros fueron recuperados posteriormente a los llamados libros árabes, pero conviene mencionarlos antes debido a que fueron los únicos libros utilizados por los matemáticos occidentales hasta bien entrado el siglo XX.
Los seis libros llamados *griegos*, tuvieron su renacimiento en torno a los siglos XI y XIII en el imperio Bizantino, donde se recuperaron los manuscritos (si bien no los originales) de los libros mencionados. Más tarde, en el año 1575 el humanista Wilhelm Holzmann (1532-1576) realiza la primera edición europea al traducir al latin el texto de Diofanto. Esta traducción fue seguida por la realizada en 1621 por Claude Gaspar Bachet de Méziriac, un Jesuita, matemático, lingüista y poeta francés. Esta traducción incluyó muchas anotaciones y en el caso del libro I, soluciones completas a todos los problemas.
Ya entre finales del siglo XIX y principios del XX, el trabajo hecho por Paul Tannery y Sit Thomas Little Heath llega la copia final, realizada por Heath, que se ha utilizado en este trabajo [7].

1.2.2. Libros *árabes*

Los primeros registros de los cuatro libros conocidos como *árabes*, datan del siglo IX. Estas traducciones fueron hechas por Qusta ibn Luqa (820-912), un traductor de la corte de Bagdad. Se estipula que su traducción abarcó los siete primeros libros, pero actualmente solamente se conservan los libros IV a VII.
No fue hasta 1968 que estos libros cobraron renovada importancia. Primero el orientalista Fuat Sezgin encontró cuatro libros anteriormente desconocidos en una mezquita en el noreste de Irán. Posteriormente, en 1975, Jacques Sesiano realizó su tesis doctoral en Brown University sobre estos libros [12]. La versión de Sesiano será la utilizada para este trabajo para completar así los 10 libros que se conocen.

En lo que respecta al orden, se había considerado siempre que los seis libros supervivientes de los griegos, a los que a partir de ahora me referiré como *libros griegos* eran los libros 1 a 6 (referidos a partir de ahora como GI-GVI, donde G indica que es un libro griego y I-VI indica el número del libro en números romanos), pero tras el descubrimiento en occidente de los libros árabes (referidos de manera análoga a los griegos como AIV-AVII), Sesiano propuso un reorden de los mismos, de manera que el orden fuese GI-GII-GIII-AIV-AV-AVI-AVII-GIV-GV-GVI, ya que por el incremento de complejidad presente en la sucesión de los libros, consideraba que ese orden era más correcto.

1.2.3. Estructura de los problemas

En lo que respecta a enunciar y resolver problemas, Diofanto siguió a lo largo de su obra siempre el mismo método. Primero enunciar el problema utilizando lenguaje natural, para después escribirlo de manera formal y obtener de él una única solución entera o racional. Para hallar la solución específica, hacía uso de algoritmos y frecuentemente condiciones necesarias para la viabilidad del problema.

Esto nos deja con una resolución de los problemas en cierto modo incompleta, ya que la obtención de una única solución no siempre satisface la curiosidad científica. De todas formas, en muchos de los problemas, como veremos en los últimos capítulos, las herramientas necesarias para su completa resolución no serían desarrolladas hasta pasados varios siglos, y en muchos casos, todavía a día de hoy no existe un método que garantice la completitud de la solución.

De la misma manera, los libros de la Aritmética, no siguen ningún tema en particular, salvo algunas excepciones, y el grado de las ecuaciones presentes en los problemas va aumentando a medida que van avanzando los libros:

GI Todo ecuaciones lineales.

GII Introduce términos cuadráticos por primera vez.

GIV Introduce términos cúbicos por primera vez (si se considera este libro anterior a AIV).

GVI Este es uno de los pocos libros con un "tema", todos los problemas son planteados como la obtención de un triángulo rectángulo de lados racionales.

AIV El único libro del que se tiene constancia de un título: *De cuadrados y cubos.*

Nótese que todos los problemas se resuelven haciendo uso de los números racionales y también es importante tener en cuenta que no tenían concepto de número negativo, por lo que muchos de los problemas se encuentran en cierto modo duplicados si se tiene en cuenta la existencia de dichos números.

De la misma manera se puede apreciar que Diofanto tenía constancia de algún método de resolución de ecuaciones cuadráticas, pero dicho método no es discutido en la obra.

1.2.4. Influencias

El trabajo de Diofanto tuvo una gran influencia en la historia de las matemáticas. Sus trabajos tuvieron una profunda importancia en el desarrollo del álgebra europea en los siglos XVI y XVII. También puede verse sobre Fermat, pero esto será discutido en el siguiente apartado. Por estos motivos se le conoce como el *padre del álgebra* ya que tuvo grandes contribuciones a la teoría de números y notación matemática.

1.3. Fermat

Pierre de Fermat fue un matemático aficionado francés del siglo XVII, responsable de las primeras bases del cálculo infinitesimal y una gran contribución a diferentes campos de las matemáticas.
En esta sección sin embargo, lo más relevante a remarcar es la enunciación del llamado último teorema de Fermat, el cual redactó en el margen de su copia de la traducción de

Bachet de la Aritmética. Esta teorema no fue más que una conjetura durante 358 años hasta que el matemático británico Andrew Wiles lo demostrase en 1994-95 [15, 17]. Más concretamente, la nota de Fermat fue en el problema ocho del libro GII, la cual dice:

Si n es un número entero mayor o igual que 3, entonces no existen números enteros positivos x, y y z, tales que se cumpla la igualdad:

$$x^n + y^n = z^n.$$

He encontrado una demostración realmente admirable, pero el margen del libro es muy pequeño para ponerla.

La demostración a la cual hace referencia nunca se ha encontrado y parece poco probable que tuviera una demostración válida para todo valor de n. Lo que sí que demostró Fermat sin embargo, fue el caso de $n = 4$ mediante descenso infinito. En esta prueba demuestra que el área de un triángulo rectángulo con lados enteros nunca puede ser igual al cuadrado de un entero, en otras palabras

$$x^4 - y^4 = z^2$$

no tiene soluciones enteras. Esto prueba el teorema previo para $n = 4$ ya que $a^4 + b^4 = c^4$ puede reescribirse como $c^4 - b^4 = (a^2)^2$.
De todas formas esto ilustra perfectamente la complejidad a la que pueden llegar las soluciones generales de los problemas de Diofanto ya que, de un enunciado aparentemente sencillo, surge uno de los teoremas más conocidos de la historia.

CAPÍTULO 2
Geometría algebraica

La geometría algebraica es el campo de las matemáticas dedicada al estudio de los conjuntos de soluciones de sistemas de ecuaciones polinómicas.
Los objetos de estudio fundamentales son las llamadas *variedades algebraicas*, que son manifestaciones geométricas de soluciones de sistemas de polinomios. Ejemplos de las clases de variedades algebraicas más utilizadas son las curvas algebraicas, que son variedades algebraicas de dimensión 1 y entre las que se encuentran las rectas, curvas cónicas y curvas cúbicas, como las curvas elípticas, elementos que van a ser de interés en este trabajo.

En este capítulo se describen los conceptos más básicos de la geometría algebraica descritos en [13, I].

Por conveniencia, se utilizará la siguiente notación a lo largo del capítulo para evitar repeticiones:

- m y n como números enteros positivos.
- K como cuerpo con $char(K) = 0$.
- $\bar{K}$ como un cierre algebraico de K.
- $G_{\bar{K}/K}$ el grupo de Galois de $\bar{K}/K$.

2.1. Espacio afín

Definición 2.1 (n-espacio afín (sobre K))**.** El n-espacio afín sobre K es el conjunto de n-tuplas:

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \{P = (x_1, ..., x_n) : x_i \in \bar{K}\}.$$

De la misma manera, el conjunto de puntos K-racionales de $\mathbb{A}^n$ es:

$$\mathbb{A}^n(K) = \{P = (x_1, ..., x_n) \in \mathbb{A}^n : x_i \in K\}.$$

Nótese que el grupo de Galois $G_{\bar{K}/K}$ actúa en $\mathbb{A}^n$ como $P^\sigma = (x_1^\sigma, ..., x_n^\sigma)$.
De ese modo: $\mathbb{A}^n(K) = \{P \in \mathbb{A}^n : P^\sigma = P,\ \forall \sigma \in Gal(\bar{K}/K)\}$.

Sea $\bar{K}[X] = \bar{K}[X_1, ..., X_n]$ un anillo de polinomios de n variables y sea $I \subset \bar{K}[X]$. A cada I le asociamos un subconjunto de $\mathbb{A}^n$,

$$V_I = \{P \in \mathbb{A}^n : f(P) = 0,\ \forall f \in I\}.$$

Definición 2.2 (Conjunto algebraico afín)**.** Sea $V \subset \mathbb{A}^n$, se le llama conjunto algebraico afín si existe un ideal $I \subset \bar{K}[X]$ tal que $V_I = V$.

Se define el ideal de un conjunto V como:

$$I(V) = \{f \in \bar{K}[X] : f(P) = 0,\ \forall P \in V\}.$$

Sea V un conjunto algebraico, y consideremos el ideal $I(V)_K$ definido por:

$$I(V)_K = \{f \in K[X] : f(P) = 0,\ \forall P \in V\} = I(V) \cap K[X].$$

Decimos que V está definido sobre K denotado por V/K si:

$$I(V) = I(V)_K \bar{K}[X].$$

Si V está definido sobre K, denotamos por $I(V/K) = I(V)_K$.
Ahora supongamos que V está definido sobre K y sean $f_1, ..., f_m \in K[X]$ generadores de $I(V/K)$. Entonces $V(K)$ es precisamente el conjunto de soluciones $X = (x_1, ..., x_n) \in \mathbb{A}^n(K)$ a las ecuaciones simultáneas:

$$f_1(X) = ... = f_m(X) = 0.$$

A los puntos de $V(K)$ se les llama K-puntos racionales de V.
Por lo tanto uno de los problemas fundamentales de la geometría aritmética, la solución de ecuaciones polinómicas en $\mathbb{Q}$, puede describirse como el problema de describir conjuntos de la forma $V(K)$ cuando K es un cuerpo de números.

Ejemplo 2.3. *Sea V el conjunto algebraico en $\mathbb{A}^2$ dado por la siguiente ecuación:*

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

Este conjunto está definido sobre K para cualquier cuerpo K.
Asumimos que $char(K) \neq 2$. Entonces el conjunto $V(K)$ se corresponde uno a uno con $\mathbb{A}^1(K)\backslash\{\pm 1\}$ teniendo como aplicación:

$$\begin{aligned} \mathbb{A}^1(K) \setminus \{\pm 1\} &\longrightarrow V(K) \\ t &\longmapsto \left(\frac{t^2+1}{t^2-1}, \frac{2t}{t^2-1}\right). \end{aligned}$$

Para obtener esta parametrización, primero tomamos un punto del conjunto, en este caso $P = (1, 0)$ y obtenemos los demás puntos como la intersección de V con la familia de rectas $y = t(x - 1)$, donde $t \in \mathbb{Q}$. Esto nos deja el siguiente sistema:

$$\begin{cases} y & = t(x-1), \\ x^2 - y^2 & = 1. \end{cases}$$

Sustituimos $y = t(x-1)$ *en la segunda ecuación de manera que simplificando nos queda:*

$$(t^2-1)x^2 - 2t^2x + (t^2+1) = 0.$$

Esto nos deja una ecuación de segundo grado que desarrollando nos da dos posibles soluciones para x*:*

$$x = \frac{t^2 \pm 1}{t^2 - 1}.$$

Entonces, tenemos dos opciones: $x = 1$*, el cual nos da* $y = 0$*, en otras palabras, el punto* P*; y* $x = \frac{t^2+1}{t^2-1}$*, el cual nos da* $y = \frac{2t}{t^2-1}$*.*

Ejemplo 2.4. *El conjunto algebraico:*

$$V : X^n + Y^n = 1$$

está definido sobre $\mathbb{Q}$*. Este ejemplo es una generalización del problema 8 del segundo libro griego de Diofanto (presente en el Apéndice A), el cual inspiró el último teorema de Fermat, probado por Andrew Wiles en 1995 [15, 17], dice que para todo* $n \geq 3$*,*

$$V(\mathbb{Q}) = \begin{cases} \{(1,0),(0,1)\} & \text{si } n \text{ es impar} \\ \{(\pm 1,0),(0,\pm 1)\} & \text{si } n \text{ es par} \end{cases}$$

Ejemplo 2.5. *El conjunto algebraico:*

$$V : Y^2 = X^3 + 17$$

tiene muchos puntos racionales en $\mathbb{Q}$*, por ejemplo*

$$(-2,3), \qquad (5234, 378661), \qquad \left(\frac{137}{64}, \frac{2651}{512}\right).$$

2.2. Espacio proyectivo

Históricamente, el espacio proyectivo surgió a través del proyecto de añadir "puntos en el infinito"al espacio afín. Definimos el espacio proyectivo como la colección de rectas a través del origen en el espacio afín de una dimensión mayor.

Definición 2.6 (n-espacio proyectivo)**.** El n-espacio proyectivo (sobre K), denotado por $\mathbb{P}^n$ o $\mathbb{P}^n(\bar{K})$, es el conjunto de todas las $(n+1)$-tuplas $(x_0, ..., x_n) \in \mathbb{A}^{n+1}$ tal que al menos un $x_i \neq 0$ modulo la relación de equivalencia:

$$(x_0, ..., x_n) \sim (y_0, ..., y_n)$$

si existe $\lambda \in \bar{K}^*$ tal que $x_i = \lambda y_i$ para todo i.
De esta manera la clase de equivalencia $\{(\lambda x_0, ..., \lambda x_n) : \lambda \in \bar{K}^*\}$ se denota por $[x_0, ..., x_n]$ y los $x_0, ..., x_n$ individuales se llaman coordenadas homogéneas para el punto correspondiente en $\mathbb{P}^n$. De modo que el conjunto de puntos K-racionales en $\mathbb{P}^n$ es el conjunto:

$$\mathbb{P}^n(K) = \{[x_0, ..., x_n] \in \mathbb{P}^n : x_0, ..., x_n \in K\}.$$

Definición 2.7 (Cuerpo mínimo de definición)**.** Sea $P = [x_0, ..., x_n] \in \mathbb{P}^n(\bar{K})$. El cuerpo mínimo de definición de P (sobre K) es el cuerpo:

$$K(P) := K(x_0/x_i, ..., x_n/x_i),\ \forall i \text{ con } x_i \neq 0$$

Obsérvese que no depende de la elección de $x_i \neq 0$. Supongamos que existe $x_j \neq 0$, entonces $K\left(x_0/x_i, ..., x_n/x_i\right) = K\left(x_0/x_j, ..., x_n/x_j\right)$ mediante la relación $\frac{x_k}{x_j} = \frac{(x_k/x_i)}{(x_j/x_i)}$.

Al igual que en el espacio afín, el grupo de Galois $G_{\bar{K}/K}$ actúa sobre las coordenadas homogéneas en $\mathbb{P}^n$:

$$[x_1, ..., x_n]^\sigma = [x_1^\sigma, ..., x_n^\sigma].$$

Esta acción está bien definida y es independiente de la elección de las coordenadas homogéneas ya que,

$$[\lambda x_0, ..., \lambda x_n]^\sigma = [\lambda^\sigma x_1^\sigma, ..., \lambda^\sigma x_n^\sigma] = [x_1^\sigma, ..., x_n^\sigma].$$

Por lo tanto tenemos que

$$\mathbb{P}^n(K) = \{P \in \mathbb{P}^n :\ P^\sigma = P,\ \forall \sigma \in G_{\bar{K}/K}\},$$

y que

$$K(P) = \bar{K}^H,$$

donde $H = \{\sigma \in G_{\bar{K}/K} :\ P^\sigma = P\}$.

Definición 2.8 (Ideal homogéneo)**.** Sea $I \subset K[X]$ un ideal, decimos que es un ideal homogéneo si está generado por polinomios homogéneos.

Definición 2.9 (Conjunto algebraico proyectivo)**.** Sea $V \subset \mathbb{P}^n$, se le llama conjunto algebraico proyectivo si existe un ideal homogéneo $I \subset K[X]$ tal que $V_I = V$. Por lo tanto tiene la forma:

$$V_I = \{P \in \mathbb{P}^n : f(P) = 0,\ \forall f \in I \text{ homogéneo}\}.$$

Nota 2.10. *Es necesario que se trate de un polinomio homogéneo, debido a la relación de equivalencia presente en el espacio proyectivo. Esto implica que para un $P \in \mathbb{P}^n$ si $f(P) = 0$, entonces para cualquier $\lambda \in \bar{K}$, $f(\lambda P) = 0$.*
En el caso de un polinomio homogéneo tendríamos $f(\lambda P) = 0$, ya que $f(\lambda P) = \lambda^d f(P) = 0$, donde d es el grado del polinomio.

Por lo tanto, análogamente a como se hizo para el espacio afín, se de define el ideal (homogéneo) de un conjunto algebraico proyectivo V como:

$$I(V) = \{f \in \bar{K}[X] : f \text{ es homogénea y } f(P) = 0\ \forall P \in V\}.$$

Si V está definido sobre K, entonces el conjunto de puntos K-racionales de V es el conjunto:

$$V(K) = V \cap \mathbb{P}^n(K).$$

Como de costumbre, también se puede describir como:

$$V(K) = \{P \in V :\ P^\sigma = P,\ \forall \sigma \in G_{\bar{K}/K}\}.$$

Ejemplo 2.11. *Una recta en $\mathbb{P}^2$ es un conjunto algebraico dado por una ecuación lineal:*

$$aX + bY + cZ = 0,$$

con $a, b, c \in \bar{K}$ no todos cero. Si, por ejemplo $c \neq 0$ entonces esa línea estaría definida sobre cualquier cuerpo que contenga a/c y b/c. Más generalmente, un hiperplano en $\mathbb{P}^n$ viene dado por una ecuación:

$$a_0X_0 + a_1X_1 + ... + a_nX_n = 0,$$

con $a_i \in \bar{K}$ no todos cero.

2.3. Variedades algebraicas

Definición 2.12 (Variedad afín)**.** Un conjunto algebraico afín V se llama variedad (afín) si $I(V)$ es un ideal primo en $\bar{K}[X]$.

Nótese que si V está definida en K, no es suficiente que $I(V/K)$ sea primo en $K[X]$. Por ejemplo, el ideal $\langle X_1^2 - 2X_2^2 \rangle$ en $\mathbb{Q}[X_1, X_2]$. En este caso el ideal es primo en $\mathbb{Q}[X_1, X_2]$, ya que no puede ser factorizado en polinomios de grado más bajo en $\mathbb{Q}[X_1, X_2]$ pero sí en $\bar{\mathbb{Q}}[X_1, X_2]$: $X_1^2 - 2X_2^2 = (X_1 - \sqrt{2}X_2)(X_1 + \sqrt{2}X_2)$.

Definición 2.13 (Anillo de coordenadas afines)**.** Sea V/K una variedad afín. El anillo de coordenadas afines de V/K está definido por

$$K[V] = \frac{K[X]}{I(V/K)}.$$

El anillo $K[V]$ es un dominio de integridad, ya que $K[X]$ es un anillo conmutativo e $I(V/K)$ es un ideal primo. Su cuerpo de fracciones está denotado por $K(V)$ y se conoce como *cuerpo de funciones de* V/K. De manera similar $\bar{K}[V]$ y $\bar{K}(V)$ se definen reemplazando K con $\bar{K}$.

Definición 2.14 (Dimensión de V)**.** Sea V una variedad afín. La dimensión de V, denotada como $dim(V)$, es el grado de trascendencia de $\bar{K}(V)$ sobre $\bar{K}$.

Ejemplo 2.15. *La dimensión de $\mathbb{A}^n$ es n, ya que $\bar{K}(\mathbb{A}^n) = \bar{K}(X_1, ..., X_n)$. De la misma manera, si $V \subset \mathbb{A}^n$ viene dado por una única ecuación polinómica no constante:*

$$f(X_1, ..., X_n) = 0,$$

entonces dim(V)= $n - 1$.
Esto se debe a que, si $(X_1, ..., X_n) \in V$ entonces $f(X_1, ..., X_n) = 0$. De aquí sacamos que podemos elegir todos los P_i de manera independiente, salvo uno, el cual viene dado por la condición de que $f(X_1, ..., X_n) = 0$. Por lo tanto quedarían $n - 1$ coordenadas independientes.

Definición 2.16 (Variedad proyectiva)**.** Un conjunto algebraico proyectivo es una variedad (proyectiva) si su ideal homogéneo $I(V)$ es un ideal primo en $\bar{K}[X]$.

Veamos que $\mathbb{P}^n$ contiene muchas copias de $\mathbb{A}^n$. Para cada $0 \leq i \leq n$, existe una inclusión:

$$\begin{aligned} \phi_i : \mathbb{A}^n &\longrightarrow \mathbb{P}^n, \\ (y_1, ..., y_n) &\longmapsto [y_1, y_2, ..., y_{i-1}, 1, y_i, ..., y_n]. \end{aligned}$$

Denotamos con H_i el hiperplano en $\mathbb{P}^n$ dado por $X_i = 0$:

$$H_i = \{P = [x_0, ..., x_n] \in \mathbb{P}^n : \ x_i = 0\}.$$

Denotamos con U_i el complemento de H_i:

$$U_i = \{P = [x_0, ..., x_n] \in \mathbb{P}^n : \ x_i \neq 0\} = \mathbb{P}^n \backslash H_i.$$

Existe entonces una biyección natural:

$$\begin{aligned} \phi_i^{-1} : U_i &\longrightarrow \mathbb{A}^n, \\ [x_0, ..., x_n] &\longmapsto \left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, ..., \frac{x_{i-1}}{x_i}, \frac{x_{i+1}}{x_i}, ..., \frac{x_n}{x_i} \right). \end{aligned}$$

Fijado i, idenficaremos $\mathbb{A}^n$ con el conjunto U_i en $\mathbb{P}^n$ a través de la aplicación ϕ_i. Sea V el conjunto algebraico proyectivo con ideal homogéneo $I(V) \subset \bar{K}[X]$. Entonces $V \cap \mathbb{A}^n$, con lo que nos referimos a $\phi_i^{-1}(V \cap U_i)$ para algún i fijo, es un conjunto algebraico afín con ideal $I(V \cap \mathbb{A}^n) \subset \bar{K}[Y]$ dado por:

$$I(V \cap \mathbb{A}^n) = \{f(Y_1, ...Y_{i-1}, 1, Y_{i+1}, ..., Y_n) : f(X_0, ..., X_n) \in I(V)\}.$$

Nótese que los conjuntos $U_0, ..., U_n$ cubren todo $\mathbb{P}^n$, por lo que cualquier variedad proyectiva V está cubierta por subconjuntos $V \cap U_0, ..., V \cap U_n$, cada uno de los cuales es una variedad afín a través de una aplicación ϕ_i^{-1} apropiada.

El proceso de reemplazar el polinomio $f(X_0, ..., X_n)$ con el polinomio $f(Y_1, ..., Y_{i-1}, 1, Y_{i+1}, ..., Y_n)$ se llama *deshomogeneización respecto de* X_i.
Este proceso se puede revertir. Para cada $f(Y) \in \bar{K}[Y]$, definimos:

$$f^*(X_0, ..., X_n) = X_i^d f \left(\frac{X_0}{X_i}, \frac{X_1}{X_i}, ..., \frac{X_{i-1}}{X_i}, \frac{X_{i+1}}{X_i}, ..., \frac{X_n}{X_i} \right).$$

donde $d = grado(f)$. Decimos que f^* es la homogeneización de f respecto de X_i.
Por ejemplo, sea $f(X, Y) = Y^2 - (X^3 + AX + B)$ un polinomio no homogéneo, entonces

$$f^*(X, Y, Z) = Z^3 f \left(\frac{X}{Z}, \frac{Y}{Z} \right) = Y^2 Z - (X^3 + AXZ^2 + BZ^3).$$

Definición 2.17 (Cierre proyectivo)**.** Sea $V \subset \mathbb{A}^n$ un conjunto algebraico afín con ideal $I(V)$ y consideremos V como subconjunto de $\mathbb{P}^n$ via:

$$V \subset \mathbb{A}^n \xrightarrow{\phi_i} \mathbb{P}^n.$$

El cierre proyectivo de V (denotado por $\bar{V}$), es el conjunto algebraico proyectivo tal que su ideal homogéneo $I(\bar{V})$ está generado por:

$$\{f^*(X) : f \in I(V)\}.$$

Definición 2.18 (Dimensión proyectiva)**.** Sea V una variedad proyectiva y elijamos $\mathbb{A}^n \subset \mathbb{P}^n$ tal que $V \cap \mathbb{A}^n \neq \emptyset$. La dimensión de V es la dimensión de $V \cap \mathbb{A}^n$.

Proposición 2.19. *(a) Sea V una variedad afín. Entonces $\bar{V}$ es una variedad proyectiva y se cumple:*

$$V = \bar{V} \cap \mathbb{A}^n.$$

(b) Sea V una variedad proyectiva, entonces $V \cap \mathbb{A}^n$ es una variedad afín y se cumple

$$V \cap \mathbb{A}^n = \emptyset \qquad o \qquad V = \overline{V \cap \mathbb{A}^n}.$$

(c) Si una variedad afín (resp. proyectiva), V está definida sobre K, entonces $\bar{V}$ (resp. $V \cap \mathbb{A}^n$) está también definida sobre K.

Demostración. Ver [6, I.2.3] para los apartados (a) y (b).
En el apartado (c) se deduce por la teoría ya que para V afín (resp. proyectiva), si está definido sobre K implica que $I(V)$ también lo está y por el proceso de deshomogeneización (resp. homogeneización) el ideal de $\bar{V}$ (resp. $V \cap \mathbb{A}^n$) también lo está y por lo tanto sus variedades. □

Ejemplo 2.20. *Sea V la variedad afín dada por la ecuación:*

$$V : y^2 = x^3 + Ax + B.$$

El cierre proyectivo de V es la variedad en $\mathbb{P}^2$ dada por la ecuación homogénea

$$\bar{V} : Y^2Z = X^3 + AXZ^2 + BZ^3.$$

Con la correspondencia

$$x = X/Z, \qquad y = Y/Z.$$

A continuación comprobamos que tiene un único punto en el infinito. Sea $Z = 0$, entonces tendríamos

$$Y^2 * 0 = X^3 + AX * 0^2 + B * 0^3 \longrightarrow X^3 = 0$$

esto implica que se trata de un punto de V si $X = 0$ y que esto se cumple para todo valor de Y, o escrito en coordenadas homogéneas, el punto $[0, 1, 0]$ pertenece a V. Esto nos resulta en que

$$V(\mathbb{Q}) = \{(x, y) \in \mathbb{A}^2(\mathbb{Q}) : y^2 = x^3 + Ax + B\} \cup \{[0, 1, 0]\}.$$

Previamente habíamos definido varios puntos en $V(\mathbb{Q})$ en el Ejemplo 2.5 para el caso $A = 0,\ B = 17$. Entonces, mediante el método de tangentes y secantes descrito en el Capítulo 3, podemos obtener más puntos en $V(\mathbb{Q})$.

Definición 2.21 (Cuerpo de funciones)**.** Sea V una variedad proyectiva, se define el cuerpo de funciones de V, denotado por $K(V)$ (resp. $\bar{K}(V)$) como

$$K(V) = \{f/g | f, g \text{ homogéneas del mismo grado, } g \notin I(V)\}/\sim .$$

Donde dos funciones $f_1/g_1 \sim f_2/g_2$ sí y solo si $f_1g_2 - g_1f_2 \in I(V)$.

Obsérvese que si $f/g \in K(V)$ y $P \in V$ tiene sentido definir $(f/g)(P)$.

2.3.1. Aplicaciones entre variedades

Hacemos un pequeño comentario sobre las aplicaciones algebraicas entre variedades proyectivas. Estos son aplicaciones definidas por funciones racionales.

Definición 2.22 (Aplicación racional)**.** Sean $V_1 \subset \mathbb{P}^n,\ V_2 \subset \mathbb{P}^m$ variedades proyectivas. Una aplicación racional de V_1 a V_2 es una aplicación de la forma:

$$\phi : V_1 \longrightarrow V_2 \qquad \phi = [f_0, ..., f_m]$$

donde las funciones $f_i \in \bar{K}(V_1)$ tienen la propiedad de que para cada punto $P \in V_1$ en el que $f_0, ..., f_m$ están definidas y exista al menos un valor de i para el cual $f_i(P) \neq 0$:

$$\phi(P) = [f_0(P), ..., f_m(P)] \in V_2.$$

Si V_1 y V_2 están definidas sobre K, entonces $G_{\bar{K}/K}$ actúa en ϕ de la siguiente manera:

$$\phi^\sigma(P) = [f_0^\sigma(P), ..., f_m^\sigma(P)].$$

Nótese que para $P \in V_1$ tenemos la fórmula:

$$\phi(P)^\sigma = \phi^\sigma(P^\sigma),\ \forall \sigma \in G_{\bar{K}/K}.$$

Si además, existe algún $\lambda \in \bar{K}^*$ tal que $\lambda f_0, ..., \lambda f_m \in K(V_1)$, entonces ϕ se dice que está definida sobre K. Nótese que $[f_0, ..., f_m]$ y $[\lambda f_0, ..., \lambda f_m]$ definen la misma aplicación en los puntos. Como es habitual, ϕ está definido sobre K sí y solo si $\phi = \phi^\sigma$ para todo $\sigma \in G_{\bar{K}/K}$.

Definición 2.23 (Anillo local de V en P)**.** El anillo local de V en P, denotado como $\bar{K}[V]_P$, es el cuerpo de polinomios tales que:

$$\bar{K}[V]_P = \{F \in \bar{K}(V) :\ F = f/g \text{ para algún } f,\ g \in \bar{K}[V] \text{ con } g(P) \neq 0\}.$$

Nótese que si $F = f/g \in \bar{K}[V]_P$, entonces $F(P) = f(P)/g(P)$ está bien definido.

Definición 2.24 (Función regular)**.** Una función $f \in \bar{K}(V)$ se dice que es regular (o definida) en P si $f \in \bar{K}[V]_P$.

Definición 2.25 (Aplicación racional regular)**.** Sean $V_1 \subset \mathbb{P}^n$ y $V_2 \subset \mathbb{P}^m$ variedades proyectivas, entonces una aplicación racional:

$$\phi = [f_0, ..., f_m] : V_1 \longrightarrow V_2$$

es regular (o definida) en $P \in V_1$ si existe una función $g \in \bar{K}(V_1)$ tal que

(i) cada gf_i es regular en P,

(ii) hay algún i para el que $(gf_i)(P) \neq 0$.

Si existe g, entonces asignamos

$$\phi(P) = [(gf_0)(P), ..., (gf_m)(P)].$$

Sean $V_1 \subset \mathbb{P}^m$ y $V_2 \subset \mathbb{P}^n$ variedades proyectivas. Recordemos que las funciones en $\bar{K}(V_1)$ pueden describirse como cocientes de polinomios homogéneos en $\bar{K}[X_0, ..., X_m]$ teniendo el mismo grado. Esto se debe a que debe conservarse la relación de equivalencia del espacio proyectivo. Entonces, multiplicando la aplicación racional $\phi = [f_0, ..., f_n]$ por un polinomio homogéneo que "elimine los denominadores "de cada f_i, obtenemos la siguiente definición alternativa de aplicación racional:

Definición 2.26. Sean $V_1 \subset \mathbb{P}^n$ y $V_2 \subset \mathbb{P}^m$ variedades proyectivas, entonces una aplicación racional $\phi : V_1 \longrightarrow V_2$ es una aplicación de la forma:

$$\phi(P) = [\phi_0(P), ..., \phi_m(P)],$$

donde

(i) $\phi_i(X) \in \bar{K}[X] = \bar{K}[X_0, ..., X_m]$ son polinomios homogéneos del mismo grado, no todos en $I(V_1)$, así existe al menos un ϕ_i tal que $\phi_i(P) \neq 0$.

(ii) para todo $f \in I(V_2)$,

$$f(\phi_0(X), ..., \phi_m(X)) \in I(V_1).$$

Entonces, $\phi(P)$ está bien definido siempre que algún $\phi_i(P) \neq 0$. Sin embargo, incluso si todos los $\phi_i(P) = 0$, puede ser posible alterar ϕ tal que $\phi(P)$ tenga sentido. Lo precisamos de la manera siguiente:
Una aplicación racional $\phi = [\phi_0, ..., \phi_m] : V_1 \longrightarrow V_2$ como en el caso anterior es regular (o definida) en $P \in V_1$ si existen polinomios homogéneos $\psi_0, ..., \psi_m \in \bar{K}[X]$ tales que

(i) $\psi_0, ..., \psi_m$ tienen el mismo grado,

(ii) $\phi_i\psi_j \equiv \phi_j\psi_i \ (mod\ I(V_1))$ para todo i,j tales que $0 \leq i, j \leq m$. De esta manera, tenemos que $\frac{\phi_i}{\psi_i} \sim \frac{\phi_j}{\psi_j}$.

(iii) $\psi_i(P) \neq 0$ para algún i.

Si esto ocurre, entonces fijamos: $\phi(P) = [\psi_0(P), ..., \psi_m(P)]$ como en el caso anterior, una aplicación racional que es regular en todo punto se llama *morfismo*.

Definición 2.27 (Variedades isomorfas)**.** Sean V_1 y V_2 variedades. Decimos que V_1 y V_2 son isomorfas y escribimos $V_1 \cong V_2$, si existen morfismos $\phi : V_1 \longrightarrow V_2$ y $\psi : V_2 \longrightarrow V_1$ tales que $\psi \circ \phi$ y $\phi \circ \psi$ son las aplicaciones identidad sobre V_1 y V_2 respectivamente. Decimos que V_1/K y V_2/K son isomorfas sobre K si ϕ y ψ pueden ser definidas sobre K.
Nótese que tanto ϕ como ψ tienen que ser morfismos, no solamente aplicaciones racionales.

Ejemplo 2.28. *Sea V la variedad*

$$V : X^2 + Y^2 = Z^2.$$

Consideremos la aplicación racional:

$$\phi : V \longrightarrow \mathbb{P}^1, \qquad \phi[X, Y, Z] = [X + Z, Y].$$

ϕ es regular en todo punto de V, por la definición de aplicación racional regular, excepto posiblemente en $[1, 0, -1]$, el punto donde $X + Z = Y = 0$. Sin embargo, usando:

$$(X + Z)(X - Z) \equiv -Y^2 \ mod(I(V)),$$

tenemos

$$\phi = [X + Z, Y] = [X^2 - Z^2, Y(X - Z)] \equiv [-Y^2, Y(X - Z)] = [-Y, X - Z].$$

Entonces

$$\phi([1, 0, -1]) = [0, 2] = [0, 1].$$

Por lo tanto ϕ es regular en todo punto de V, es decir ϕ es un morfismo. Análogamente, se puede comprobar que la aplicación

$$\psi : \mathbb{P}^1 \longrightarrow V, \qquad \psi[S, T] = [S^2 - T^2, 2ST, S^2 + T^2],$$

es un morfismo, ya que es regular para todo $P \in \mathbb{P}$. Por lo tanto, V y $\mathbb{P}^1$ son isomorfas.

Ejemplo 2.29. *Usando la definición de aplicación racional, vemos que la aplicación:*

$$\phi : \mathbb{P}^2 \longrightarrow \mathbb{P}^2, \qquad \phi = [X^2, XY, Z^2]$$

es regular en todo punto salvo en $[0, 1, 0]$.

Ejemplo 2.30. *Sea V la variedad*

$$V : Y^2Z = X^3 + X^2Z$$

y consideremos las siguientes aplicaciones:

$$\begin{array}{ll} \psi : \mathbb{P}^1 \longrightarrow V, & \psi = [(S^2 - T^2)T, (S^2 - T^2)S, T^3], \\ \phi : V \longrightarrow \mathbb{P}^1, & \phi = [Y, X]. \end{array}$$

Aquí ψ es un morfismo construido de la siguiente manera:

$$X = T, \quad Y = S, \qquad Z = \frac{X^3}{Y^2 - X^2},$$

el cual reescribiendo para eliminar los denominadores nos deja

$$X = (S^2 - T^2)T, \qquad Y = (S^2 - T^2)S, \qquad Z = T^3.$$

Por otro lado ϕ no es regular en $P = [0, 0, 1]$ ya que, $\phi_1(P) = \phi_2(P) = 0$ y $P \in V$. Enfatizamos que, pese a que las composiciones $\phi \circ \psi$ y $\psi \circ \phi$ son la aplicación identidad, las aplicaciones ϕ y ψ no son isomorfismos, porque ϕ no es un morfismo.

Ejemplo 2.31. *Consideremos las variedades:*

$$V_1 : X^2 + Y^2 = Z^2 \qquad y \qquad V_2 : X^2 + Y^2 = 3Z^2$$

no son isomorfas sobre $\mathbb{Q}$ *ya que* $V_2(\mathbb{Q}) = \emptyset$*. Para ello supongamos que* $[x, y, z] \in V_2(\mathbb{Q})$*, con* $x, y, z \in \mathbb{Z}$ *y* $gcd(x, y, z) = 1$ *por simplicidad en el espacio proyectivo. Entonces*

$$x^2 + y^2 \equiv 0 (mod\ 3).$$

Como -1 *no es un cuadrado módulo* 3*, esto implica que*

$$x \equiv y \equiv 0 (mod\ 3).$$

Por lo tanto x^2 *e* y^2 *son divisibles por* 3^2*. Por la ecuación de* V_2 *sabemos que* 3 *también divide* z*, lo cual contradice la hipótesis de que* $gcd(x, y, z) = 1$*. Por otro lado,* $V_1(\mathbb{Q})$ *contiene muchos puntos (más precisamente,* $V_1(\mathbb{Q}) = \mathbb{P}^1(\mathbb{Q})$ *del Ejemplo 2.28). Sin embargo, las variedades* V_1 *y* V_2 *son isomorfas sobre* $\mathbb{Q}(\sqrt{3})$ *con isomorfismo dado por*

$$\phi : V_1 \longrightarrow V_2, \qquad \phi = [X, Y, \sqrt{3}Z].$$

2.4. Puntos singulares

En el estudio de los objetos geométricos, surge un interés particular sobre si son suaves. La siguiente definición formaliza esta noción en términos de las derivadas de las aplicaciones.

Definición 2.32 (Singularidad en el espacio afín)**.** Sea V una variedad afín, $P \in V$ y $f_1, ..., f_m \in \bar{K}[X]$ un conjunto de generadores de $I(V)$. Entonces V es suave (o no singular) en P si la matriz $m \times n$:

$$\left(\frac{\partial f_i}{\partial X_j}(P) \right)_{\substack{1 \le i \le m \\ 1 \le j \le n}} \tag{2.1}$$

tiene rango $n - dim(V)$. Si V es no singular en todo punto, decimos que V es suave (o no singular).

Ejemplo 2.33. *Sea* V *la variedad algebraica generada por un polinomio no constante:*

$$V : f(X_1, ..., X_n) = 0.$$

Por lo tanto $P \in V$ *es un punto singular sí y solo sí:*

$$\frac{\partial f}{\partial X_1}(P) = ... = \frac{\partial f}{\partial X_n}(P) = 0.$$

Como P *también satisface* $f(P) = 0$*, esto nos da* $n + 1$ *ecuaciones para las* n *coordenadas de cualquier punto singular.*

Ejemplo 2.34. *Consideremos las dos variedades:*

$$V_1 : Y^2 = X^3 + X \qquad y \qquad V_2 : Y^2 = X^3 + X^2.$$

Usando el Ejemplo 2.33, vemos que cualquier punto singular en V_1 o V_2 satisface respectivamente:

$$V_1^{sing} : 2Y = 3X^2 + 1 = 0 \qquad y \qquad V_2^{sing} : 2Y = 3X^2 + 2X = 0.$$

De la misma manera deben de ser puntos en V_1 o V_2 respectivamente.
Por lo que V_1 es no singular, mientras que V_2 tiene un punto singular, $(0, 0)$. La figura 2.1 ilustra la diferencia:

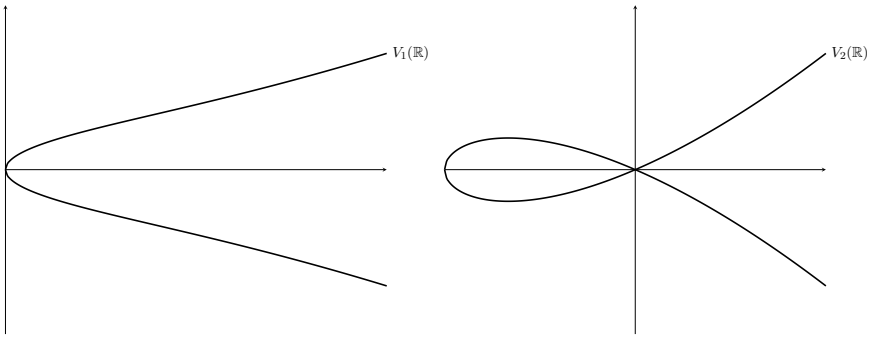

Figura 2.1: Grafos de V_1 y V_2.

Definición 2.35 (Singularidad en el espacio proyectivo)**.** Sea V una variedad proyectiva, $P \in V$ y elijamos $\mathbb{A}^n \subset \mathbb{P}^n$ con $P \in \mathbb{A}^n$. Entonces V es suave (o no singular) en P si $V \cap \mathbb{A}^n$ es no singular en P.

Proposición 2.36. *Sea E la curva dada por la ecuación*

$$y^2 = x^3 + Ax + B,$$

donde $A, B \in \mathbb{Q}$. La cual se escribe en el espacio proyectivo $\mathbb{P}^2$ como

$$ZY^2 = X^3 + AXZ^2 + BZ^3.$$

Entonces, E es no singular sí y solo si $\Delta_E = 4A^3 + 27B^2 \neq 0$, donde Δ_E se le conoce como discriminante de E.

Demostración. Para la demostración, siguiendo con la definición de singularidad en el espacio proyectivo. Tomaremos en primer lugar $U_1 \subset \mathbb{P}^2$ dado por $[x, y, 1]$ y en segundo lugar $U_2 \subset \mathbb{P}^2$ dado por $[x, 1, z]$, donde se demostrará la no singularidad del punto $[0, 1, 0]$.
En primer lugar tomemos $f(x, y) = x^3 + Ax + B - y^2$ como el polinomio de definición de E en U_1. Por el Ejemplo 2.33, sabemos que nuestra variedad es singular si existe un punto $P = (x, y)$ tal que

$$\frac{\partial f}{\partial x}(P) = \frac{\partial f}{\partial y}(P) = 0.$$

Derivando obtenemos que para ello

$$\begin{cases} 3x^2 + A & = 0, \\ -2y & = 0. \end{cases}$$

De aquí sacamos entonces que dichos puntos P serían los puntos

$$P_{\pm} = \left(\pm\sqrt{\frac{-A}{3}}, 0 \right),$$

de manera que comprobamos si estos puntos satisfacen $f(P_{\pm}) = 0$. Entonces tenemos

$$\left(\pm\sqrt{\frac{-A}{3}} \right)^3 + A \left(\pm\sqrt{\frac{-A}{3}} \right) + B = 0.$$

Simplificando la anterior expresión llegamos a

$$4A^3 + 27B^2 = 0.$$

Es decir, $\Delta_E = 0$.

A continuación nos movemos a U_2. Recordemos que vimos en el Ejemplo 2.20 que el único punto de E en U_2 es $[0, 1, 0]$, que en coordenadas en U_2 es $Q = (0, 0)$. Ahora el polinomio de definición de E en U_2 $g(x, z) = z - (x^3 + Axz^2 + Bz^3)$. Para ver si Q es un punto singular de E tendremos que ver si $\frac{\partial g}{\partial x}(Q) = \frac{\partial g}{\partial z}(Q) = 0$:

$$\begin{cases} -3x^2 - Az^2 = 0, \\ 1 - 2Axz - 3Bz^2 = 0. \end{cases}$$

Evaluando en $(x, z) = (0, 0)$ vemos que la segunda ecuación no se cumple y por lo tanto $[0, 1, 0]$ nunca es un punto singular de E. □

2.5. Curvas algebraicas

Las curvas algebraicas son variedades proyectivas de dimensión 1. De ahora en adelante todas las curvas mencionadas se tratarán de curvas algebraicas.

2.5.1. Aplicaciones entre curvas

Empezamos con el resultado fundamental, que para curvas suaves, una aplicación racional se define en todo punto.

Proposición 2.37. *Sea C una curva, sea $V \subset \mathbb{P}^n$ una variedad, sea $P \in C$ un punto suave, y sea $\phi : C \longrightarrow V$ una aplicación racional. Entonces ϕ es regular en P. En particular, si C es suave, entonces ϕ es un morfismo.*

Demostración. Ver [13, II.2.1]. □

Ejemplo 2.38. *Sea C/K una curva suave y sea $f \in K(C)$ una función. Entonces f define una aplicación racional, que también denotamos con f*

$$f : C \longrightarrow \mathbb{P}^1, \qquad P \longmapsto [f(P), 1].$$

Por la proposición anterior, esta aplicación es realmente un morfismo. Dado explícitamente por

$$f(P) = \begin{cases} [f(P), 1] & \text{si } f \text{ es regular en } P, \\ [1, 0] & \text{si } f \text{ tiene un polo en } P. \end{cases}$$

Por el contrario, sea

$$\phi : C \longrightarrow \mathbb{P}^1, \qquad \phi = [f, g]$$

una aplicación racional definida sobre K. Entonces o bien $g = 0$, en cuyo caso ϕ es la aplicación constante $\phi = [1, 0]$, o bien ϕ es la aplicación correspondiente a la función $f/g \in K(C)$.
Tenemos entonces una correspondencia uno a uno

$$K(C) \cup \{\phi\} \longleftrightarrow \{\text{aplicaciones } C \to \mathbb{P}^1 \text{ definido sobre } K\}.$$

Habitualmente se identifican implícitamente estos dos conjuntos.

Teorema 2.39. *Sean C_1 y C_2 curvas y sea $\phi : C_1 \to C_2$ un morfismo de curvas. Entonces ϕ es o bien constante o bien sobreyectivo.*

Demostración. Véase [6, II.6.8] □

2.5.2. Género de una curva

El género de una curva es un invariante numérico de una curva algebraica.

Existen muchas maneras de definir y calcular el género, pero para este trabajo nos remitiremos al uso de la llamada fórmula de Plücker:

Teorema 2.40. *Sea C la curva $C : f(x, y) = 0$ en $\mathbb{A}^2$ y sea $d = grado(f)$. Entonces tenemos que si C es suave, se tiene que su género es:*

$$g(C) = \frac{1}{2}(d-1)(d-2).$$

Demostración. Ver [8, V.2.1]. □

Ejemplo 2.41. *Sea E la curva elíptica $E : y^2 = x^3 + Ax + B$, $\Delta_E \neq 0$, entonces*

$$g(E) = \frac{(3-1)(3-2)}{2} = 1.$$

Nota 2.42. *En general si la curva C no es lisa*

$$g(C) = \frac{1}{2}(d-1)(d-2) - s$$

donde s es un entero que depende de las singularidades de C.

CAPÍTULO 3
Curvas elípticas

Uno de los temas más estudiados en la geometría algebraica son las llamadas curvas elípticas. A lo largo de este capítulo, al igual que en el anterior, se utilizarán los conceptos explicados en [14, I].

3.1. Forma normal de Weierstrass

En primer lugar, definimos la llamada forma normal de Weierstrass, la expresión más común para expresar curvas elípticas.

Definición 3.1 (Forma normal de Weierstrass)**.** Se conoce como forma normal de Weierstrass a las ecuaciones de la forma:

$$y^2 = x^3 + ax^2 + bx + c,$$

donde $a, b, c \in \mathbb{Q}$.

Sin embargo, por simplicidad, a lo largo de este trabajo se utilizará la siguiente forma de Weierstrass:

$$y^2 = x^3 + Ax + B.$$

Para llegar a esta fórmula, primero se parte de la anterior:

$$y^2 = x^3 + ax^2 + bx + c,$$

a continuación sustituimos x por $(x - \frac{a}{3})$ obteniendo la ecuación

$$y^2 = x^3 + Ax + B \quad \text{con} \quad \begin{cases} A = \frac{1}{3}\left(3b - a^2\right), \\ B = \frac{1}{27}\left(2a^3 - 9ab + 27c\right). \end{cases}$$

A raíz de esta forma definimos las curvas elípticas.

Definición 3.2 (Curva elíptica)**.** Una curva elíptica E sobre un cuerpo K es una curva algebraica de la forma $y^2 = x^3 + Ax + B$ donde $A, B \in K$ tal que $\Delta_E = 4A^3 + 27B^2 \neq 0$.

Nota 3.3. *Recordemos por el Ejemplo 2.20 que si* $E : y^2 = x^3 + Ax + B$ *con* $A, B \in K$, *entonces* $\mathcal{O} = [0, 1, 0] \in E(K)$. *Además por el Ejemplo 2.41 se tiene que si* $\Delta_E \neq 0$ *entonces* $g(E) = 1$.

En general, se puede demostrar[1] *que toda curva lisa de género* 1 *sobre un cuerpo* K *de característica* 0 *con un punto* K*-racional tiene un modelo de la forma* $y^2 = x^3 + Ax + B$. *Esa es la definición general de curva elíptica.*

3.2. Ley de las tangentes y las secantes

En una curva elíptica E definida sobre un cuerpo K, existe una manera de obtener puntos racionales a partir de puntos ya conocidos. Este método se conoce como la *Ley de las tangentes y las secantes*. Este consiste en tomar dos puntos $P_1, P_2 \in E(K)$ y obtener un tercer punto $P_1 * P_2 \in E(K)$. Supongamos que $P_1 = (x_1, y_1)$ y $P_2 = (x_2, y_2)$ son distintos. La recta secante que pasa por ambos tiene por ecuación $y = \lambda x + \nu$, donde $\lambda = \frac{y_2 - y_1}{x_2 - x_1}$ y $\nu = y_1 - \lambda x_1 = y_2 - \lambda x_2$. La recta R interseca a E en un tercer punto (x_3, y_3). De esta manera, y sabiendo que la ecuación de la curva es $y^2 = x^3 + Ax + B$, queremos obtener el valor de (x_3, y_3). Sabemos que, por construcción, la recta interseca a la curva en los puntos (x_1, y_1), (x_2, y_2), por lo tanto sustituimos $y = \lambda x + \nu$ en la ecuación de la curva para obtener:

$$y^2 = (\lambda x + \nu)^2 = x^3 + Ax + B.$$

Llevando todo al mismo lado tenemos:

$$0 = x^3 + (-\lambda^2)x^2 + (A - 2\lambda\nu)x + (B - \nu^2).$$

Esto es una ecuación cúbica en x y sus raíces son los valores $x_1,\ x_2,\ x_3$ que estábamos buscando, entonces

$$x^3 + (-\lambda^2)x^2 + (A - 2\lambda\nu)x + (B - \nu^2) = (x - x_1)(x - x_2)(x - x_3).$$

Desarrollando la ecuación en función de las raíces e igualando los coeficientes de x^2 de ambos lados, obtenemos que

$$-\lambda^2 = -x_1 - x_2 - x_3,$$

esto resulta en que las coordenadas $P_1 * P_2 = (x_3, y_3)$ pueden ser obtenidos de la siguiente manera:

$$x_3 = \lambda^2 - x_1 - x_2, \qquad y_3 = \lambda x_3 + \nu. \tag{3.1}$$

Así hemos obtenido que $P_3 \in E(K)$.

En el caso en el que $P_1 = P_2$, entonces se toma la recta tangente a E que pasa por P_1. En este caso la pendiente de la recta tangente viene dada por

$$\lambda = \frac{dy}{dx}\Big|_{P_1} = \frac{f'(x_1)}{2y_1}, \tag{3.2}$$

[1] Una consecuencia del Teorema de Rieman-Roch [13, II.5.4]

donde $f(x) = x^3 + Ax + B$. De forma análoga se obtiene $P_1 * P_1 \in E(K)$.

De modo que, empezando con dos puntos $P,\ Q \in E(K)$ y trazando la recta a través de P y Q, generamos dos escenarios distintos:

(i) Si $P \neq Q$, la recta interseca a la curva en un tercer punto al que llamaremos $P * Q \in E(K)$.

(ii) Si $P = Q$, la recta será la tangente a la curva E en el punto P, la cual interseca en el punto que llamaremos $P * P \in E(K)$.

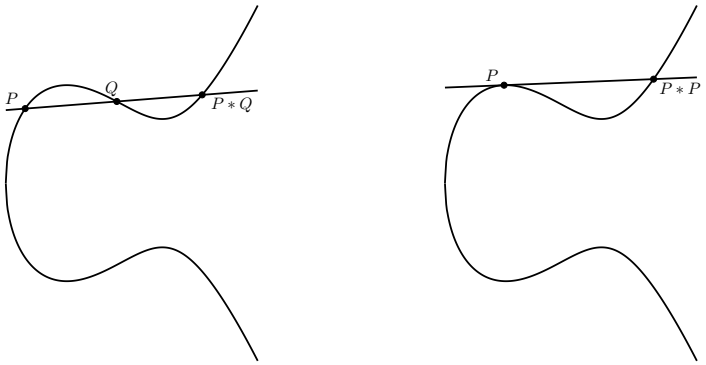

Figura 3.1: Composición de puntos en una cúbica

Mediante este método, comenzando con un punto racional, pueden obtenerse otros. A medida que vamos calculando los puntos nuevos, vemos que se define una estructura entre ellos, la cual cobrará gran importancia.

Obsérvese que el método anterior sirve para puntos en $\mathbb{A}^2$. Nos falta ver que ocurre con el único punto $\mathcal{O}$ que esta en el infinito. Veamos como podemos determinar $P * \mathcal{O}$ si $P = (x_0, y_0) \in E(K)$. Para ello calculemos cuál es la recta que une $\mathcal{O}$ con un punto de la curva elíptica $P = [x_0, y_0, 1]$.
Sea la recta en el espacio proyectivo

$$\alpha X + \beta Y + \gamma Z = 0,$$

con $\alpha, \beta, \gamma \in K$. La recta tiene que pasar por el punto $\mathcal{O}$, por lo que

$$\alpha * 0 + \beta * 1 + \gamma * 0 = 0,$$

entonces $\beta = 0$. Esto nos deja con la recta $\alpha X + \gamma Z = 0$, como queremos que esta recta pase por el punto $P = (x_0, y_0)$, sustituimos y obtenemos:

$$\alpha x_0 + \gamma = 0 \longrightarrow x_0 = \frac{-\gamma}{\alpha}.$$

Por último, como la recta la representaremos en el espacio de puntos $[x, y, 1]$, esto nos deja:

$$\alpha X + \gamma = 0 \longrightarrow X = \frac{-\gamma}{\alpha} = x_0.$$

En otras palabras, la recta que une P con $\mathcal{O}$ es la recta $X = x_0$, una recta paralela al eje y.
Así hemos obtenido $P * \mathcal{O} = (x_0, -y_0) \in E(K)$.

Por último, el Ejemplo 2.20 nos dice que $\mathcal{O} * \mathcal{O} = \mathcal{O}$.

3.3. Ley de grupo

El método descrito en la sección previa define una operación $*$, que llamaremos composición, en $E(K)$. Pero esto no es suficiente para definir una estructura de grupo en $E(K)$. La siguiente definición permite solventar este problema:

Definición 3.4 (Suma de puntos)**.** Sea E una curva elíptica definida sobre un cuerpo K. Definimos la suma de $P \in E(K)$ y $Q \in E(K)$ como:

$$P + Q = \mathcal{O} * (P * Q).$$

Nota 3.5. *Nótese que, como la curva elíptica bajo la forma de Weierstrass es simétrica respecto del eje x, $P + Q$ es el punto simétrico a $P * Q$ respecto del eje x.*

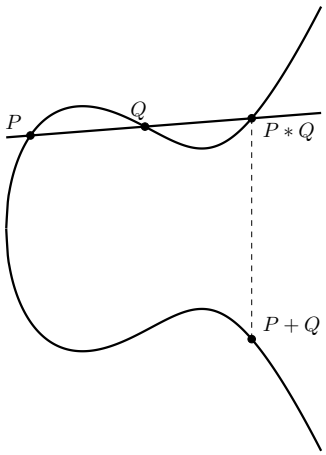

Figura 3.2: Suma de dos puntos

De esta manera, haciendo uso de la composición de puntos, definimos la operación de suma de puntos en una curva elíptica. Una vez establecida, queda demostrar que esta operación da estructura de grupo al conjunto de puntos racionales en la curva elíptica.

Teorema 3.6 (Estructura de grupo)**.** *Sea E una curva elíptica definida sobre un cuerpo K. Entonces $(E(K), +)$ es un grupo abeliano, donde $\mathcal{O}$ es el elemento neutro.*

Demostración. Esta demostración será dividida en las diferentes propiedades de los grupos abelianos.

- En primer lugar tenemos que comprobar que la operación + está contenida en $E(K)$, es decir, sean $P,\ Q \in E(K)$, entonces $P + Q \in E(K)$.
  Esto surge como consecuencia de la composición de puntos. Como hemos visto, con $P,\ Q \in E(K)$ sabemos que $P * Q \in E(K)$. Al tener $P + Q = \mathcal{O} * (P * Q)$, como $\mathcal{O} \in E(K)$, tenemos que $P + Q \in E(K)$.

- A continuación se demuestra que el grupo es abeliano, es decir, que para todo par de elementos $P, Q \in E(K)$ se cumple $P + Q = Q + P$. Esto será utilizado en los demás apartados de la demostración.
  Esta condición se cumple de manera bastante directa, ya que la recta que une P con Q hasta $P * Q$ (y por tanto $P + Q$) es la misma que la que une Q con P y por tanto obtenemos el mismo resultado.

- La siguiente propiedad a demostrar es la existencia de un elemento neutro. Este papel lo va a jugar $\mathcal{O} \in E(K)$
  Se tiene que al componer el punto $P * \mathcal{O}$ con $\mathcal{O}$, nos da el P original (ver Figura 3.3). Por lo que $P + \mathcal{O} = P$.

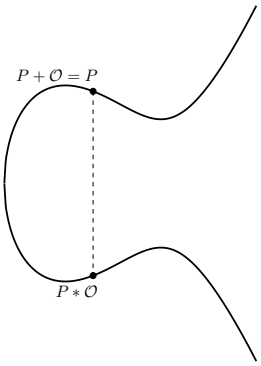

Figura 3.3: Verificación de que $\mathcal{O}$ es el elemento neutro

Veamos el caso $P = \mathcal{O}$:

$$\mathcal{O} + \mathcal{O} = \mathcal{O} * (\mathcal{O} * \mathcal{O}) = \mathcal{O} * \mathcal{O} = \mathcal{O}.$$

- La existencia de elementos inversos, es decir, para todo elemento P del grupo, existe un elemento $-P$ tal que $P + (-P) = \mathcal{O}$, se demuestra de manera similar. Para ello tomamos un punto P en la curva, tomamos también su reflejo respecto del eje x, al que denominaremos $-P$. Al trazar la recta que une ambos puntos, obtenemos $\mathcal{O}$ como tercer punto de corte, de manera que, $P + (-P) = \mathcal{O} * (P * (-P)) = \mathcal{O} * \mathcal{O} = \mathcal{O}$. Así hemos demostrado que $-P$ es el inverso de P.

- Por último queda demostrar la asociatividad de la operación, pero debido a su complejitud, no se escribirá en este trabajo. Puede consultarse en [13].

□

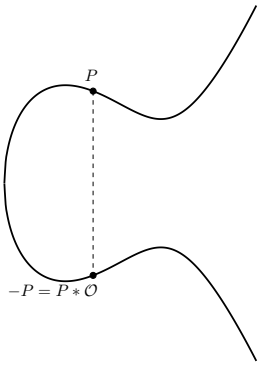

Figura 3.4: Inverso de un punto

3.4. Teorema de Mordell

Partiendo de la estructura de grupo definida por la operación de composición de puntos explicada anteriormente, surge el llamado Teorema de Mordell.

Teorema (Teorema de Mordell)**.** *Sea E una curva elíptica definida sobre $\mathbb{Q}$, entonces $(E(\mathbb{Q}), +)$ es un grupo abeliano finitamente generado.*

Demostración. La demostración de este teorema se encuentra en [13]. Debido a su complejidad no será desarrollada aquí. □

A raíz de este teorema, surge que $E(\mathbb{Q})$ es isomorfo a $\mathbb{Z}^r \oplus E(\mathbb{Q})_{tors}$ para algún entero r; r se le conoce como el rango de E y donde $E(\mathbb{Q})_{tors}$ es el grupo de puntos de torsión (puntos de orden finito) de $E(\mathbb{Q})$. Al grupo $E(\mathbb{Q})$ se le llama grupo de Mordell-Weil [2].

Sin embargo, a pesar de este teorema, quedan muchas cuestiones sin resolver en el campo de las curvas elípticas, como el cálculo del rango y el significado del mismo. De este último sale la famosa conjetura de Birch y Swinnerton-Dyer, uno de los problemas del milenio del Instituto Clay de Matemáticas.

CAPÍTULO 4
Puntos racionales en variedades algebraicas

4.1. Introducción

Una ecuación diofántica, es un polinomio en varias variables con coeficientes son racionales.
La forma más simple de una ecuación diofántica es una ecuación polinómica en una variable,

$$a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0 = 0.$$

Asumiendo que todo $a_i \in \mathbb{Z}$, ¿cómo podemos encontrar todas las soluciones enteras y racionales? El lema de Gauss nos da una respuesta simple. Si p/q es una solución racional, el lema de Gauss nos dice que q divide a_n y que p divide a_0. Esto nos da una pequeña lista de soluciones racionales y podemos sustituirlas dentro de la ecuación para determinar la solución de verdad.

Una vez nos movemos a las ecuaciones diofánticas de dos variables, la situación cambia dramáticamente. Supongamos que tenemos un polinomio $f(x, y)$ con coeficientes enteros y miremos a la ecuación

$$f(x, y) = 0.$$

De aquí surgen diferentes preguntas, de entre las cuales destacamos dos:

(a) ¿Existen soluciones racionales?

(b) ¿Existen infinitas soluciones racionales?

Estas preguntas han sido resueltas parcialmente, como por ejemplo la pregunta (b) para las curvas de género mayor que 1, lo cual veremos a continuación.

4.2. Clasificación

Habiendo ya definido tanto la dimensión de las variedades algebraicas como el género de las curvas algebraicas, el siguiente paso será agrupar las mismas en función

de estos parámetros. Si bien este campo está todavía abierto y hay diferentes aspectos por descubrir y desarrollar, se realizará lo más rigurosamente posible.

Por claridad, en la lista a continuación denotaremos dimensión como **d** y género como **g**. Para ilustrar los diferentes tipos de variedades algebraicas, se utilizarán problemas de la Aritmética de Diofanto, los cuales se nombrarán siguiendo la notación establecida en el Capítulo 1.

d = 0 Una variedad algebraica de dimensión 0 implica que estamos tratando de un punto.
Como ejemplo podemos ver el problema GI-11, el cual dice:

"*Dados dos números, sumar uno de ellos a un número y restar el otro de este mismo número, de modo que los respectivos resultados estén en una razón dada.*"

Es decir, dados los números a, b y $m > 1$, encontremos x tal que

$$x + a = m(x - b).$$

Aquí podemos ver que una vez tenemos los valores a, b, m solo existe una solución posible, para la cual Bachet dio la regla general $x = \frac{ma+b}{m-1}$.
Diofanto obtiene la solución $x = 140$ para $a = 20,\ b = 100,\ m = 3$.
Este tipo de variedades es muy común a lo largo de todo el libro GI de la Aritmética, pero van desapareciendo a medida que aumenta la complejidad de los problemas.

d = 1 Las variedades algebraicas de dimensión 1, como ya hemos comentado, se conocen como curvas algebraicas, y son las variedades estudiadas con más éxito a día de hoy. Estas curvas al dividirlas en función del género surgen tres grupos:

g = 0 Esta familia de curvas algebraicas puede no tener puntos racionales o tener infinitos y son las que comúnmente se conocen como cónicas (circunferencia, elipse, hipérbola y parábola) y son birracionalmente equivalentes a la recta proyectiva. En otras palabras, sea $C \subset \mathbb{P}^2$ tal que $C(\mathbb{Q}) \neq \emptyset$, entonces existe una parametrización tal que $C(\mathbb{Q}) \simeq \mathbb{P}^1(\mathbb{Q})$:

$$\begin{array}{rl} \mathbb{P}^1 & \longrightarrow C \\ [s,t] & \longmapsto [X(s,t), Y(s,t), Z(s,t)]. \end{array}$$

Como ejemplo podemos ver el problema GVI-8, el cual dice:
"*Encontrar un triángulo rectágulo tal que al añadir el área a la suma de los dos catetos se forme un número dado.*"
Es decir, dado a, encontrar x, y tales que

$$\frac{1}{2}xy + (x + y) = a.$$

Diofanto obtiene las soluciones $x = \frac{6}{35},\ y = \frac{102}{39}$ para el caso $a = 6$.
Mediante la sustitución $x = X/Z,\ y = Y/Z$ homogeneizamos la curva, obteniendo la forma siguiente:

$$C : XY + 2XZ + 2YZ = 2aZ^2.$$

De esta manera, despejando Y de manera que $Y = \frac{2aZ^2-2XZ}{X+2Z}$, y con las sustituciones $X = s,\ Z = t$, y eliminando los denominadores multiplicando por $X + 2Z$, obtenemos la parametrización

$$\begin{cases} X &= s(s+2t), \\ Y &= 2at^2 - 2st, \\ Z &= t(s+2t). \end{cases}$$

La cual establece una parametrización de $\mathbb{P}^1$ a la curva en el espacio proyectivo:

$$\begin{array}{rl} \mathbb{P}^1 & \longrightarrow C \\ [s,t] & \longmapsto [s(s+2t), 2at^2 - 2st, t(s+2t)]. \end{array}$$

g = 1 Para el caso de las curvas de género 1, tomaremos las curvas elípticas como representante, debido al desarrollo previo en Capítulo 3.
El problema que tomaremos como ejemplo es el GIV-24, el cual dice:

"*Descomponer un número dado en dos partes, tales que su producto sea la diferencia entre un cubo y su lado.*"

Es decir, dado a, encontrar x, y, z tales que

$$\begin{cases} z + y &= a, \\ zy &= x^3 - x. \end{cases}$$

Diofanto obtiene las soluciones $x = \frac{17}{9}$, $y = \frac{26}{27}$ y $z = \frac{136}{27}$ para el caso $a = 6$. Para mayor simplicidad en los cálculos reescribimos las ecuaciones de nuestro problema de la siguiente forma: de la primera ecuación obtenemos $y = a - z$, que sustituyendola en la segunda ecuación obtenemos:

$$y(a - y) = x^3 - x.$$

Ahora, mediante las sustituciones $x = -x,\ y = y + \frac{a}{2}$, se obtiene la forma de Weierstrass:

$$E_a : y^2 = x^3 - x + \frac{a^2}{4},$$

cuyo discriminante $\Delta_{E_a} = \frac{1}{16}\left(27a^4 - 64\right)$ es distinto de 0 para todo $a \in \mathbb{Q}$. Por lo tanto, tenemos que E_a es una curva elíptica.

Una vez que hemos visto que E_a es una curva elíptica, procedemos a buscar sus puntos racionales. Para ello nos apoyaremos en el artículo de Ezra Brown y Bruce T. Meyers [2]. En primer lugar se observa si sustituimos $y = a/2$ en la ecuación de E_a se obtiene $x(x + 1)(x - 1) = 0$. Por lo tanto se tiene los siguientes puntos en E_a:

$$P = \left(0, \frac{a}{2}\right), \qquad Q = \left(1, \frac{a}{2}\right), \qquad R = \left(-1, \frac{a}{2}\right).$$

Se observa que $P+Q=-R$. De esta manera y con las fórmulas explícitas, se pueden calcular muchos puntos racionales como:

$$\begin{array}{ll} 2P & = \left(\frac{1}{a^2}, \frac{-\frac{1}{2}a^4+1}{a^3}\right) \\ 2Q & = \left(\frac{-2a^2+4}{a^2}, \frac{-\frac{1}{2}a^4+6a^2-8}{a^3}\right) \\ P+2Q & = \left(\frac{1}{4}a^2, -\frac{1}{8}a^3\right) \\ 2P+Q & = \left(a^2+1, -a^3-\frac{3}{2}a\right) \end{array}$$

Como hemos comprobado, todos estos puntos pueden ser llevados de vuelta a soluciones del problema planteado por Diofanto.

De hecho, Brown y Meyers [2, Theorem 1] demuestran que $E_a(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$ si $a \geq 2$ y si $a \geq 4$ entonces P y Q son independientes (como elementos del grupo $E_a(\mathbb{Q})$), en particular el rango del grupo $E_a(\mathbb{Q})$ es ≥ 2. Así se obtienen infinitas soluciones al problema planteado por Diofanto.

Tomando la curva del problema de Diofanto para $a=6$, que nos queda con la ecuación:

$$E_3 : y^2 = x^3 - x + 9,$$

podemos ver que $E_a(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}\}$ y que P y Q son independientes. Es más, para E_3 se puede calcular que su rango es 2. Por lo tanto podemos expresar cualquier punto como una suma $mP+nQ$ para m, n números enteros. Si tomamos la solución de Diofanto al problema con $a=6$, $x=\frac{17}{9}$, $y=\frac{26}{27}$, que por la transformación anterior corresponde al punto $S=\left(-\frac{17}{9}, -\frac{55}{27}\right)$, el cual corresponde con el punto $2Q$.

g >1 Para las curvas de género mayor que 1, para hablar de la cantidad de puntos racionales que poseen es necesario mencionar el teorema de Faltings, el cual fue conjeturado por Mordell en 1922 [9].

Teorema (Teorema de Faltings)**.** *Sea C una curva algebraica de género >1 sobre $\mathbb{Q}$. Entonces C tiene un número finito de puntos racionales. Es decir,*

$$\#C(\mathbb{Q}) < \infty.$$

Demostración. Véase [4, 5]. □

En este caso encontramos un ejemplo en el problema AVI-17, el cual dice: "*Encontrar tres cuadrados cuya suma es un cuadrado y tales que el primero es el lado del segundo y el segundo es el lado del tercero.* "
Es decir, encontrar x^2, y^2, z^2 tales que

$$\begin{cases} x^2+y^2+z^2 & = \square, \\ x^2 & = y, \\ y^2 & = z. \end{cases}$$

Donde Diofanto encuentra las soluciones $x=\frac{1}{2}$ y $\square = \frac{9^2}{16^2}$. Este problema, denotando $w^2 = \square$ nos resulta en la ecuación:

$$w^2 = x^8 + x^4 + x^2.$$

Esta ecuación ha sido estudiada por Joseph L. Wetherell en su tesis [16]. Mediante el cambio de variable $w = xt$ la convierte en

$$C : t^2 = x^6 + x^2 + 1.$$

Se puede determinar que el género de la curva C es 2. Ahora, gracias al Teorema de Faltings, sabemos que tiene un número finito de puntos racionales. Wetherell demuestra que C solo tiene los siguientes 6 puntos afines

$$\left(\frac{1}{2}, \frac{9}{8}\right),\ \left(-\frac{1}{2}, \frac{9}{8}\right),\ \left(\frac{1}{2}, -\frac{9}{8}\right),\ \left(-\frac{1}{2}, -\frac{9}{8}\right),\ (0,1),\ (0,-1).$$

Así Wetherell completa el problema planteado por Diofanto.

d = 2 Las superficies algebraicas, son variedades algebraicas de dimensión 2, y debido a su complejidad, este apartado servirá como una simple ilustración de un tipo de superficie. Por otro lado, existe la llamada clasificación Enriques-Kodaira, la cual clasifica en diez clases distintas las superficies algebraicas; pero al incluir muchos conceptos nuevos y avanzados no se incluyen en esta memoria. El caso más sencillo de superficie algebraica es el de las superficies racionales. Es decir, aquellas que son isomorfas a $\mathbb{P}^2$. Un ejemplo de superficie algebraica, lo podemos encontrar en el problema GII-20, cuyo enunciado dice:

"*Encontrar dos números tales que la suma del cuadrado de cualquiera de los dos con el otro sea un cuadrado.*"

El problema pide obtener x e y tales que:

$$S : \begin{cases} x^2 + y &= u^2, \\ x + y^2 &= v^2. \end{cases}$$

Diofanto obtiene las soluciones $x = \frac{3}{13}$ e $y = \frac{19}{13}$.
Las soluciones del anterior sistema de ecuaciones definen una superficie algebraica S. René Pannekoek [10] estudió este caso obteniendo una parametrización de S. La siguiente es una pequeña modificación de la que aparece en [10]. Sin perdida de generalidad denotemos por S el cierre proyectivo de S cuyas ecuaciones son:

$$S : \begin{cases} X^2 + YZ &= U^2, \\ XZ + Y^2 &= V^2. \end{cases}$$

Definiendo:

$$\begin{cases} X(r,s,t) &= t(-r^2 + st)(r^2 + st), \\ Y(r,s,t) &= r(2r^4 - 4r^2st + 2s^2t^2 + rt^3), \\ U(r,s,t) &= t(3r^4 - 4r^2st + s^2t^2 + rt^3), \\ V(r,s,t) &= 2r^5 - 4r^3st + 2rs^2t^2 - st^4, \\ Z(r,s,t) &= t^2(4r^3 - 4rst + t^3). \end{cases}$$

tenemos la parametrización:

$$\begin{array}{rl} \mathbb{P}^2 & \longrightarrow S \\ [r,s,t] & \longmapsto [X(r,s,t), Y(r,s,t), U(r,s,t), V(r,s,t), Z(r,s,t)]. \end{array}$$

d >2 Finalmente sobre las variedades algebraicas de dimensión mayor que 2 no se conoce mucho a nivel general. En la Aritmética de Diofanto solo aparecen problemas de dimensión 3 y de dimensión 4.
Como ejemplo de dimensión 3, tenemos el problema GIII-5, cuyo enunciado dice:

"*Encontrar tres números cuya suma sea un cuadrado y la suma de dos cualesquiera exceda al tercero por un cuadrado.*"

Es decir, encontrar x, y, z tales que

$$\begin{cases} x+y+z & = \square, \\ y+z-x & = \square, \\ z+x-y & = \square, \\ x+y-z & = \square. \end{cases}$$

Para este problema, Diofanto encuentra las soluciones $x = 20,\ y = \frac{13}{2},\ z = \frac{45}{2}$.

Del mismo modo, como ejemplo de dimensión 4, tenemos el problema GIV-20, cuyo enunciado dice:

"*Encontrar cuatro números tales que el producto de dos cualesquiera incrementado en una unidad sea un cuadrado.*"

Es decir, encontrar x, y, z, w tales que

$$\begin{cases} yz+1 & = \square \\ zx+1 & = \square \\ xy+1 & = \square \\ xw+1 & = \square \\ yw+1 & = \square \\ zw+1 & = \square \end{cases}$$

Para este problema, Diofanto encuentra las soluciones $x = \frac{1}{16},\ y = \frac{33}{16},\ z = \frac{68}{16},\ w = \frac{105}{16}$.

CAPÍTULO 5
Cálculo con MAGMA de los problemas de la Aritmética

Uno de los objetivos de este trabajo, fue siempre el estudio de los problemas de la Aritmética desde el punto de vista algebraico. En lugar de obtener soluciones concretas, como hizo Diofanto, obtener todas las soluciones posibles a ellos. Esto, como hemos visto anteriormente, no es posible para la mayoría de los problemas en el estado actual de las matemáticas.
El estudio realizado en este trabajo ha consistido en calcular la dimensión de las variedades algebraicas generadas en cada problema. Después, para las que resultasen de dimensión 1, se calculó el género de la misma.

Para realizar este trabajo, se decidió utilizar la herramienta de álgebra computacional `Magma` [1], y el proceso a seguir ha consistido en varias partes:

- Transcripción de los problemas, dividiendo cada uno en ecuaciones, datos dados e incógnitas.
- Definir cuerpo de coeficientes y el espacio de variables de cada problema.
- Calcular la dimensión de la variedad generada por las ecuaciones enunciadas en el problema.

Este código se ecuentra en el Apéndice B.

5.1. Funcionamiento del código

Este proceso, fue condensado en diversos ficheros de código, los cuales fueron ejecutados localmente con MAGMA.

En el archivo *init.m*, el programa primero crea un directorio para cada libro, luego prosigue leyendo los ficheros de los libros, los cuales contienen los problemas, parseados de manera que delimitados por el símbolo ": ", queden de la siguiente manera

$$valores\ conocidos : incógnitas : [ecuaciones]$$

estando estos elementos separados por comas, como se puede ver por ejemplo en el problema AV-7:

$$a, b : x, y : [x + y - a, x^3 + y^3 - b].$$

Una vez obtenidos los valores, crea un archivo para cada problema en el que escribe la declaración del cuerpo de coeficientes, el espacio de variables y el esquema de las ecuaciones.
De manera que este código representa un problema en el que, dados a, b se pide encontrar los valores de x e y tales que:

$$\begin{cases} x + y & = a, \\ x^3 + y^3 & = b. \end{cases}$$

Estos archivos serán utilizados por el archivo *run.m* (Apéndice B) de la siguiente manera. En primer lugar, declara una función que se encargará de calcular y escribir la dimensión y en caso de ser de dimensión 1, escribir su género. Posteriormente, procede a crear archivos con el nombre `run + nombre del libro`, en los cuales escribe los comandos pertinentes para la ejecución completa de los problemas del libro y carga la función anterior ubicada en el archivo *cuenta.m* (Apéndice B). Estos son ejecutados después, guardando su salida en unos ficheros llamados `out + nombre del libro`, donde se pueden leer de manera clara todos los datos calculados.

5.2. Tablas de resultados

Tras todo este proceso, los datos fueron estructurados en dos tablas, la primera conteniendo las dimensiones (y género para los casos de dimensión 1) de cada problema, y la segunda con la cantidad de problemas de cada tipo de cada libro.

Tabla 5.1: Dimensiones (y género)

	GI	GII	GIII	GIV	GV	GVI	AIV	AV	AVI	AVII
1	0	1(0)	3	0	2	3	2	2	1(0)	1
2	0	1(0)	3	0	2	3	2	2	1(0)	3
3	0	1(0)	3	1(0)	3	2	2	2	1(0)	3
4	0	1(0)	3	1(0)	3	2	2	2	1(0)	3
5	0	1(0)	3	1(0)	3	2	2	2	1(0)	3
6	0	0	3	3	3	1(0)	2	2	1(0)	1
7	0	1(0)	2	3	3	1(0)	2	0	1(0)	3
8	0	1(0)	3	1(0)	3	1(0)	2	0	2	2
9	0	1(0)	3	1(0)	1	1(0)	2	0	2	2
10	0	1(0)	3	1(0)	1	2	1(0)	0	2	2
11	0	2	3	1(0)	2	2	1(0)	0	2	1
12	0	2	3	1(0)	2	2	1(0)	0	2	1
13	0	2	3	2	2	2	1(0)	2	2	2
14	1(0)	2	3	2	3	3	1(0)	2	2	2
15	0	2	3	0	3	3	0	2	2	3

Continuación de la tabla 5.1

	GI	GII	GIII	GIV	GV	GVI	AIV	AV	AVI	AVII
16	0	1(0)	3	3	3	3	1(0)	2	2	2
17	0	1(0)	3	3	3	3	0		1(2)	3
18	0	0	3	2	3	3	0		3	3
19	0	2	4	3	3	3	0		3	
20	0	2	2	4	2	3	0		3	
21	0	2	2	2	3	3	0		3	
22	1(0)	2		3	3	3	0		2	
23	1(0)	2		3	3	2	2		2	
24	1(0)	2		1(1)	3	3	2			
25	1(0)	2		1(0)	3		2			
26	0	1(0)		2	3		2			
27	0	1(0)		2	3		2			
28	0	2		2	3		2			
29	0	2		3	3		2			
30	0	2		3	1(0)		2			
31	0	2		1(0)			2			
32	0	3		2			2			
33	0	3		1(0)			2			
34	0	3		0			2			
35	0	3		0			2			
36	0			0			1(0)			
37	0			0			1(0)			
38	0			3			1(0)			
39	0			2			1(0)			
40				2			2			
41							2			
42							2			
43							2			
44							2			

A continuación la tabla agrupando los problemas dentro de cada libro en función de su dimensión (**d**).

Tabla 5.2: Número de problemas en función de la dimensión

d	GI	GII	GIII	GIV	GV	GVI	AIV	AV	AVI	AVII	Total
0	34	2	0	7	0	0	7	6	0	0	56
1	5	13	0	12	3	4	10	0	8	4	59
2	0	16	3	10	6	8	27	10	11	6	97
3	0	4	17	10	21	12	0	0	4	8	76
4	0	0	1	1	0	0	0	0	0	0	2

Se ha optado por no hacer subdivisión de los problemas de dimensión 1 por género, ya que solo existen dos que no tienen género 0: GIV-24 (con $\mathbf{g} = 1$) y AVI-17 (con $\mathbf{g} = 2$).

Como podemos ver en la tabla anterior, la cantidad de problemas de dimensiones mayores que 1 supera considerablemente a los otros, esto pone en una situación interesante la resolubilidad de estos problemas.
Por un lado tenemos al menos una solución de cada problema. Para dimensión 0, tenemos todas las posibles soluciones, y para dimensión 1, tenemos también todas las soluciones en el caso de los problemas que tienen género 0. Los otros dos problemas de dimensión 1, son los tratados en el capítulo anterior como los ejemplos de género 1 y género mayor que 1. Sin embargo, una vez abandonamos esos dos tipos de variedades algebraicas la cosa se complica.
A día de hoy no existen métodos para obtener todos los puntos racionales de todos los tipos de variedades algebraicas y en algunos casos, ni siquiera se sabe si la cantidad de puntos racionales es finita o infinita. Por estos motivos, pese a tener soluciones concretas de todos los problemas de la Aritmética, mientras este problema persista, esta obra seguirá sin estar completamente resuelta.

APÉNDICE A
Problemas de Diofanto

En este apéndice se recogen todos los problemas que se conocen actualmente de la Aritmética. Estos problemas se han recogido de los *Conspectus* (lista de los problemas) del los trabajos de Heath [7] y Sesiano [12], al igual que del libro de Benito Muñoz, Fernández Moral y Sánchez Benito [3].

A lo largo de estos problemas se utilizarán como valores ya conocidos unas letras y como incógnitas otras que estarán a continuación:

Conocidos: a,b,c,d,e,l,m,n

Incógnitas: o,p,q,r,s,t,u,v,w,x,y,z

Libro GI

1. Problema 1: $x + y = a,\ x - y = b$
2. Problema 2-4: $x \pm y = a,\ x = my$
3. Problema 3: $x + y = a,\ x = my + b$
4. Problema 5-6: $x + y = a,\ \frac{x}{m} \pm \frac{y}{n} = b$
5. Problema 7-8: $x \mp a = m(x \mp b)$
6. Problema 9-10: $a \mp x = m(b - x)$
7. Problema 11: $x + a = m(x - b)$
8. Problema 12: $a = x + y = z + w,\ x = mw,\ z = ny$
9. Problema 13: $a = x + y = z + w = u + v,\ x = mw,\ z = nv,\ u = by$
10. Problema 14: $xy = m(x + y)$
11. Problema 15: $x + a = m(y - a),\ y + b = n(x - b)$
12. Problema 16: $x + y = a\ y + z = b\ z + x = c$

13. Problema 17: $x+y+z=a\ y+z+w=b\ z+w+x=c\ w+x+y=d$
14. Problema 18: $x+y-z=a\ y+z-x=b\ z+x-y=c$
15. Problema 19: $x+y+z-w=a\ y+z+w-x=b,\ z+w+x-y=c\ w+x+y-z=d$
16. Problema 20: $x+y+z=a\ x+y=mz\ y+z=nx$
17. Problema 21: $x-y=\frac{1}{m}z,\ y-z=\frac{1}{n}x,\ z-a=\frac{1}{b}y$
18. Problema 22: $x-\frac{1}{m}x+\frac{1}{a}z=y-\frac{1}{n}y+\frac{1}{m}x=z-\frac{1}{a}z+\frac{1}{n}y$
19. Problema 23: $x-\frac{1}{m}x+\frac{1}{b}w=y-\frac{1}{n}y+\frac{1}{m}x=z-\frac{1}{a}z+\frac{1}{n}y=w-\frac{1}{b}w+\frac{1}{a}z$
20. Problema 24: $x+\frac{1}{m}(y+z)=y+\frac{1}{n}(z+x)=z+\frac{1}{a}(x+y)$
21. Problema 25: $x+\frac{1}{m}(y+z+w)=y+\frac{1}{n}(x+z+w)=z+\frac{1}{a}(x+y+w)=w+\frac{1}{b}(x+y+z)$
22. Problema 26: $ax=y^2,\ bx=y$
23. Problema 27-30: $x\pm y=a\ xy=b$
24. Problema 28-29: $x+y=a\ x^2\pm y^2=b$
25. Problema 31-32: $\frac{x}{y}=m,\ \frac{x^2+y^2}{x\pm y}=n$
26. Problema 33-34: $\frac{x}{y}=m,\ \frac{x^2-y^2}{x\pm y}=n$
27. Problema 35: $\frac{x}{y}=m,\ \frac{y^2}{x}=n$
28. Problema 36: $\frac{x}{y}=m,\ \frac{y^2}{y}=n$
29. Problema 37-38: $\frac{x}{y}=m,\ \frac{y^2}{x\pm y}=n$
30. Problema 39: $(a+x)b-(b+x)a=(b+x)a-(a+b)x$

Libro GII

1. Problema 1-2: $x\pm y=\frac{1}{m}(x^2\pm y^2)$
2. Problema 3: $xy=m(x+y)$
3. Problema 4-5: $x^2\pm y^2=m(x\mp y)$
4. Problema 6: $x-y=a,\ (x^2-y^2)-(x-y)=b$
5. Problema 7: $x^2-y^2=m(x-y)+b$
6. Problema 8: $x^2+y^2=a^2$
7. Problema 9: $x^2+y^2=a^2+b^2$

8. Problema 10: $x^2 - y^2 = a$
9. Problema 12: $a - x = u^2,\ b - x = v^2$
10. Problema 11-13: $x \pm a = u^2,\ x \pm b = v^2$
11. Problema 14-15: $x + y = a,\ z^2 \pm x = u^2,\ z^2 \pm y = v^2$
12. Problema 16: $x = my,\ x + a^2 = u^2,\ y + a^2 = v^2$
13. Problema 17-(18): $(x + y + z = e),\ x - (\frac{1}{m}x + a) + (\frac{1}{d}z + c) = y - (\frac{1}{n}y + b) + (\frac{1}{m}x + a) = z - (\frac{1}{d}z + c) + (\frac{1}{n}y + b)$
14. Problema 19: $x^2 - y^2 = m(y^2 - z^2)$
15. Problema 20-21: $x^2 \pm y = u^2,\ y^2 \pm x = v^2$
16. Problema 22-23: $x^2 \pm (x + y) = u^2,\ y^2 \pm (x + y) = v^2$
17. Problema 24-25: $(x + y)^2 \pm x = u^2,\ (x + y)^2 \pm y = v^2$
18. Problema 26-27: $xy \pm x = u^2,\ xy \pm y = v^2,\ u + v = a,\ (u, v > 0)$
19. Problema 28-29: $x^2y^2 \pm x^2 = u^2,\ x^2y^2 \pm y^2 = v^2$
20. Problema 30-(31): $(x + y = w^2),\ xy + (x + y) = u^2,\ xy - (x + y) = v^2$
21. Problema 32-33: $x^2 \pm y = u^2,\ y^2 \pm z = v^2,\ z^2 \pm x = w^2$
22. Problema 34-35: $x^2 \pm (x+y+z) = u^2,\ y^2 \pm (x+y+z) = v^2,\ z^2 \pm (x+y+z) = w^2$

Libro GIII

1. Problema 1: $(x + y + z) - x^2 = u^2,\ (x + y + z) - y^2 = v^2,\ (x + y + z) - z^2 = w^2$
2. Problema 2-3: $(x+y+z)^2 \pm x = u^2,\ (x+y+z)^2 \pm y = v^2,\ (x+y+z)^2 \pm z = w^2$
3. Problema 4: $x - (x + y + z)^2 = u^2,\ y - (x + y + z)^2 = v^2,\ z - (x + y + z)^2 = w^2$
4. Problema 5: $x + y + z = t^2,\ y + z - x = u^2,\ z + x - y = v^2,\ x + y - z = w^2$
5. Problema 6: $x + y + z = t^2,\ y + z = u^2,\ z + x = v^2,\ x + y = w^2$
6. Problema 7: $x - y = y - z,\ y + z = u^2,\ z + x = v^2,\ x + y = w^2$
7. Problema 8-9: $x + y + z \pm a = t^2,\ y + z \pm a = u^2,\ z + x \pm a = v^2,\ x + y \pm a = w^2$
8. Problema 10-11: $yz \pm a = u^2,\ zx \pm a = v^2,\ xy \pm a = w^2$
9. Problema 12-13: $yz \pm x = u^2,\ zx \pm y = v^2,\ xy \pm z = w^2$
10. Problema 14: $yz + x^2 = u^2,\ zx + y^2 = v^2,\ xy + z^2 = w^2$

11. Problema 15-16: $yz \pm (y+z) = u^2,\ zx \pm (z+x) = v^2,\ xy \pm (x+y) = w^2$
12. Problema 17-18: $xy \pm (x+y) = u^2,\ xy \pm x = v^2,\ xy \pm y = w^2$
13. Problema 19: $(x+y+z+w)^2 \pm x = \square,\ (x+y+z+w)^2 \pm y = \square,\ (x+y+z+w)^2 \pm z = \square,\ (x+y+z+w)^2 \pm w = \square$
14. Problema 20-21: $x+y = a,\ z^2 \mp x = u^2,\ z^2 \mp y = v^2$

Libro GIV

1. Problema 1-2: $x^3 \pm y^3 = a,\ x \pm y = b$
2. Problema 3: $x^2 y = u,\ xy = u^3$
3. Problema 4: $x^2 + y = u^2,\ x + y = u$
4. Problema 5: $x^2 + y = u,\ x + y = u^2$
5. Problema 6: $x^3 + y^2 = u^3, z^2 + y^2 = v^2$
6. Problema 7: $x^3 + y^2 = u^2, z^2 + y^2 = v^3$
7. Problema 8: $x + y^3 = u^3,\ x + y = u$
8. Problema 9: $x + y^3 = u,\ x + y = u^3$
9. Problema 10-11: $x^3 \pm y^3 = x \pm y$
10. Problema 12: $x^3 + y = x + y^3$ (mismo problema que el 11)
11. Problema 13: $x + 1 = t^2,\ y + 1 = u^2,\ x + y + 1 = v^2,\ x - y + 1 = w^2$
12. Problema 14: $x^2 + y^2 + z^2 = (x^2 - y^2) + (y^2 - z^2) + (x^2 - z^2),\ (x > y > z)$
13. Problema 15: $(y+z)x = a,\ (z+x)y = b,\ (x+y)z = c$
14. Problema 16-17: $x + y + z = t^2,\ x^2 \pm y = u^2,\ y^2 \pm z = v^2,\ z^2 \pm x = w^2$
15. Problema 18: $x^3 + y = u^3,\ y^2 + x = v^2$
16. Problema 19: $yz + 1 = u^2,\ zx + 1 = v^2,\ xy + 1 = w^2$
17. Problema 20: $yz + 1 = r^2,\ zx + 1 = s^2,\ xy + 1 = t^2,\ xp + 1 = u^2,\ yp + 1 = v^2,\ zp + 1 = w^2$
18. Problema 21: $xz = y^2,\ x - y = u^2,\ x - z = v^2,\ y - z = w^2,\ (x > y > z)$
19. Problema 22-23: $xyz \pm x = u^2,\ xyz \pm y = v^2,\ xyz \pm z = w^2$
20. Problema 24: $x + y = a,\ xy = z^3 - z$
21. Problema 25: $x + y + z = a,\ xyz = \{(x-y) + (x-z) + (y-z)\}^3 (= 2(x-z))$

22. Problema 26-27: $xy \pm x = u^3,\ xy \pm y = v^3$
23. Problema 28: $xy + (x + y) = u^3,\ xy - (x + y) = v^3$
24. Problema 29-30: $x^2 + y^2 + z^2 + w^2 \pm (x + y + z + w) = a$
25. Problema 31: $x + y = 1,\ (x + a)(y + b) = u^2$
26. Problema 32: $x + y + z = a,\ xy + z = u^2,\ xy - z = v^2$
27. Problema 33: $x + \frac{1}{z}y = m(y - \frac{1}{z}y),\ y + \frac{1}{z}x = n(x - \frac{1}{z}x)$
28. Problema 34-35: $yz \pm (y+z) = a^2 - 1,\ zx \pm (z+x) = b^2 - 1,\ xy \pm (x+y) = c^2 - 1$
29. Problema 36: $yz = m(y + z),\ zx = n(z + x),\ xy = l(x + y)$
30. Problema 37: $yz = m(x + y + z),\ zx = n(x + y + z),\ xy = l(x + y + z)$
31. Problema 38: $(x + y + z)x = \frac{1}{2}u(u + 1),\ (x + y + z)y = v^2,\ (x + y + z)x = w^3$
32. Problema 39: $x - y = m(y - z),\ y + z = u^2,\ z + x = v^2,\ x + y = w^2$
33. Problema 40: $x^2 - y^2 = m(y - z),\ y + z = u^2,\ z + x = v^2,\ x + y = w^2$

Libro GV

1. Problema 1-2: $xz = y^2,\ x \mp a = u^2,\ y \mp a = v^2,\ z \mp a = w^2$
2. Problema 3-4: $x \pm a = r^2,\ y \pm a = s^2,\ z \pm a = t^2,\ yz \pm a = u^2,\ zx \pm a = v^2,\ xy \pm a = w^2$
3. Problema 5: $y^2z^2 + x^2 = r^2,\ z^2x^2 + y^2 = s^2,\ x^2y^2 + z^2 = t^2,\ y^2z^2 + y^2 + z^2 = u^2,\ z^2x^2 + z^2 + x^2 = v^2,\ x^2y^2 + x^2 + y^2 = w^2$
4. Problema 6: $x - 2 = r^2,\ y - 2 = s^2,\ z - 2 = t^2,\ yz - y - z = u^2,\ zx - z - x = v^2,\ xy - x - y = w^2,\ yz - x = o^2,\ zx - y = p^2,\ xy - z = q^2$
5. Problem 7: $x^2 \pm (x + y + z) = \square,\ y^2 \pm (x + y + z) = \square,\ z^2 \pm (x + y + z) = \square$
6. Problem 8: $yz \pm (x + y + z) = \square,\ zx \pm (x + y + z) = \square,\ xy \pm (x + y + z) = \square$
7. Problema 9(11): $x + y(+z) = 1,\ x + a = u^2,\ y + a = v^2,\ (z + a = w^2)$
8. Problema 10(12): $x + y(+z) = 1,\ x + a = u^2,\ y + b = v^2,\ (z + c = w^2)$
9. Problema 13: $x + y + z = a,\ y + z = u^2,\ z + x = v^2,\ x + y = w^2$
10. Problema 14: $x + y + z + w = a,\ x + y + z = s^2,\ y + z + w = t^2,\ z + w + x = u^2,\ w + x + y = v^2$
11. Problema 15-16: $(x+y+z)^3 \pm x = u^3,\ (x+y+z)^3 \pm y = v^3,\ (x+y+z) \pm z = w^3$
12. Problema 17: $x - (x + y + z)^3 = u^3,\ y - (x + y + z)^3 = v^3,\ z - (x + y + z)^3 = w^3$

13. Problema 18-19: $x+y+z=t^2,\ (x+y+z)^3 \pm x = u^2,\ (x+y+z)^3 \pm y = v^2,\ (x+y+z)^3 \pm z = w^2$
14. Problema 19_a: $x+y+z=t^2,\ x-(x+y+z)^3 = u^2,\ y-(x+y+z)^3 = v^2,\ z-(x+y+z)^3 = w^2$
15. Problema 19_b-19_c: $x+y+z=a,\ (x+y+z)^3 \pm x = u^2,\ (x+y+z)^3 \pm y = v^2,\ (x+y+z)^3 \pm z = w^2$
16. Problema 20: $x+y+z=\frac{1}{m},\ x-(x+y+z)^3 = u^2,\ y-(x+y+z)^3 = v^2,\ z-(x+y+z)^3 = w^2$
17. Problema 21-22: $x^2y^2z^2 \pm x^2 = u^2,\ x^2y^2z^2 \pm y^2 = v^2,\ x^2y^2z^2 \pm z^2 = w^2$
18. Problema 23: $x^2 - x^2y^2z^2 = u^2,\ y^2 - x^2y^2z^2 = v^2,\ z^2 - x^2y^2z^2 = w^2$
19. Problema 24-25: $y^2z^2 \pm 1 = u^2,\ z^2x^2 \pm 1 = v^2,\ x^2y^2 \pm 1 = w^2$
20. Problema 26: $1 - y^2z^2 = u^2,\ 1 - z^2x^2 = v^2,\ 1 - x^2y^2 = w^2$
21. Problema 27-28: $y^2+z^2 \pm a = u^2,\ z^2+x^2 \pm a = v^2,\ x^2+y^2 \pm a = w^2$
22. Problema 29: $x^4+y^4+z^4 = u^2$
23. Problema 30: $mx+ny = u^2,\ u^2+a = (x+y)^2$

Libro GVI

1. Problema 1-2: $z \mp x = u^3,\ z \mp y = v^3$
2. Problema 3-4: $\frac{1}{2}xy \pm a = u^2$
3. Problema 5: $a - \frac{1}{2}xy = u^2$
4. Problema 6-7: $\frac{1}{2}xy \pm x = a$
5. Problema 8-9: $\frac{1}{2}xy \pm (x+y) = a$
6. Problema 10-11: $\frac{1}{2}xy \pm (x+z) = a$
7. Problema 12-13: $\frac{1}{2}xy \pm x = u^2,\ \frac{1}{2}xy \pm y = v^2$
8. Problema 14-15: $\frac{1}{2}xy \mp z = u^2,\ \frac{1}{2}xy \mp x = v^2$
9. Problema 16: $u+v=x,\ \frac{u}{v} = \frac{y}{z}$
10. Problema 17: $\frac{1}{2}xy + z = u^2,\ x+y+z = v^3$
11. Problema 18: $\frac{1}{2}xy + z = u^3,\ x+y+z = v^2$
12. Problema 19: $\frac{1}{2}xy + x = u^2,\ x+y+z = v^3$
13. Problema 20: $\frac{1}{2}xy + x = u^3,\ x+y+z = v^2$

14. Problema 21: $x+y+z=u^2,\ \frac{1}{2}xy+(x+y+z)=v^3$
15. Problema 22: $x+y+z=u^3,\ \frac{1}{2}xy+(x+y+z)=v^2$
16. Problema 23: $z^2=u^2+u,\ \frac{z^2}{x}=v^3+v$
17. Problema 24: $z=u^3+u,\ x=v^3-v,\ y=w^3$

Libro AIV

1. Problema 1-2: $x^3\pm y^3=u^2$
2. Problema 3-4: $x^2\pm y^2=u^3$
3. Problema 5: $x^2y^2=u^3$
4. Problema 6: $x^3y^2=u^2$
5. Problema 7: $x^3y^2=u^3$
6. Problema 8-9: $x^3y^3=u^2$
7. Problema 10-11: $x^3\pm ax^2=u^2$
8. Problema 12-13: $x^3\pm ax^2=u^3$
9. Problema 14: $ax=u^2,\ bx=v^3$
10. Problema 15: $ax=u^2,\ bx=u^3$
11. Problema 16: $ax=u^3,\ ay=u$
12. Problema 17: $x=my,\ ax^2=u^3,\ ay^2=u$
13. Problema 18: $x=my,\ ax^3=u^2,\ ay^3=u$
14. Problema 19: $ax=u^3,\ bx=u$
15. Problema 20: $ax^3=u^2,\ bx^3=u$
16. Problema 21: $ax^2=u^3,\ bx^2=u$
17. Problema 22: $ax^3=u^3,\ bx^3=u$
18. Problema 23-24: $(x^2)^2\pm(y^2)^2=u^3$
19. Problema 25: $(x^3)^2+(y^2)^2=u^2$
20. Problema 26: $(x^3)^2-(y^2)^2=u^2,\ (y^2)^2-(x^3)^2=v^2$
21. Problema 27: $(x^3)^2+ay^2=u^2$
22. Problema 28: $(x^2)^2+ay^3=u^2$

23. Problema 29-30: $(x^3)^3 \pm (y^2)^2 = u^2$
24. Problema 31: $(y^2)^2 - (x^3)^3 = u^2$
25. Problema 32-33: $(x^3)^3 \pm ax^3y^2 = u^2$
26. Problema 34-35: $x^3 + y^2 = u^2,\ \pm(x^3 - y^2) = v^2$
27. Problema 36-37: $x^3 + ax^2 = u^2,\ x^3 \mp bx^2 = v^2$
28. Problema 38-39: $\pm(x^3 - ax^2) = u^2,\ \pm(x^3 - bx^2) = v^2$
29. Problema 40-41: $(x^2)^2 + y^3 = u^2,\ \pm((x^2)^2 - y^3) = v^2$
30. Problema 42-42$_b$: $(x^3)^3 + (y^2)^2 = u^2,\ \pm((x^3)^3 - (y^2)^2) = v^2$
31. Problema 43-44: $(x^3)^3 + a(y^2)^2 = u^2,\ (x^3)^3 \mp b(y^2)^2 = v^2$
32. Problema 44$_b$-44$_c$: $\pm((x^3)^3 - a(y^2)^2) = u^2,\ \pm((x^3)^3 - b(y^2)^2) = v^2$

Libro AV

1. Problema 1-2: $(y^2)^2 + ax^3 = u^2,\ (y^2)^2 \mp bx^3 = v^2$
2. Problema 3: $(y^2)^2 - ax^3 = u^2,\ (y^2)^2 - bx^3 = v^2$
3. Problema 4-5: $(y^2)^2 + a(x^3)^3 = u^2,\ (y^2)^2 \mp b(x^3)^3 = v^2$
4. Problema 6: $(y^2)^2 - a(x^3)^3 = u^2,\ (y^2)^2 - b(x^3)^3 = v^2$
5. Problema 7-8: $x \pm y = a,\ x^3 \pm y^3 = b$
6. Problema 9-10: $x \pm y = a,\ x^3 \pm y^3 = b(x \mp y)^2$
7. Problema 11-12: $x \mp y = a,\ x^3 \pm y^3 = b(x \pm y)$
8. Problema 13-14: $ax^2 \pm b = y + z,\ x^3 \pm y = u^3,\ x^3 \pm z = v^3$
9. Problema 15-16: $ax^2 - b = y + z,\ x^3 \pm y = u^3,\ \pm(x^3 - z) = v^3$

Libro AVI

1. Problema 1-2: $(x^3)^2 \pm (y^2)^2 = u^2,\ x = my$
2. Problema 3: $(y^2)^2 - (x^3)^2 = u^2,\ x = my$
3. Problema 4: $x^3y^2 \pm (x^3)^2 = u^2,\ x = my$
4. Problema 5-7: $x^3y^2 \pm (y^2)^2 = u^2,\ x = y$
5. Problema 6: $x^3y^2 - (x^3)^2 = u^2,\ x = y$

6. Problema 8-9: $x^3y^2 \pm \sqrt{x^3y^2} = u^2$
7. Problema 10: $\sqrt{x^3y^2} - x^3y^2 = u^2$
8. Problema 11: $(x^3)^2 + x^3 = u^2$
9. Problema 12-13: $x^2 \pm \frac{x^2}{y^2} = u^2,\ y^2 \pm \frac{x^2}{y^2} = v^2$
10. Problema 14: $\frac{x^2}{y^2} - x^2 = u^2,\ \frac{x^2}{y^2} - y^2 = v^2$
11. Problema 15-16: $x^2 \pm (x^2 - y^2) = u^2,\ y^2 \pm (x^2 - y^2) = v^2$
12. Problema 17: $x^2 + y^2 + z^2 = u^2,\ x^2 = y,\ y^2 = z$
13. Problema 18-19: $x^2y^2z^2 \pm (x^2 + y^2 + z^2) = u^2$
14. Problema 20: $(x^2 + y^2 + z^2) - x^2y^2z^2 = u^2$
15. Problema 21: $(x^2)^2 + (x^2 + y^2) = u^2,\ (y^2)^2 + (x^2 + y^2) = v^2$
16. Problema 22: $x^2 + y^2 = u^2,\ x^2y^2 = v^3$
17. Problema 23: $\frac{a^2}{x^2} + \frac{a^2}{y^2} = u^2,\ x^2 + y^2 + a^2 = v^2$

Libro AVII

1. Problema 1: $x^3y^3z^3 = u^2,\ x = ay,\ y = az$
2. Problema 2: $(x^2)^3(y^2)^3(z^2)^3 = (u^2)^2$
3. Problema 3: $(y^2)^2 = x^3 + z^3 + w^3$
4. Problema 4: $(y^2)^3 = x^2 + z^2 + w^2$
5. Problema 5: $(x^3)^3y^3 + (x^3)^3z^2 = u^2$
6. Problema 6: $x^2y^2 = a(x^2 + y^2),\ x^2 + y^2 = u^2$
7. Problema 7: $x + z + w = (y^3)^2,\ x + z = u^2,\ z + w = v^2,\ w + x = t^2$
8. Problema 8-9: $(x^3)^2 \pm y = u^2,\ (x^3)^2 \pm 2y = v^2$
9. Problema 10: $(x^3)^2 + y = u^2,\ (x^3)^2 - y = v^2$
10. Problema 11-12: $x + y = a^2,\ a^2 \pm x = u^2,\ a^2 - y = v^2$
11. Problema 13-14: $x + y + z = a^2,\ a^2 \pm x = u^2,\ a^2 \pm y = v^2,\ a^2 \pm z = w^2$
12. Problema 15: $x+y+z+w = a^2,\ a^2+x = s^2,\ a^2+y = t^2,\ a^2-z = u^2,\ a^2-w = v^2$
13. Problema 16: $x^2z^2 = y^4,\ y^2 - x^2 = u^2,\ z^2 - y^2 = v^2$
14. Problema 17: $x^2w^2 = y^2z^2,\ x^2 + y^2 + z^2 + w^2 = u^2$
15. Problema 18: $x^2w^2 = y^2z^2,\ y^2 - x^2 = u^2,\ z^2 - y^2 = v^2,\ w^2 - z^2 = t^2$

APÉNDICE B
Código MAGMA

En este capítulo del apéndice está el código utilizado para obtener los resultados del Capítulo 5.

Primero el código del archivo *init.m* el cual inicializa el proceso a ejecutar en MAGMA.

```
// Crear carpetas para cada libro y los archivos
   ↪ correspondientes a cada problema
for book in ["GI","GII","GIII","GIV","GV","GVI","AIV","AV","AVI
   ↪ ","AVII"] do
leer:=book cat ".txt";
X:=Split(Read(leer));
printf "n%o:=%o;\n",book,#X;
System("mkdir " cat book);

for k in [1..#X] do
s:=X[k];
ss:=Split(s,":");
case #ss:
  when 2:
    m:=#Split(ss[1],",");
    sch:=ss[2];
    file:="./" cat book cat "/" cat book cat IntegerToString(k);
    fprintf file, "// Book %o ::: Problem %o\n",book,k;
    fprintf file, "label:=\"%o%o\";\n",book,k;
    fprintf file,"A<%o>:=AffineSpace(Rationals(),%o);\n",ss[1],m
       ↪ ;
    fprintf file,"S:=Scheme(A,%o);\n",sch;
  when 3:
    n:=#Split(ss[1],",");
    m:=#Split(ss[2],",");
    sch:=ss[3];
    file:="./" cat book cat "/" cat book cat IntegerToString(k);
    fprintf file, "// Book %o ::: Problema %o\n",book,k;
    fprintf file, "label:=\"%o%o\";\n",book,k;
    fprintf file, "K<%o>:=RationalFunctionField(Rationals(),%o)
       ↪ ;\n",ss[1],n;
    fprintf file,"A<%o>:=AffineSpace(K,%o);\n",ss[2],m;
```

```
    fprintf file,"S:=Scheme(A,%o);\n",sch;
  end case;
end for;
end for;
```

A continuación el código del archivo *run.m*, el cual se encarga de terminar la preparación de la ejecución de los problemas y la ejecución real de los mismos, así como la salida de los problemas en ficheros ordenados.

```
// Numero de problemas de cada libro
nGI:=39;
nGII:=35;
nGIII:=21;
nGIV:=40;
nGV:=30;
nGVI:=24;
nAIV:=44;
nAV:=16;
nAVI:=23;
nAVII:=18;

// Resolver los problemas
procedure Cuenta(S,label)
    printf "============== %o ==============\n",label;
    print DefiningEquations(S);
        printf "Dimension = %o;\n",Dimension(S);
    if Dimension(S) eq 0 then Points(S); end if;
    if Dimension(S) eq 1 then [Genus(Curve(s)) : s in
       ↪ IrreducibleComponents(S)]; end if;
end procedure;


// Procedimiento que escribe en el archivo run para cargar todos
   ↪  los problemas
procedure Libro(book,nbook)
  file:="./" cat book cat "/run" cat book;
  fprintf file, "load \"../cuenta\";";
  for k in [1..nbook] do
    f:="load " cat book cat IntegerToString(k);
    fprintf file,"\n%o;",f;
    fprintf file, "%o;","Cuenta(S,label)";
  end for;
end procedure;

// Bucle que ejecuta el procedimiento Libro para todos los
   ↪ libros
Libro("GI", nGI);
Libro("GII", nGII);
Libro("GIII", nGIII);
Libro("GIV", nGIV);
Libro("GV", nGV);
Libro("GVI", nGVI);
Libro("AIV", nAIV);
```

```
Libro("AV", nAV);
Libro("AVI", nAVI);
Libro("AVII", nAVII);

// Ejecucion de los ficheros run redirigiendo el output
for book in ["GI","GII","GIII","GIV","GV","GVI","AIV","AV","AVI
   ↪ ","AVII"] do
  System("cd " cat book);
  System("magma < run" cat book cat " > out" cat book cat " &\n
     ↪ ");
  System("cd ..");
end for;
```

Por último el código del archivo *cuenta.m*, el cual no se ejecuta directamente pero es accedido por *run.m*.

```
// Numero de problemas de cada libro
nGI:=39;
nGII:=35;
nGIII:=21;
nGIV:=40;
nGV:=30;
nGVI:=24;
nAIV:=44;
nAV:=16;
nAVI:=23;
nAVII:=18;

// Resolver los problemas
procedure Cuenta(S,label)
    printf "============== %o ==============\n",label;
    print DefiningEquations(S);
        printf "Dimension = %o;\n",Dimension(S);
    if Dimension(S) eq 0 then Points(S); end if;
    if Dimension(S) eq 1 then [Genus(Curve(s)) : s in
       ↪ IrreducibleComponents(S)]; end if;
end procedure;
```

Bibliografía

[1] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993).

[2] Ezra Brown and Bruce T. Myers. Elliptic curves from Mordell to Diophantus and back. *Amer. Math. Monthly*, 109(7):639–649, 2002.

[3] Diofanto. *La aritmética y el libro sobre los números poligonales.* Epistéme 6-7. Nivola, Tres Cantos, 2007.

[4] Gerald Faltings. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. Math.*, 73(3):349–366, 1983.

[5] Gerald Faltings. Erratum: "Finiteness theorems for abelian varieties over number fields". *Invent. Math.*, 75(2):381, 1984.

[6] Robin Hartshorne. *Algebraic geometry.* Graduate Texts in Mathematics, No. 52. Springer-Verlag, New York-Heidelberg, 1977.

[7] Thomas L. Heath. *Diophantus of Alexandria: A study in the history of Greek algebra.* Dover Publications, Inc., New York, second edition, 1964. With a supplement containing an account of Fermat's theorems and problems connected with Diophantine analysis and some solutions of Diophantine problems by Euler.

[8] Rick Miranda. *Algebraic curves and Riemann surfaces*, volume 5 of *Graduate Studies in Mathematics.* American Mathematical Society, Providence, RI, 1995.

[9] Louis J. Mordell. On the rational solutions of the indeterminate equations of the third and fourth degrees. *Proc. Camb. Philos. Soc.*, 21:179–192, 1922.

[10] René Pannekoek. Diophantus revisited: On rational surfaces and k3 surfaces in the arithmetica. *arXiv: Number Theory*, 2015.

[11] Norbert Schappacher. "Wer war Diophant?". *Math. Semesterber.*, 45(2):141–156, 1998. English translation.

[12] Jacques Sesiano. *Books IV to VII of Diophantus' Arithmetica in the Arabic translation attributed to Qusṭā ibn Lūqā*, volume 3 of *Sources in the History of Mathematics and Physical Sciences.* Springer-Verlag, New York, 1982.

[13] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer, Dordrecht, second edition, 2009.

[14] Joseph H. Silverman and John T. Tate. *Rational points on elliptic curves.* Undergraduate Texts in Mathematics. Springer, Cham, second edition, 2015.

[15] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[16] Joseph Loebach Wetherell. *Bounding the number of rational points on certain curves of high rank*. ProQuest LLC, Ann Arbor, MI, 1997. Thesis (Ph.D.)–University of California, Berkeley.

[17] Andrew Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.