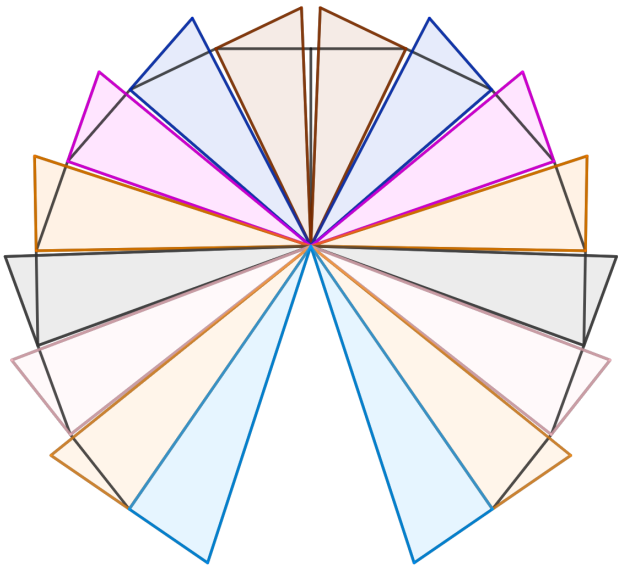
JORGE MORRA

Tema 15. Ecuaciones diofánticas.

OPOSICIONES
MATEMÁTICAS

JORGE MORRA

Tema 15. Ecuaciones diofánticas.



OPOSICIONES
MATEMÁTICAS

Prólogo

Tiene delante el lector el decimoquinto cuadernillo de la serie "Oposiciones Matemáticas", concretamente el de ecuaciones diofánticas.

Como ya expuse en prólogos anteriores, para poder enfrentarse con cierta solvencia al examen de oposición de Matemáticas, la construcción de cada tema debe contener y diferenciar tres partes: una presentación, un nudo y un desenlace. Parecen las mismas tres partes que encontramos en una película o un libro, sí, lo son, pero es que cuando contamos algo necesitamos que *"ese algo"* tenga entidad por sí solo. Pensemos que un tribunal no es más que nuestro público, y si queremos aprobar tenemos que *"entretenerlos"*. ¿Qué mejor forma de gustarles que contarles un cuento?

De las tres partes, la primera la utilizaremos para presentar el tema, justificar todo el contenido que vamos a exponer y encuadrarlo dentro de la Historia y dentro de nuestra propuesta.

En la segunda debemos ordenar todos los contenidos de acuerdo a los resultados que vayamos a mostrar, aunque no probemos todo porque no va a ser posible con todas las proposiciones, teoremas, lemas o corolarios que enunciemos. Pero, insisto, es necesario que al menos se expongan en el orden correcto. Sobre esto los matemáticos somos bastante exigentes, los lemas preceden a los teoremas, y los corolarios los suceden, por poner un ejemplo.

Acabaremos poniendo la "guinda" al pastel en la tercera y última parte. Bueno..., así dicho parece más una receta de cocina que el desarrollo de un tema de Matemáticas. Básicamente debemos acabar con un resultado importante, demostrado o no, eso importa menos, pero sí relevante.

Para que las tres partes puedan funcionar y constituirse como un todo, es imprescindible que sepamos a priori lo que tenemos tiempo de escribir, presentar o exponer; y para ello es también preciso que nos preparemos el tema *"a conciencia"*.

Las oposiciones de Matemáticas no son fáciles, como tampoco lo son las Matemáticas. *"A conciencia"* significa que hay que conocer todo o casi todo de lo que estamos tratando, porque controlando el tema evitamos que él nos controle a nosotros. Cuando sabemos de lo que hablamos, podemos improvisar en cualquier momento; no importa que no recordemos un paso en un teorema porque sabemos dónde queremos llegar, saltamos el teorema o el paso correspondiente dándolo por demostrado y añadimos algún otro apartado para completar el desarrollo. Todo depende de lo que lo dominemos.

Pero preparar o prepararse un tema de oposición no es nada sencillo. Debemos *saber* Matemáticas, y además las *mínimas* del tema que escribamos. Pero si no es así porque nos ha tocado uno de los peor preparados, tenemos que dar a entender al Tribunal que *sí las sabemos*, y que las cosas que no contamos no es porque las desconozcamos sino porque nos falta tiempo.

No quiero extenderme más, espero que la lectura y el trabajo con este decimoquinto

cuadernillo sea productivo para todos aquellos que quieran o bien conocer algo más de esta ciencia o bien convertirse en profesores de Secundaria..., o ambas cosas.

Por último agradecer al lector el trabajo que está a punto de comenzar y mencionarle que todos aquellos comentarios que considere oportunos, bien de profundización de algunos puntos, bien de inconsistencias, errores o erratas en algunas demostraciones, o bien sugiriendo nuevos apartados o secciones, puede hacérmelos llegar a través de mi correo electrónico: jorgemorra@outlook.es. Si bien es cierto que aunque no pueda asegurar contestarlos, sí puedo asegurar leerlos.

Jorge Morra

Madrid, agosto de 2020

Índice

Página

1. ¿Cómo preparar este tema?

Como en todos los temas hasta ahora es importante leer y entender todo el contenido al completo, desde la primera hasta la última línea. Siempre insisto en lo mismo porque en ocasiones tendemos a saltarnos partes de un texto ya que lo consideramos poco importante, o porque creemos que lo conocemos; en este caso le pido al lector que no lo haga.

Cuando lo haya leído y entendido, ya tendrá una idea de lo que le quiero contar, ahora viene la parte más difícil, que es la de sintetizar, resumir y concretar lo que quiere escribir.

En ese momento puede optar por una de dos alternativas, o lo hace por sí mismo, que es posiblemente la mejor propuesta puesto que de esta forma aprenderá todo del tema; o bien se deja aconsejar por mí y estudia lo que yo le propongo, siempre por supuesto con posibilidades de cambiar lo que estime oportuno.

Es necesario también que tenga claro que lo que le voy a proponer es lo que le debe dar tiempo a desarrollar. Si puede escribir más tendrá que añadir más, y si escribe menos, tendrá que eliminar parte del tema; todo a su criterio.

Las ecuaciones diofánticas entrañan cierta dificultad en el procedimiento de resolución, y éstos distan mucho de ser universales.

El tema al completo contiene muchos resultados y conceptos. El lector encontrará probados los teoremas y proposiciones más importantes, habiéndonos quedado algunos sin demostrar. Es aconsejable que los restantes se intenten, las demostraciones que se dejan para el lector deben pensarse como ejercicios del tema que nos ayudarán a comprenderlo en su totalidad.

- La sección *introducción* es importante y debe incluirse al completo. Es un desarrollo sintetizado de las ecuaciones diofánticas a lo largo de la historia.
- La sección *ecuaciones diofánticas lineales* contiene las distintas ecuaciones de primer grado que podemos encontrarnos en la práctica. Los teoremas que caracterizan las de dos incógnitas deben enunciarse y demostrarse. Los de varias incógnitas solamente enunciarse. En ambos casos es importante que el lector intente los ejemplos por su cuenta. Debe incluirse también uno de ellos. El *teorema chino del resto* debe enunciarse solamente, y si es posible añadir el ejemplo.
- De la sección *ecuación diofántica de 2º grado* es importante toda la parte de la introducción de dichas ecuaciones. Sobre la ecuación de Pell debe definirse el concepto de fracción continua y el teorema 4.1. El ejemplo 4.2 debe entenderse, y si es posible hacer algunos parecidos; aunque no es necesario que se añada en el desarrollo del tema. La ecuación $x^2 - y^2 = n$ debe desarrollarse y dar sus soluciones. De la parte de la descomposición de un número de sumas de dos cuadrados, debe enunciarse el teorema 4.4, también las observaciones que se incluyen y al menos uno de los ejemplos. La última parte de esta sección, la *ecuación pitagórica*, debe añadirse al completo.
- De la sección *ecuaciones diofánticas de grado mayor que 2* es importante mencionar toda la parte histórica relativa al *Último Teorema de Fermat*, a la *Conjetura de*

Taniyama-Shimura-Weil y a la demostración de Wiles. Debe enunciarse y demostrarse el teorema que afirma que $x^4 + y^4 = z^2$ no tiene solución en los enteros porque es la base de la demostración de la Conjetura de Fermat para $n = 4$ y sus múltiplos.

- La sección *conclusiones* recopila lo tratado y desarrollado en el tema.

2. Introducción

Una ecuación diofántica puede ser considerada como una ecuación algebraica cuya solución se busca dentro del anillo de los números enteros o en su defecto dentro del cuerpo de los racionales. En esencia se suele también extender la definición a un conjunto de ecuaciones, o mejor dicho a un sistema de ecuaciones algebraicas, donde como podría esperarse el número de incógnitas supera al de ecuaciones, y también se suele extender el conjunto de soluciones pertenecientes a extensiones algebraicas de los racionales, números $p-$ádicos, etc.

Ya desde la antigüedad nos encontramos con el problema de resolver ecuaciones algebraicas dentro de los números enteros. De hecho en la antigua Babilonia, en la Tabilla[1] Plimpton 322 podemos encontrarnos las primeras ternas pitagóricas de la historia. Pero el mayor resurgimiento lo encontramos en la Grecia Antigua. Diofanto, matemático griego del siglo III, escribe en su obra *Arithmetica* la resolución de ecuaciones de segundo y tercer grado principalmente. Supone un cambio en cuanto a los métodos tradicionales griegos, de mayor tratamiento de los problemas y soluciones geométricas en detrimento de otros métodos menos visuales. En su *Arithmetica*, Diofanto da una resolución exacta de ecuaciones determinadas e indeterminadas, algo en lo que se desmarca de las soluciones babilónicas, mucho más aproximadas. Dentro de ellas, las indeterminadas son las que tienen una mayor importancia. No obstante, no encontramos en esta obra una sistematización de los procedimientos de resolución de ecuaciones algebraicas, sino que contiene una colección de problemas, resueltos en términos numéricos determinados y precisos. Se desconoce si Diofanto pretendía con ello introducir procedimientos y métodos más generales.

Por poner un ejemplo, en uno de los problemas Diofanto calcula dos números tales que al sumar cualquiera de ellos con el cuadrado del otro se obtiene un cuadrado perfecto. En nuestra notación, se trata de buscar m, n tales que

$$\begin{cases} n^2 + m = p^2 \\ m^2 + n = q^2 \end{cases}$$

siendo p, q dos enteros positivos. Es claro que este problema solamente tiene soluciones dentro del conjunto de los racionales. En otro introduce la ecuación del tipo $x^2 = 1 + dy^2$ con d entero (denominada erróneamente *ecuación de Pell*), aunque en todos los casos se limita a dar una solución, no en desarrollar todas las que puedan cumplir la ecuación. A este respecto Diofanto se limitó en su obra a resolver problemas, no ecuaciones.

El primero en dar una solución general a la ecuación diofántica lineal, $ax + by = c$, con a y b primos entre sí, fue el matemático hindú Brahmagupta, quien también estudió la ya

[1] Pequeña tabla de arcilla que fueron descubiertas a mediados del XIX y que contenían conocimientos matemáticos de la época. Se considera que puede haber cerca de las 400.

mencionada ecuación cuadrática $x^2 - dy^2 = 1$. Sobre ella, el también matemático hindú Bhaskara (1114-1185) la resolvió en algunos casos particulares; no obstante no fue hasta el siglo XVIII, cuando Lagrange dio la solución completa para todos los casos.

Cuando los matemáticos hablamos de ecuaciones diofánticas, de forma implícita reconocemos cierta dificultad en el proceso de resolverlas. Ya las más elementales no siempre tienen solución y aquellas que la tienen no suele ser trivial. Concretamente en uno de los 23 problemas que enunció Hilbert en la conferencia de 1900, el décimo para ser exactos, planteaba la posibilidad de idear un procedimiento que dilucidara si una ecuación algebraica con coeficientes enteros, es decir, una ecuación diofántica, tenía solución en $\mathbb{Z}$ o en $\mathbb{Q}$.

Tuvieron que transcurrir setenta años para que un matemático ruso, Yuri Matiyasévich, demostrara que no existe ningún algoritmo que sea capaz de determinar si una ecuación diofántica la tiene. De hecho se puede escribir explícitamente una ecuación $P(x, y_1, y_2, \ldots, y_n) = 0$ con coeficientes enteros en los que no se puede determinar si tiene soluciones.

Al margen de lo descubierto en el siglo XX y de lo desarrollado por babilonios, griegos, árabes e hindúes, la teoría general de la solución de las ecuaciones lineales con dos incógnitas fue desarrollada en el siglo XVII por el matemático francés Claude Gaspard Bachet (1612-1635). Posteriormente, matemáticos como Pierre de Fermat (1601-1665), William Brouncker (1620-1684), John Wallis (1616-1713) y otros del XVIII y comienzos del XIX como Euler (1707-1783), Lagrange (1736-1813) y Gauss (1777-1885) investigaron la ecuación diofántica del tipo:

$$ax^2 + bxy + cy^2 + dx + ey + f = 0$$

donde $a, b, c, d, e, f \in \mathbb{Z}$.

En los estudios de las ecuaciones diofánticas de grado superior a 2 con dos incógnitas, A. Thue (1863-1922), demostró que si $n \geqslant 3$ y $a_0, a_1, \ldots, a_n, b \in \mathbb{Z}$, la ecuación

$$a_0x^n + a_1x^{n-1}y + a_2x^{n-2}y^2 + \ldots + a_ny^n = b$$

no tiene solución o su número es finito, siempre que el polinomio $P(t) = a_0t^n + a_1t^{n-1} + \ldots + a_{n-1}t + a_n$ sea irreducible en $\mathbb{Q}$.

Cuando aumentamos el número de incógnitas no podemos por menos que mencionar uno de los problemas más importantes que ha conocido la historia de los Matemáticas: el *Teorema o Conjetura de Fermat*. Al parecer este ilustre matemático del siglo XVIII dejó una nota en el margen de uno de los libros de la edición de Bachet de la *Arithmetica* de Diofanto anunciando una *demostración* de que la ecuación

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

no tenía soluciones para $n \geqslant 3$ dentro de los números enteros. La prueba no se encontró y el problema estuvo abierto durante más de tres siglos. No fue hasta finales del XX cuando un matemático británico, Andrew Wiles demostró la tesis de Fermat. En realidad probó que toda curva elíptica podía parametrizarse por medio de funciones modulares, o dicho con otras palabras, demostró que toda curva elíptica era modular. Tristemente después

de tanto tiempo, la demostración del *Ultimo teorema de Fermat* no tuvo el romanticismo de ser la idea brillante de un matemático, sino más bien la conjunción de una serie de resultados concebidos y demostrados a lo largo de la segunda mitad del siglo XX.

Antes de comenzar con el estudio de los tipos de ecuaciones diofánticas diremos que en todo el tema trabajaremos con ecuaciones algebraicas con coeficientes en los números enteros, y cuyas soluciones las buscaremos también dentro de los enteros. Además, el lector podrá comprobar que todos los métodos conocidos para determinar la existencia de solución solo pueden aplicarse a un tipo concreto de ecuación, no existe generalización.

3. Ecuaciones diofánticas lineales

Comencemos con las básicas. Para este tipo de ecuación podemos suponer que el número de incógnitas es superior a uno.

3.1. La ecuación $ax + by = c$

Nos encontramos con una de las ecuaciones más conocidas. Podemos dar una caracterización tanto de la existencia como de sus soluciones.

Proposición 3.1 *La condición necesaria y suficiente para que la ecuación $ax + by = c$, con $a, b, c \in \mathbb{Z}$ tenga solución en $\mathbb{Z}$ es que $mcd(a, b)|c$ (el máximo común divisor de a y b divida a c).*

Demostración: En efecto, consideraremos en primer lugar que (x_0, y_0) es una solución. Se cumple

$$ax_0 + by_0 = c$$

Sea $d = \text{mcd}(a, b)$, entonces existen a' y b' tales que $da' = a$ y $db' = b$. Sustituyendo:

$$da'x_0 + db'y_0 = d(a'x_0 + b'y_0) = c$$

lo que implica que $d|c$.

Para la condición suficiente, supongamos ahora que, siendo $d = \text{mcd}(a, b)$ se cumple $d|c$. Entonces existe c' tal que $dc' = c$. Por el teorema de Bézout[2] existen r, s enteros tales que

$$ar + bs = d$$

Si ahora multiplicamos por c', obtenemos

$$c'ar + c'bs = c'd = c$$

luego

$$a(c'r) + b(c's) = c$$

Tomando $x = c'r$ e $y = c's$ habremos obtenido una solución de $ax + by = c$.

⊗

[2] Matemático francés del siglo XVIII que demostró que si $d = \text{mcd}(a, b)$ entonces existen r y s enteros tales que $ar + bs = d$.

Corolario 3.2 *Si la ecuación $ax + by = c$, con $a, b, c \in \mathbb{Z}$ tiene una solución entonces tiene infinitas.*

$\otimes$

En efecto, consideremos que tiene una solución. Por el teorema anterior, $d = \text{mcd}(a, b)$ divide a c, por tanto, siendo $da' = a$ y $db' = b$, con $\text{mcd}(a'b') = 1$, tendríamos que existe c' con $dc' = c$. Sustituyendo en la ecuación:

$$da'x + db'y = dc'$$

simplificando obtenemos otra ecuación con las mismas soluciones que la original

$$a'x + b'y = c'$$

Por tanto, a partir de la proposición anterior, si $x = c'r$ e $y = c's$ son soluciones, resulta

$$ac'r + bc's = c$$

Igualamos:

$$ax + by = ac'r + bc's$$

Pasamos al primer miembro y operamos:

$$a(x - c'r) + b(y - c's) = 0$$

Dividimos entre d

$$a'(x - c'r) + b'(y - c's) = 0$$

Utilizamos el teorema de Euclides[3], ya que $\text{mcd}(a', b') = 1$ y $a'|b'(y - c's)$ resulta $a'|(y - c's)$, y como también $b'|a'(x - c'r)$ tenemos $b'|(x - c'r)$.

Existen entonces $p, q \in \mathbb{Z}$ tales que:

$$\begin{cases} b'q = x - c'r \\ a'p = y - c's \end{cases}$$

Con lo que

$$\begin{cases} x = b'q + c'r \\ y = a'p + c's \end{cases}$$

Sustituyendo en $a'x + b'y = c'$, y teniendo en cuenta que $a'r + b's = 1$, tenemos

$$\begin{aligned} c' = a'x + b'y =& a'(b'q + c'r) + b'(a'p + c's) = a'b'q + a'c'r + a'b'p + b'c's = \\ =& c'(a'r + b's) + a'b'(p + q) = c' + a'b'(p + q) \end{aligned}$$

Por consiguiente, para que x e y sean soluciones es necesario y suficiente que $p + q = 0$, con lo que $p = -q$. Pero además, $a'd = a$ y $b'd = b$, y ya que podemos tomar cualquier q entero, resulta que podemos reescribir el conjunto de soluciones en la forma

$$\begin{cases} x = bq + c'r \\ y = -aq + c's \end{cases}$$

[3]El teorema de Euclides dice que si a, b, c son números enteros, tales que $a|bc$ y $\text{mcd}(a, b) = 1$, entonces $a|c$.