ECUACIONES DIOFÁNTICAS

Alveiro Chanchin Gómez
Omar Felipe Quintana Ramírez

UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE EDUCACIÓN
LICENCIATURA EN MATEMÁTICAS
NEIVA - HUILA
2011

ECUACIONES DIOFÁNTICAS

Alveiro Chanchin Gómez
Código:2004200727
Omar Felipe Quintana Ramírez
Código:2005101408

Trabajo presentado como requisito para grado

Asesorado por:
Mg. Ricardo Cedeño Tovar

UNIVERSIDAD SURCOLOMBIANA
FACULTAD DE EDUCACIÓN
LICENCIATURA EN MATEMÁTICAS
NEIVA - HUILA
2011

Nota de aceptación

_____

_____

_____

_____

_____

Firma Asesor del Trabajo de Grado

_____

Firma Segundo Lector

_____

Firma Jefe de Programa

Neiva, Huila. Enero de 2011

"La matemática es la ciencia del orden y la medida, de bellas cadenas de razonamientos, todos sencillos y fáciles."

René Descartes (1596-1650)

Índice general

Capítulo 1
AGRADECIMIENTOS

El presente trabajo de grado es un esfuerzo en el cual, directa o indirectamente, participaron varias personas leyendo, opinando, corrigiendo, dando ánimo, acompañando en los momentos de crisis y en los momentos de felicidad.

Agradecemos al Mg. Ricardo Cedeño Tovar por haber confiado en nosotros, por la paciencia y por la dirección de este trabajo, por sus comentarios en todo el proceso de elaboración de la Tesis y sus atinadas correcciones. Al Mg. Augusto Silva Silva por las aclaraciones oportunas y la atenta lectura de este trabajo.

Gracias también a nuestros queridos compañeros, que nos apoyaron y nos permitieron entrar en su vida durante estos casi cinco años de convivir dentro y fuera del salón de clase. Jarol Cuenca, Sergio Trujillo, Oscar Martínez, Ronal Sánchez y Diana Paola Puentes.

A nuestros padres y hermanos que nos acompañaron en esta aventura que significó el desarrollo de la Licenciatura en Matemáticas y que, de forma incondicional, entendieron nuestras ausencias y malos momentos.

Capítulo 2
INTRODUCCIÓN

Una ecuación lineal con dos incógnitas no es suficiente para determinar el valor de éstas, si deseamos encontrar una solución única. Pues dos cantidades x e y no están unívocamente determinadas más que en el caso de haber entre ellas dos ecuaciones independientes. Pero si alguna de las incógnitas x e y, se les exige que sean números enteros positivos, esta condición puede reemplazar la segunda ecuación. En este caso la ecuación se llama diofántica, en recuerdo del matemático Diofanto, quien vivió en Alejandría hacia el año 275 de nuestra era y creó el análisis indeterminado o análisis diofántico, que es un método para buscar soluciones enteras de ecuaciones y de sistemas de ecuaciones algebráicas con coeficientes enteros.

En este trabajo de grado lo que pretendemos es mostrar algunas Ecuaciones Diofánticas que son interesantes, que motivan y despiertan interés en este campo de la teoría de números.

Comenzaremos con la definición de ecuación diofántica, luego haremos un poco de historia de la forma en que se introduce este concepto en el análisis matemático. A la vez presentaremos varios ejercicios que muestran la resolución de problemas con una y varias variables, es decir, dada una ecuación diofántica con cualquier número de incógnitas y con coeficientes numericos enteros a través de un proceso determinamos si la ecuación es o no es resoluble en los números enteros.

En términos más modernos, Hilbert les solicitaba a sus colegas, un algoritmo capaz de admitir como entrada una Ecuación Diofántica cualquiera; este consistía en dar como resultado "Si"; si la ecuación procesada tenia soluciones en los enteros o dar como resultado un "No"si la ecuación procesada no tenia soluciones en los enteros. Por ejemplo, la ecuación $x^2 + y^2 = z^2$ obtendría un Si, puesto que tiene soluciones enteras, empezando con $x = 3$, $y = 4$ y $z = 5$ y siguiendo con otros infinitos tripletes.

En cambio, cualquier ecuación $x^n + y^n = z^n$ con $n > 2$ obtendría un No, puesto que no tiene soluciones enteras.

Observando lo interesante e importante de este tema, pretendemos dar a conocer una propuesta clara y sencilla para desarrollar y entender las ecuaciones Diofánticas.

Capítulo 3
JUSTIFICACIÓN

Este trabajo se realiza para conocer las Ecuaciones Diofánticas y algunos procedimientos existentes para su resolución.

Estas nos permite trabajar en una variedad de ecuaciones con distintos números de incognitas; además, nos permite aplicar distintos métodos para la resolución de problemas. "La resolución de problemas, obedece a una comprensión tanto de la educación matemática como de la naturaleza de las matemáticas". [1]

Alumnos que se apropian de su entorno, que lo interpretan e interactúan con él desde una perspectiva de la lógica matemática, desarrollan habilidades que les permitir solucionar problemas de manera eficiente.

La estrategia basada en la resolución de problemas, se ha convertido desde hace algunas décadas en una importante contribución a la educación matemática en el mundo. Tal vez la obra de Pólya, que aunque escrita en los años 40 del siglo XX, fue la pionera en este tipo de propuestas y logra trascendencia en la medida que fundamenta las bases de una pedagogía matemática. Él planteó una sucesión de pasos en la resolución de problemas; entender el problema, configurar un plan, ejecutar un plan y mirar hacia atrás. "Para un matemático, que es activo en la investigación,

[1](13 de diciembre de 1887 - 7de septiembre de 1985, Pólya Gyrgy en húngaro) fue un matemático que nació en Budapest, Hungría y murió en Palo Alto, EUA. Trabajó en una gran variedad de temas matemáticos, incluidas las series, la teoría de números, geometría, álgebra, análisis matemático la combinatoria y la probabilidad. En sus últimos años, invirtió un esfuerzo considerable en intentar caracterizar los métodos generales que usa la gente para resolver problemas, y para describir cómo debería enseñarse y aprender la manera de resolver problemas. Escribió tres libros sobre el tema: Cómo plantear y resolver problemas (How to solve it), Matemáticas y razonamiento plausible, Volumen I: Inducción y analogía en matemáticas y Matemáticas y razonamiento plausible, Volumen II: Patrones de inferencia plausible

la matemática puede aparecer algunas veces como un juego de imaginación: hay que imaginar el teorema matemático antes de probarlo; hay que imaginar la idea de la prueba antes de ponerla en práctica. Los aspectos matemáticos son primero imaginados y luego probados. Si el aprendizaje de la matemática tiene algo que ver con el descubrimiento en matemática, a los estudiantes se les debe brindar alguna oportunidad de resolver problemas en los que primero imaginen y luego prueben alguna cuestión matemática adecuada a su nivel".

Capítulo 4
OBJETIVOS

4.1. Generales

✓ Exponer de una manera práctica la solución de algunas Ecuaciones Diofánticas.

✓ Mostrar los distintos procedimientos para resolver las Ecuaciones Diofánticas.

4.2. Específicos

✓ Recordar los origenes de las Ecuaciones Diofánticas.

✓ Mostrar la solución de algunas Ecuaciones Diofánticas.

✓ Aplicar distintos métodos algebraicos y teoremas para la resolución de problemas.

✓ Desarrollar varios ejercicios aplicando las Ecuaciones Diofánticas.

Capítulo 5
ECUACIONES DIOFÁNTICAS

5.1. Historia de las Ecuaciones Diofánticas

El período que va del año 250 al 350 d.C, suele considerarse como la Edad de Plata de la matemática griega. La vida de Diofanto de Alejandría, el algebrista griego más importante, se desarrolla a comienzos de este período. Se conoce muy poco sobre su vida. En una colección de problemas, la Antología, que data de los siglos V o VI ha quedado registrada su edad en la forma siguiente:

Su infancia duró $\frac{1}{6}$ *de su vida y su adolescencia hasta* $\frac{1}{2}$ *más. Se casó tras* $\frac{1}{7}$ *más y su hijo nació* 5 *años después. El hijo vivió la mitad de la edad de su padre, muriendo éste* 4 *años después que el hijo. El problema consistía en determinar la edad de Diofanto. La solución resulta ser* 84 *años.*

Su trabajo se destaca por encima del de sus contemporáneos, desgraciadamente nació demasiado tarde para que pudiera tener una gran influúencia en su tiempo, pues una corriente de destrucción estaba acabando con la civilización. Escribió varios libros que se han perdido. Su gran obra es la Aritmética. Se conserva la mitad de esta obra en manuscritos del siglo $XIII$ que son copia de versiones más antiguas. La Aritmética es una colección de problemas independientes y según Diofanto, fue escrita para ayudar a uno de sus estudiantes. Una de sus contribuciones más importantes es la introducción del simbolismo en el álgebra. Los griegos clásicos no consideraron productos con más de tres factores ya que no tenían ningún significado geométrico para ellos, ya que x^2 era el área de un cuadrado y x^3 el volumen de un cubo. Diofanto consideró potencias como x^4; x^5, etc. Desde el punto de vista de una aritmética no condicionada por la geometría, tales productos tienen un significado. Diofanto utiliza la letra griega "ζ"para nuestra x (esta letra no representaba ningún número en el sistema griego de servirse de letras para designar números). Por el uso de símbolos

para la igualdad y para las operaciones suma y producto, el álgebra de Diofanto se llama sincopada. El álgebra anterior a Diofanto indica las operaciones y la igualdad en el lenguaje escrito usual; este álgebra se llama retórica.

Una rama actual del álgebra se llama análisis diofántico. Para entender de qué se ocupa esta rama, pensemos en la ecuación con dos incógnitas $x + 2y - 5 = 0$. Se desea encontrar todas las soluciones enteras de esta ecuación. Diofanto se ocupaba de problemas de este tipo, incluso con ecuaciones de mayor grado y un número mayor de incógnitas. Demuestra una gran habilidad para reducir las ecuaciones de los diferentes tipos a formas que puede manejar más fácilmente. Este tipo de ecuaciones indeterminadas (ecuaciones en las que existen más de una solución) no fueron consideradas por los griegos anteriores a Diofanto.

Hay indicios de influencia babilónica, pero no hay prueba alguna de que haya una conexión directa entre los trabajos de Diofanto y el álgebra babilónica. Pero sus números son completamente abstractos y no se refieren a medidas de granos o unidades monetarias como era el caso de egipcios y babilonios. Otra diferencia es que Diofanto estaba interesado únicamente en soluciones racionales exactas, mientras que los babilonios estaban siempre dispuestos a aceptar como soluciones aproximaciones de números irracionales.

La Aritmética de Diofanto es sorprendentemente original, pero es posible que ello se deba a que puedan haberse perdido otras colecciones de problemas rivales. No obstante, lo cierto es que Diofanto ha tenido una influencia sobre la teoría de números moderna mucho mayor que cualquier otro algebrista griego. Por ejemplo, Fermat se vió conducido a su célebre gran Teorema cuando intentaba generalizar un problema de la Aritmética de Diofanto.

No tenía ningún método general, cada uno de los 189 problemas de la Aritmética se resuelve de un modo distinto. No hace ningún intento por clasificarlos. Parece que no buscaba ideas generales, sino que se contentaba con encontrar soluciones correctas. No encuentra todas las soluciones de las ecuaciones indeterminadas, sólo se limita a dar una solución. Pero esto es comprensible si tenemos en cuenta que lo que quería era resolver un problema y no resolver una ecuación.

5.2. Generalidades

Estas ecuaciones reciben este nombre en honor a Diofanto, matemático que trabajó en Alejandría a mediados del siglo III d.c. Fue uno de los primeros en introducir la notación simbólica en matemáticas y escribió seis libros sobre problemas en las que consideraba la representación de números como suma de cuadrados.

5.3. Definición de Ecuación Diofántica

Se llama ecuación diofántica (en recuerdo a Diofanto de Alejandría) a cualquier ecuación algebraica con coeficientes enteros, generalmente de varias variables, planteada sobre el conjunto de los números enteros $\mathbb{Z}$ o los números naturales $\mathbb{N}$, es decir, se trata de ecuaciones cuyas soluciones sean números enteros.

5.4. Solución de una Ecuación Diofántica

Comenzaremos dando algunas definiciones y conceptos que vamos a necesitar en el transcurso de este trabajo.

1. Si a es un número entero lo notaremos por $a \in \mathbb{Z}$
2. Diremos que el número entero a divide al número entero b, si existe otro número entero c tal que $b = ca$, notamos este hecho como $a \mid b$, si a no divide a b lo notaremos por $a \nmid b$.
3. El máximo común divisor de a y b notado $d = m.c.d.(a, b)$ es tal que,
   a. $d \mid a$, y, $d \mid b$
   b. Si $c \mid a$, y, $c \mid b$ entonces $c \mid d$.

Tenemos algunos resultados que a pesar de ser elementales van a resultar de suma importancia más adelante.

1. Si $a|b$ entonces $a|bx$, cualquiera que sea $x \in \mathbb{Z}$.

   Efectivamente, si $a \mid b$ entonces existe $c \in \mathbb{Z}$ tal que $b = ca$, luego $bx = (ca)x = a(cx)$, de aqui $a \mid bx$.

2. Si $a \mid b$, y, $a \mid c$ entonces $a \mid (bx + cy)$, es decir que si a divide a b y a divide a c entonces a divide a cualquier combinación lineal de b y c.

   Efectivamente, si $a \mid b$, y, $a \mid c$ entonces existen d y e en los enteros tales que $b = ad$, y, $c = ae$, luego $bx + cy = (ad)x + (ae)y = a(dx + ey)$, así que $a \mid (bx + cy)$.

3. Si $m.c.d.(a, b) = d$, entonces $m.c.d.\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

   En efecto:

$$\begin{aligned} d &= m.c.d(a, b) \\ &= m.c.d\left(\frac{a}{d} \cdot d, \frac{b}{d} \cdot d\right) \\ &= d \cdot m.c.d\left(\frac{a}{d}, \frac{b}{d}\right) \end{aligned}$$

   Luego: $m.c.d\left(\frac{a}{d}, \frac{b}{d}\right) = 1$

4. El Algoritmo de Euclides. Al dividir a entre b (números enteros), se obtiene un cociente q y un residuo r. Es posible demostrar que el máximo común divisor de a y b es el mismo que el de b y r. Éste es el fundamento principal del algoritmo. También es importante tener en cuenta que el máximo común divisor entre cualquier número a y 0 es precisamente a.

5. Si $m.c.d.(a, b) = d$ entonces existen x, y, y tales que $ax + by = d$.

   Dados $a, b \in \mathbb{Z}$, con $a \neq 0$, o, $b \neq 0$, y, $d = m.c.d.(a, b)$. La escritura del $m.c.d.(a, b)$ como combinación lineal de a y b se consigue despejando cada residuo en las igualdades del algoritmo de Euclides, empezando por el último hasta rescatar a y b. Explicitamente:

$$\begin{aligned} a &= bq + r \\ b &= rq_1 + r_1 \\ r &= r_1q_2 + r_2 \\ r_1 &= r_2q_3 + r_3 \\ &\vdots \end{aligned}$$

$r_{n-1} = r_n q_{n+1} + r_{n+1}$
$r_n = r_{n+1} q_{n+2}$

de acá nos devolvemos,
$r_{n+1} = r_{n-1} - r_n(q_{n+1})$
$r_{n+1} = r_{n-1}(1 + q_n q_{n+1}) - r_{n-2}(q_{n+1})$
$r_{n+1} = r_{n-3}(1 + q_n q_{n+1}) - r_{n-2}[(1 + q_n q_{n-1})q_{n-1} + q_{n+1})]$
$r_{n+1} = r_{n-3}\{(1+q_n q_{n+1})+q_{n-2}[(1+q_n q_{n+1})q_{n-1}-q_{n+1}]\}-r_{n-4}[(1+q_n q_{n+1})q_{n-1}-q_{n+1}]$
$r_{n+1} = r_{n-5}\{(1+q_n q_{n+1})+q_{n-2}[(1+q_n q_{n+1})q_{n-1}-q_{n+1}]\}-r_{n-4})\{q_{n-3}[(1+q_n q_{n+1})+$
$q_{n-2}[(1+q_n q_{n+1})q_{n-1}-q_{n+1}]]+[(1+q_n q_{n+1})q_{n-1}-q_{n+1}]\}$
$\vdots$
$r_{n+1} = r_1\{(1+q_4 q_5)+q_2[(1+q_4 q_5)q_3-q_5]\}-r[(1+q_4 q_5)q_3-q_5]$
$r_{n+1} = r\{(1+q_3 q_4)+q_1[(1+q_3 q_4)q_2-q_4]\}-b[(1+q_3 q_4)q_2-q_4]$
$r_{n+1} = b\{(1+q_2 q_3)+q[(1+q_2 q_3)q_1-q_3]\}-a[(1+q_2 q_3)q_1-q_3]$

Cabe anotar que el reciproco de éste resultado no es cierto o sea: si $ax + by = d$, no necesariamente el $m.c.d.(a, b) = d$.

Por ejemplo: $2 \cdot 3 + 4 \cdot 1 = 10$ y sin embargo $m.c.d.(2, 4) \neq 10$.

Según lo antes mencionado, para calcular el máximo común divisor de 2366 y 273 se puede proseguir de la siguiente manera:

Paso	Operación	Significado
1	2366 dividido entre 273 es 8 y sobran 182	$m.c.d.(2366, 273) = m.c.d.(273, 182)$
2	273 dividido entre 182 es 1 y sobran 91	$m.c.d.(273, 182) = m.c.d.(182, 91)$
3	182 dividido entre 91 es 2 y sobra 0	$m.c.d.(182, 91) = m.c.d.(91, 0)$

La secuencia de igualdades $m.c.d.(2366, 273) = m.c.d.(273, 182) = m.c.d.(182, 91) = m.c.d.(91, 0)$ implican que $m.c.d.(2366, 273) = m.c.d.(91, 0) = 91$, entonces se concluye que $m.c.d.(2366, 273) = 91$. Este mismo procedimiento se puede aplicar a cualesquiera dos números naturales. En general, si se desea encontrar el máximo común divisor de dos números naturales a y b, se sigue la siguiente regla:

1. Si $b = 0$ entonces $m.c.d.(a, b) = a$ y el algoritmo termina.

2. En otro caso, $m.c.d.(a, b) = m.c.d.(b, r)$ donde r es el resto de dividir a entre b. Para calcular $m.c.d.(b, r)$ se utiliza la misma regla.

Supongamos que llamamos $a = r_0$ y $b = r_1$. Aplicando estas reglas se obtiene la siguiente secuencia de operaciones:

Paso	Operación	Significado
1	r_0 dividido entre r_1 es q_1 y sobran r_2	$m.c.d.(r_0, r_1) = m.c.d.(r_1, r_2)$
2	r_1 dividido entre r_2 es q_2 y sobran r_3	$m.c.d.(r_1, r_2) = m.c.d.(r_2, r_3)$
3	r_2 dividido entre r_3 es q_3 y sobran r_4	$m.c.d.(r_2, r_3) = m.c.d.(r_3, r_4)$
$\vdots$	$\vdots$	$\vdots$
n	r_{n-1} dividido entre r_n es q_n y sobran r_{n+1}	$m.c.d.(r_{n-1}, r_n) = m.c.d.(r_n, r_{n+1})$
$n+1$	r_n dividido entre r_{n+1} es q_{n+1} y sobra 0	$m.c.d.(r_n, r_{n+1}) = m.c.d.(r_{n+1}, 0)$

5.4.1. Solución Particular

Iniciaremos con un teorema de existencia, el cual nos garantiza cuándo una ecuación de la forma $ax + by = c$, con a, b, $c \in \mathbb{Z}$, tiene solución entera.

Teorema: Sean a, b y c tres números enteros. La ecuación lineal $ax + by = c$ tiene solución entera si, y sólo si el máximo común divisor de a y b divide a c.

Demostración

"Solo si". En efecto, supongamos que los enteros x_0, e, y_0 son solución de la ecuación $ax + by = c$, es decir, $ax_0 + by_0 = c$. Si $d = m.c.d.(a, b)$ entonces $d \mid a$ y $d \mid b$, por lo tanto, $d \mid (ax_0 + by_0)$, así que $d \mid c$.

"Si". Recíprocamente, supongamos que $d = m.c.d.(a, b) \mid c$, entonces $m.c.d.\left(\frac{a}{d}, \frac{b}{d}\right) = 1$, esto de acuerdo al resultado 3, por lo tanto, existen $p, q \in \mathbb{Z}$ tales que $\frac{ap}{d} + \frac{bq}{d} = 1$, esto de acuerdo al resultado 4, así que $\frac{acp}{d} + \frac{bcq}{d} = c$, hagamos $x_0 = \frac{cp}{d}$, $y_0 = \frac{cq}{d}$. De esto tendríamos que:

$$ax_0 + by_0 = c$$

Es decir los enteros x_0 e y_0 son solución de la ecuación. La solución encontrada se llamará solución particular.

Ejemplo:

Encontrar una solución para la ecuación diofántica $525x + 100y = 50$

Solución: Veamos si existe solución entera para la ecuación, calculando el máximo común divisor entre 525 y 100 mediante el algoritmo de Euclides.

$$525 = 5 \times 100 + 25;\ 100 = 4 \times 25 + 0$$

es decir, el máximo común divisor de 525 y 100 es 25, y como 25 divide a 50 el teorema anterior asegura la existencia de solución entera para la ecuación. Ahora calculamos una solución particular.

Siguiendo el método indicado en la demostración del teorema, hallamos los coeficientes de la combinación lineal del máximo común divisor entre 525 y 100. Basta seguir el algoritmo de Euclides hacia atrás.

$$25 = 1 \times 525 + (-5) \times 100$$

Por tanto, los coeficientes buscados son $p = 1$ y $q = -5$ y según el citado teorema una solución para la ecuación es:

$$x_0 = \frac{cp}{d} = \frac{50 \times 1}{25} = 2, \text{e}, y_0 = \frac{cq}{d} = \frac{50 \times (-5)}{25} = -10$$

Esta es la solución particular para la ecuación.

5.4.2. Solución General

Sean a, b y c tres números enteros no nulos tales que $d = m.c.d.(a, b) \mid c$, es decir d divide a c. Entonces la solución general de la ecuación $ax + by = c$ es

$$x = x_0 + k \times \frac{b}{d},\ \ e,\ \ y = y_0 - k \times \frac{a}{d}$$

donde x_0 e y_0 es una solución particular de la misma y $k \in \mathbb{Z}$.

Demostración

Sea $d = m.c.d.(a, b)$. Por hipótesis d divide a c luego el teorema 2.4.1 asegura la existencia de una solución particular $x = x_0$ e $y = y_0$ para la ecuación.
Efectivamente,

$$ax + by = a\left(x_0 + \frac{kb}{d}\right) + b\left(y_0 - \frac{ka}{d}\right) = ax_0 + \frac{akb}{d} + by_0 - \frac{bka}{d} = c + 0 = c$$

Esto muestra que $x = x_0 + \frac{kb}{d}$, y, $y = y_0 - \frac{ka}{d}$ es solución de la ecuación $ax + by = c$.

Veamos como encontrar otra solución x_1, y, y_1. De la ecuación $ax + by = c$, tenemos que $ax_0 + by_0 = c$, puesto que $d \mid c$, así que $\frac{ax_0}{d} + \frac{by_0}{d} = \frac{c}{d}$; $\frac{a}{d}$, $\frac{b}{d}$, $\frac{c}{d} \in \mathbb{Z}$ y $m.c.d.\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. Si x_1, y, y_1, son solución entonces:

$$\frac{ax_1}{d} + \frac{by_1}{d} = \frac{c}{d}$$

Así que, si:

$\frac{ax_1}{d} + \frac{by_1}{d} = \frac{c}{d}$, y, $\frac{ax_0}{d} + \frac{by_0}{d} = \frac{c}{d}$, entonces $\frac{a(x_1 - x_0)}{d} + \frac{b(y_1 - y_0)}{d} = 0$, luego $\frac{a(x_1 - x_0)}{d} = \frac{b(y_0 - y_1)}{d}$, de aquí $\frac{b}{d} \mid \frac{a}{d}(x_1 - x_0)$, al ser $\frac{b}{d}$ primo con $\frac{a}{d}$, entonces $\frac{b}{d} \mid (x_1 - x_0)$, por lo tanto existe $k \in \mathbb{Z}$, tal que $x_1 - x_0 = \frac{kb}{d}$, es decir, $x_1 = x_0 + \frac{kb}{d}$. Ahora $\frac{a}{d}\left(\frac{kb}{d}\right) + \frac{b(y_1 - y_0)}{d} = 0$, de donde $y_1 - y_0 = -\frac{ak}{d}$, así que $y_1 = y_0 - \frac{ak}{d}$.

Veamos finalmente que x_1 e y_1 son efectivamente, solución de la ecuación $ax + by = c$.

En efecto,

$$\begin{aligned} ax_1 + by_1 &= a\left(x_0 + \frac{bk}{d}\right) + b\left(y_0 - \frac{ak}{d}\right) \\ &= ax_0 + \frac{abk}{d} + by_0 - \frac{abk}{d} \\ &= ax_0 + by_0 \\ &= c \end{aligned}$$

luego, $x = x_0 + \frac{bk}{d}$, y, $y = y_0 - \frac{ak}{d}$, es solución de la ecuación $ax + by = c$ cualquiera que sea $k \in \mathbb{Z}$. La llamaremos solución general de dicha ecuación.

En el ejemplo anterior, teníamos que, $x_0 = 2$, e, $y_0 = -10$ es una solución particular para la ecuación, $525x + 100y = 50$ luego una solución general de la misma, es: $x = 2 + \frac{100k}{25} = 2 + 4k$, y, $y = -10 - \frac{525k}{25} = -10 - 21k$, siendo k cualquier número entero.

Ejercicios

1. Calcular las soluciones enteras de la ecuación diofántica $66x + 550y = 88$

   Solución: Veamos si la ecuación $66x + 550y = 88$ admite solución entera. Para ello calculemos el máximo común divisor de 66 y 550, lo haremos utilizando el algoritmo de Euclides.

   Tenemos que: $550 = 8 \times 66 + 22$, y, $66 = 3 \times 22 + 0$, así que $(66, 550) = 22$ y como 22 divide a 88, por el teorema de la solución particular se sigue que la ecuación propuesta admite una solución particular $x = x_0, y = y_0$.

   Calculamos esta solución particular. Revertiendo el algoritmo de Euclides, tenemos que:

   $22 = 1 \times 550 + (-8) \times 66$, luego, $x_0 = \frac{88 \cdot (-8)}{22} = -32$, y, $y_0 = \frac{88 \cdot 1}{22} = 4$ es una solución particular de la ecuación.

   Efectivamente $66(-32) + 500(4) = -2112 + 2200 = 88$

   Ahora, la solución general viene dada por $x = -32 + \frac{550k}{22} = -32 + 25k$, y, $y = 4 - \frac{66k}{22} = 4 - 3k$, siendo k cualquier número entero.

2. Una persona va a un supermercado y compra 12 litros de leche, unos de leche entera y otros de desnatada, por 1200 pesetas. Si la leche entera vale 30 pesetas. más por litro que la desnatada, y ha comprado el mínimo posible de leche desnatada, Cuántos litros habrá comprado de cada una?

   Solución:
   Si x el número de litros de leche entera, entonces $12 - x$ es el número de litros

de leche desnatada y si y es el precio de la leche desnatada, entonces el precio de la leche entera será $y + 30$. Como el precio total de la leche comprada es 1200, tendremos que:

$x(y + 30) + y(12 - x) = 1200$, tal que $x \geq 0$, y, $12 - x \geq 1$

luego,

$$xy + 30x + 12y - xy = 1200$$

entonces,

$$30x + 12y = 1200$$

Puesto que $m.c.d.(30, 12) = 6$ y 6 divide a 1200, entonces hay solución entera. Puesto que $6 = 1 \cdot 30 + (-2) \cdot 12$, entonces

$$x_0 = \frac{1200 \cdot 1}{6} = 200, \text{ y, } y_0 = \frac{1200 \cdot (-2)}{6} = -400$$

La solución general será:

$$x = 200 + \frac{12k}{6} = 200 + 2k, \text{ y, } y = -400 - \frac{30k}{6} = -400 - 5k$$

siendo k cualquier número entero.

Veamos, finalmente, cuántos litros se han comprado de cada tipo de leche. Según lo visto hasta ahora, la cantidad de leche entera es:

$$C_e = 200 + 2k; k \in \mathbb{Z}$$

y la cantidad de leche desnatada será, por tanto,

$$C_d = 12 - C_e = 12 - 200 - 2k = -188 - 2k; k \in \mathbb{Z}$$

Pues bien, suponiendo que se compra alguna cantidad de leche desnatada, tendremos que:

$0 < C_e < 12$, luego, $0 < 200 + 2k < 12$, así que, $-200 < 2k < -188$, y de esto, $-100 < k < -94$, por lo tanto, $k \in \{-99, -98, -97, -96, -95\}$.

Y la cantidad mínima de leche desnatada se correspondería con la máxima de leche entera y esta se da para el valor máximo que pueda tener k, es decir para $k = -95$. Por tanto,

$C_e = 200 + 2(-95) = 200 - 190 = 10$, y, $C_d = 12 - C_e = 2$, o sea, se compraron 10 litros de leche entera y 2 litros de leche desnatada.

5.5. Método de Euler

Supongamos que queremos encontrar una solución particular de la ecuación diofántica lineal en dos variables $ax + by = c$. Sea $a < b$ (si fuera al reves, bastaría intercambiar los papeles de x e y). Descomponemos b y c dividiendo cada uno de estos términos por a, tenemos que $b = Ba + B_1$ y $c = Ca + C_1$, así que $ax + (Ba + B_1)y = Ca + C_1$, de donde $ax = Ca + C_1 - (Ba + B_1)y$, por lo tanto $x = (C - By) + \frac{C_1 - B_1 y}{a}$.

Puesto que $x \in \mathbb{Z}$, entonces $\frac{C_1 - B_1 y}{a} \in \mathbb{Z}$, por lo que bastaría ir dando a y los valores $0, 1, \ldots, (a-1)$ para encontrar una solución particular y_0.

Ejemplo 1.

Una bufanda cuesta 19 rublos, pero el comprador no tiene más que billetes de tres rublos; y la cajera, solo de cinco. puede en estas condiciones abonarse el importe de la compra, y cómo hacerlo?

La misión de este ejercicio se reduce a saber cuántos billetes de tres rublos deben entregarse a la cajera para que ella dé las vueltas con billetes de cinco, cobrando los 19 rublos. Las incógnitas del problema son dos: el número de billetes de tres rublos x y el número de billetes de cinco y.

Asi que la ecuación para este problema es: $3x - 5y = 19$

Solución: Aquí tenemos que hallar valores enteros de x y de y en la ecuación $3x - 5y = 19$.

De aquí tenemos que $-5y + 3x = 19$, y, dado que $-5 < 3$, tenemos que $3 = -5(-2) - 7$, y, $19 = -5(-5) - 6$, por lo tanto $y = \frac{19 - 3x}{-5} = \frac{25 - 6 - 10x + 7x}{-5} = -5 + 2x + \frac{6 - 7x}{5}$. Puesto

que $y \in \mathbb{Z}$, entonces $6 - 7x$ debe ser multiplo de 5, así que x puede ser 3 con lo cual $y = -2$, o, $x = 8$, y, $y = 1$, tomamos a estos últimos como los valores iniciales porque x, y, y deben ser positivos.

Como $y, -5$ y x son números enteros, la ecuación puede ser acertada sólo en el caso de que $-5 + 2x + \frac{6-7x}{5}$ sea también un número positivo.

Donde la solución particular es $(x_0, y_0) = (8, 1)$

Ahora buscaremos la solución general utilizando el Algortimo de Euclides y teniendo presente un resultado anterior:

$$y = y_0 - \frac{bt}{d} = 1 + 3t, \text{ y, } x = x_0 + \frac{at}{d} = 8 - (-5)t = 8 + 5t$$

Como, $1 + 3t > 0$, y, $8 + 5t > 0$, entonces $t > -\frac{1}{3}$, o sea $t \in \{0, 1, 2, 3, 4, \ldots\}$

De esta manera hemos encontrado valores para x, y, y. Algunos de ellos son $(8, 1); (13, 4); (18, 7) \ldots$

En realidad sólo se ha demostrado que toda solución entera para la ecuación $-5y + 3x = 19$ se presenta como $x = 3 + 5t$, $y = -2 - 3t$ donde t representa un número entero. Más no hemos demostrado lo contrario, que siendo t un número entero cualquiera obtendremos cierta solución entera. Sin embargo, es fácil convencerse de ello cuando invertimos el orden de nuestro razonamiento o cuando colocamos el valor de x y de y en la ecuación inicial.

Sabemos que x, y, y son enteros y además positivos, por lo tanto, con esto el valor de t esta acotado inferiormente

Como t es un número entero no negativo, entonces t puede tener los siguientes valores:

$$t = 0, 1, 2, 3, 4, \ldots$$

Ejemplo 2.

Hallar todos los pares de enteros x e y tales que:

$$x \cdot y = 20 - 3x + y$$

Solución: Puesto que $xy = 20 - 3x + y$, tenemos que $xy + 3x = 20 + y$, de donde $x(y+3) = 20 + y$, así que:

$$x = \frac{20+y}{3+y} = 1 + \frac{17}{y+3}, \text{ haciendo, } t = \frac{17}{y+3} \in \mathbb{Z},$$

obtenemos $x = 1 + t$

Puesto que 17 es un número primo tenemos que: $y + 3 = \pm 1$, o, $y + 3 = \pm 17$

Si $y + 3 = 1$, entonces $y = -2$; Si $y + 3 = -1$, entonces $y = -4$;
Si $y + 3 = 17$, entonces $y = 14$; Si $y + 3 = -17$, entonces $y = -20$

Así que y puede ser $-2, -4, 14, -20$ y x seria respectivamente $18, -16, 2, 0$ y los pares que satisfacen la condición serian $(18, -2); (-16, -4); (2, 14); (0, -20)$.

Ejemplo 3

Un granjero gastó 100000 pesetas, en 100 animales entre pollos, conejos y terneros. Si los pollos los compró a 50 pesetas, los conejos a 1000 pesetas y los terneros a 5000 pesetas, y adquirió animales de las tres clases, Cuántos animales compró de cada clase?

Solución: Sean x, y y z el número de pollos, conejos y terneros, respectivamente. De acuerdo con el enunciado tendremos las siguientes ecuaciones:

$$x + y + z = 100 \quad (5.1)$$
$$50x + 1000y + 5000z = 100000 \quad (5.2)$$

Simplificando la ecuación (5.2) tenemos,

$$x + 20y + 100z = 2000 \quad (5.3)$$

Así que $19y + 99z = 1900$

Para resolver la ecuación calculamos el máximo común divisor de 19 y 99 por el algoritmo de Euclides así que:

$99 = 5 \cdot 19 + 4 = 5(4 \cdot 4 + 3) + 4 = 5[4(1 \cdot 3 + 1) + 3] + 4$ de donde $m.c.d.(99, 19) = 1$

Por lo tanto la ecuación tiene solución entera.

Calculamos una solución particular
Tenemos que:

$$\begin{aligned} 1 &= 4 - 1 \cdot 3 = 4 - 1(19 - 4 \cdot 4) \\ &= 4 - 19 + 4 \cdot 4 = 5 \cdot 4 - 19 \\ &= 5(99 - 5 \cdot 19) - 19 \\ &= 5 \cdot 99 - 26 \cdot 19 \end{aligned}$$

de donde

$$\begin{aligned} 1900 &= 99(5 \cdot 1900) - 19(26 \cdot 1900) \\ &= 99(9500) - 19(49400) \end{aligned}$$

por lo tanto, $y_0 = -49400$, y, $z_0 = 9500$

La solución general será,

$$\begin{aligned} y &= -49400 + \frac{99k}{1} = -49400 + 99k \\ z &= 9500 - \frac{19k}{1} = 9500 - 19k \end{aligned}$$

siendo k cualquier número entero.

Finalmente, para determinar cuántos animales de cada clase se compró. Sabiendo que adquirió animales de las tres clases, tendremos que: $y \geq 1$ es decir $-49400 + 99k \geq 1$, de donde, $99k \geq 49401$, y, $k \geq 499$, además $z > 0$ de aquí $9500 - 19k > 0$ y $19k < 9500$ así que $k < 500$, por lo tanto $k = 499$, de esto se obtiene que $y = -49400 + 99 \cdot 499 = 1$, $z = 9500 - 19 \cdot 499 = 19$, y, $x = 100 - (y + z) = 100 - 20 = 80$.

Por tanto compró 80 pollos, 1 conejo y 19 terneros.

5.6. Congruencias Modulares

5.6.1. Definición de Congruencia:

Dos enteros, a y b, son congruentes módulo m si dan el mismo resto cuando se dividen por m . Se acostumbra a simbolizar por $a \equiv b \pmod{m}$. Así, por ejemplo, los números 5 y 9 son congruentes modulo 2, pues al dividir cada uno de ellos por 2, se obtiene igual resto, 1. Lo indicaremos, como $5 \equiv 9 \pmod{2}$.

Algunas propiedades de las congrunecias son:

1. $a \equiv b \pmod{m}$ si y sólo si existe $k \in \mathbb{Z}$ tal que $a-b = k \cdot m$, o sea, es equivalente que dos números enteros sean congruentes modulo m y que su diferencia sea un múltiplo de m. Si representamos al conjunto de los múltiplos de m por (m), podemos escribir la propiedad asi: $a \equiv b \pmod{m}$ si y sólo si $(a-b) \in (m)$.

2. Si $a \equiv b \pmod{m}$ y $m.c.d.(a,m) = 1$ entonces $m.c.d.(b,m) = 1$. Es decir, si dos números son congruentes módulo m, y m es primo con uno de ellos, entonces m es primo con el otro.

3. Si $a \equiv b \pmod{m}$ entonces $(q_0 + q_1^n a) \equiv (q_0 + q_1^n b) \pmod{m}$, para todo $q_0, q_1 \in \mathbb{Z}$. Si dos números enteros son congruentes módulo m, también son congruentes módulo m si se les multiplica por una misma potencia natural de un entero q_1 y se les suma un mismo entero q_0.

4. Si $a \equiv b \pmod{m}$, y, $f(x) = q_0 + q_1 x + \ldots q_n x^n$ entonces $f(a) \equiv f(b) \pmod{m}$. Esta propiedad generaliza la anterior para un polinomio cualquiera $f(x)$ con coeficientes enteros.

5. Si $a = b + k \cdot m$ entonces $a \equiv b \pmod{m}$.

6. Si $a = km$ entonces $a \equiv 0 \pmod{m}$.

7. Si $a \equiv b \pmod{m}$ y $q \mid a$; $q \mid b$; $m.c.d.(q,m) = d$ entonces $\frac{a}{q} \equiv \frac{b}{q} \pmod{\frac{m}{d}}$. Esto es, si dos números enteros son congruentes módulo m y el entero q divide a ambos entonces los cocientes respectivos también son congruentes módulo $\frac{m}{d}$, siendo d el máximo común divisor de q y de m.

Demostración

1. Si $a \equiv b \pmod{m}$ si y sólo si a y b dejan el mismo resto al dividirlos por m, es decir, existen $q_1,\ q_2 \in \mathbb{Z}$ tales que $a - mq_1 = b - mq_2 = r$, y de aquí $a - b = m(q_1 - q_2)$, esto quiere decir que $m \mid (a - b)$.

2. Puesto que m.c.d. $(a, m) = 1$ existen $x_1, x_2 \in \mathbb{Z}$, tales que, $x_1a + x_2m = 1$, y de aqui se tendría: $x_1a = 1 - x_2m$, ahora $a - b = km$, por lo tanto $ax_1 = bx_1 + kmx_1$, de donde $1 - x_2m = x_1b + kmx_1$, así que $1 = x_1b + (x_2 + kx_1)m$ y de aqui tenemos que $m.c.d.(b, m) = 1$

3. Hay que probar que la diferencia es múltiplo de m: $(q_0 + aq_1^n) - (q_0 + bq_1^n) = q_1^n(a - b) = q_1^n(km)$, de donde $(q_0 + aq_1^n) \equiv (q_0 + bq_1^n) \pmod{m}$ siempre y cuando $a \equiv b \pmod{m}$

4. Es una generalización de la propiedad anterior.

5. Si $a = b + km$ entonces $(a - b) = km$, lo cual significa que $m \mid (a - b)$ así que $a \equiv b \pmod{m}$

6. Si $a = km$ entonces $a - 0 = km$ de donde $a \equiv 0 \pmod{m}$

7. Si $a \equiv b \pmod{m}$ y $q \mid a, q\_$ y $m.c.d.(q, m) = d$ entonces $a - b = km$; $a = ql, b = qn$, ademas $d \mid q$ y $d \mid m$, de esto obtenemos que $ql - qn = km; q = dq', m = dm'$ por lo tanto $dq'l - dq'n = kdm', \frac{a}{q} - \frac{b}{q} = \frac{a-b}{q} = \frac{km}{dq'}$ así que $\frac{a}{q} - \frac{b}{q} = \left(\frac{k}{q'}\right)\left(\frac{m}{d}\right)$, de donde $\frac{a}{q} \equiv \frac{b}{q}(\pmod{\left(\frac{m}{d}\right)})$, lo único que faltaria sería probar que $\frac{k}{q}, \in \mathbb{Z}$, pero eso se obtiene porque $dq'l - dq'n = kdm'$ por lo que $q'(l - n) = km'$, así que $\frac{kd}{q} = \frac{l-n}{m'} = \frac{k}{q'}$

Ejemplo de aplicación de estas propiedades:

Si $12 \equiv 7x \pmod{5}$, se tiene que $12 - 7x = 5m$, para algún $m \in \mathbb{Z}$, así que: $12 - 5m = 7x$, de donde $10 + (2 - 5m) = 5x + 2x$, y de aquí $2 - 5m = 2x$, hemos eliminado a 10 y $5x$, por ser multiplos de 5 por lo tanto $2 - 2x = 5m$, y esto a la vez equivale a $1 \equiv x \pmod{5}$, porque el $m.c.d.(2, 5) = 1$, de esto podemos decir que $1 - x = 5k$, así que $5m = 2 - 2x = 2(1 - x) = 2(5k) = 10k$, de donde $m = 2k$

5.6.2. Inversos Modulares

Supóngase que se conocen los valores de a, b y m, pero que se desconoce el valor x de la siguiente ecuación:

$$ax \equiv b \pmod{m}$$

Resolvemos $ax \equiv b \pmod{m}$, donde a, b y m son constantes, con $a \neq 0$. Puesto que $ax \equiv b \pmod{m}$ equivale a $ax - b = km$, así que basta encontrar un valor de a^{-1} que satisfaga que $a^{-1} \cdot a \equiv 1 \pmod{m}$, luego $a^{-1} \cdot (ax) = a^{-1}(b + km)$, es decir $x = a^{-1}b + a^{-1}km$, de donde $x \equiv a^{-1}b \pmod{m}$.

Al valor a^{-1} se le llama inverso modular de a módulo m.

Ejemplo 1:
Resolver la congruencia $5x \equiv 2 \pmod{9}$
Aquí tenemos que $5x = 2 + 9k$, puesto que $9 = 10 - 1$, tenemos que multiplicar por 2 para obtener $10x = 4 + 9(2k) = 9x + x$, así que $x \equiv 4 \pmod{9}$, y de esta manera $x = 4 + 9m$, con $m \in \mathbb{Z}$. Una solución es $x = 4$.

Observemos que 2 es un inverso modular de 5 ya que $5 \cdot 2 \equiv 1 \pmod{9}$.

Podemos verificar que $x = 4 + 9m$ es solución de $5x \equiv 2 \pmod{9}$ ya que $5x = 5(4 + 9m) = 20 + 45m$, así que $5x - 2 = 45m + 18 = 9(5m + 2)$, lo que significa que $5x \equiv 2 \pmod{9}$.

5.6.3. Congruencias lineales

Son congruencias de la forma $a \cdot x \equiv b \pmod{m}$, donde m no divide a a.

Si x_1 es solución de la congruencia lineal, también es solución $x_1 + k_1 m$, cualquiera que sea el entero k_1. Los valores $x_1 + k_1 m$ representan la clase residual si $b \pmod{m}$ es el resto al dividir b por m, la relación de tener el mismo módulo se llama relación de congruencia y es de equivalencia y clase residual $x_1 + k_1 m$ es la clase constituida por todos los números congruentes módulo m, es decir por todos los números que tienen el mismo resto x_1 al dividirlos por m a la cual pertenece $x_1 : a(x_1 + k_1 m) - b = km$ es decir $ax_1 - b = (k - k_1)m$, de donde $ax_1 \equiv b \pmod{m}$.

Así, si x_1 verifica la congruencia lineal, también la verifican todos los elementos de su clase residual:

$$x_1 + m, x_1 + 2m, \ldots$$

Ejemplo 1: Cuál es la solución de la congruencia lineal $3x \equiv 4 \pmod 7$?

Puesto que $m.c.d.(3, 7) = 1$ entonces la congruencia planteada tiene solución. De $3x \equiv 4 \pmod 7$, tenemos que $3x = 4 + 7k$; puesto que $15 - 1 = 2 \cdot 7$, multiplicamos la ecuación por 5 y obtenemos $15x = 20 + 7(5k) = 14x + x$ y de aquí $x \equiv 20 \pmod 7$, de donde $x = 20 + 7\alpha$, $\alpha \in \mathbb{Z}$

Si $\alpha = -2$ tenemos que $x = 6$, que es una solución.

Aquí 5 es un inverso modular de 3 ya que $5 \cdot 3 \equiv 1 \pmod 7$.

Ejemplo 2:

La congruencia lineal $3 \cdot x \equiv 5 \pmod 2$ es satisfecha, por ejemplo, por $x = 1$, también la verifican los elementos de su clase residual: $1+2\cdot 1; 1+2\cdot 2; 1+2\cdot 3; \ldots; 1+2\cdot k_1; \ldots$

Sin embargo, usando la propiedad 5 de las congruencias, la congruencia lineal de este ejemplo es equivalente a $(2x + x) \equiv (4 + 1) \pmod 2$ y de aquí $x \equiv 1 \pmod 2$.

5.6.4. Soluciones congruentes y soluciones incongruentes:

Se denominan soluciones congruentes de una congruencia lineal módulo m a los enteros que las satisfacen y pertenecen a la misma clase residual módulo m.

Son soluciones incongruentes de una congruencia lineal módulo m a los enteros que la satisfacen y pertenecen a clases residuales distintas.

Por convenio, entenderemos que el conjunto solución de una congruencia lineal módulo m contiene exactamente un representante de cada una de las diferentes clases residuales módulo m cuyos miembros satisfacen la congruencia lineal dada. Esto es, las soluciones incongruentes que pertenecen a cualquier sistema completo de residuos módulo m constituye un conjunto solución.

El problema clave es, por consiguiente, determinar cuántas soluciones incongruentes existen, esto es, cuántas clases residuales, tiene la congruencia lineal dada. Para ello estudiaremos el siguiente teorema.

La congruencia lineal $a{\cdot}x \equiv b \pmod{m}$ tiene exactamente d soluciones incongruentes, donde es $d = m.c.d.(a, m)$ si y sólo si d divide a b. Si d no divide a b, entonces la congruencia lineal no tiene solución.

Demostración

Veamos en primer lugar que si es $d = m.c.d.(a, m)$, entonces d ha de dividir a b. En efecto si $d = m.c.d.(a, m)$, entonces $d \mid a$ y $d \mid m$, puesto que $ax \equiv b \pmod{m}$, entonces $ax = b + my$, de aquí, $b = ax - my$, así que $d \mid b$.

Ahora miraremos el número de soluciones incongruentes módulo m. Puesto que $ax \equiv b \pmod{m}$ es equivalente a $ax - my = b$ entonces $\frac{a}{d}x - \frac{m}{d}y = \frac{b}{d}$, o sea $a'x - m'y = b'$ y $m.c.d.(a', m') = 1$. Las soluciones de $a'x - m'y = b'$; son $x = x_0 + m't; t = 0, 1, \ldots$, todas congruentes módulo m'.

Estas soluciones, que también son soluciones de la ecuación $ax - my = b$, aunque son congruentes módulo m' podrían, algunas de ellas, no ser congruentes módulo m. Vamos a encontrar las que no son congruentes módulo m.

Si dos de estas soluciones, $x_0 + m't_1$ y $x_0 + m't_2$, fueran congruentes módulo m, tendrian que verificar:

$$x_0 + m't_1 \equiv (x_0 + m't_2) \pmod{m}$$

y, por las propiedades de las congruencias:
$m't_1 \equiv m't_2 \pmod{m}$ o bien: $t_1 \equiv t_2 \pmod{\frac{m}{m'}}$ es decir, $t_1 \equiv t_2 \pmod{d}$.

Es decir, los valores de t que dan soluciones $x = x_0 + m't$ congruentes módulo m son aquellos que son congruentes módulo d. Las soluciones $x = x_0 + m't$ incongruentes módulo m, son, por consiguiente, aquellas en las que figuren valores de t que no sean congruentes módulo d. Y, obviamente, como los valores de t son la sucesión $0, 1, 2, \ldots, n, \ldots$,los únicos que son incongruentes módulo d son aquellos menores que $d : 0, 1, 2, \ldots, (d - 1)$

Por tanto, las soluciones incongruentes de la congruencia lineal $ax \equiv b \pmod{m}$ son las soluciones $\{x_0, x_0 + m', x_0 + 2m', \ldots, x_0 + (d-1)m'\}$, donde $d = m.c.d.(a, m)$.

Ejemplo 1.

Hallemos las soluciones de la congruencia lineal $18x \equiv 24 \pmod{12}$. Se tiene que $m.c.d.(18, 12) = 6$, que obviamente divide también a 24, por lo que la congruencia tiene solución.

Dividiendo toda ella por 6 obtenemos la congruencia reducida: $3x \equiv 4 \pmod{2}$, que se puede escribir como la ecuación diofántica: $3x - 2y = 4$, con solución particular $x_0 = 2, y_0 = 1$.

Los valores de x que verifican la ecuación son, en definitiva: $x = x_0 + m't, t = 0, 1, \ldots$ esto es, $x = 2 + 2t, t = 0, 1, \ldots$ que son soluciones congruentes módulo m', es decir, la ecuación reducida tiene una sola solución incongruente, que podemos representar por $x_0 = 2$.

Pero no todas estas soluciones congruentes modulo $m' = 2$ son también congruentes módulo $m = 12$. Así, no son congruentes módulo 12 aquellas que corresponden a valores de t que no sean congruentes modulo 6:

No son congruentes módulo 12 las soluciones en las que $t = 0, 1, 2, 3, 4, 5$ que serían:

$$2 = 2; 2 + 2 \cdot 1 = 5;\ 2 + 2 \cdot 2 = 6;\ 2 + 3 \cdot 2 = 8;\ 2 + 4 \cdot 2 = 10;\ 2 + 5 \cdot 2 = 12$$

es decir: $2, 4, 6, 8, 10, 12$

Si restamos dos cualesquiera de ellas tendría que ser la diferencia un múltiplo de 12, lo cual no ocurre, y, sin embargo, cada una de ellas verifica la congruencia lineal $18x \equiv 24 \pmod{12}$. Son por tanto soluciones incongruentes, cada una representando un conjunto infinito de soluciones entre si congruentes:

{2} = {2, 14, 26, 38,. . . }, {4}= {4, 16, 28, 40,. . . }, {6}= {6, 18, 30, 42,. . . }

{8} = {8, 20, 32, 44, . . . }, {10}= {10, 22, 34, 46,. . . }, {12}= {12, 24, 36, 48,. . . }

Ejemplo 2.

Hallemos las soluciones de la congruencia lineal $39x \equiv 60$ (mód 6). Se tiene que $m.c.d.(39, 6) = 3$, que obviamente divide también a 60, por lo que la congruencia tiene solución.

Dividiendo toda ella por 3 obtenemos la congruencia lineal reducida: $13x \equiv 20$ (mód 2), que se puede escribir como la ecuación diofántica: $13x - 2y = 20$, con solución particular $x_0 = 2, y_0 = 3$.

Soluciones de la congruencia lineal reducida: $x = 2 + 2t, t = 0, 1, 2, \ldots,$ y los valores de t que son incongruentes módulo $3 : t = 0, t = 1, t = 2$. Por tanto, las soluciones incongruentes módulo 6, de la congruencia lineal de partida son: $2, 4, 6$ cada una de ellas, representando obviamente los infinitos elementos de una clase residual:$\{2\} = \{2, 8, 14, 20, \ldots\}, \{4\} = \{4, 10, 16, 22, \ldots\}, \{6\} = \{6, 12, 18, 24, \ldots\}$.

5.7. Resolución de ecuaciones diofánticas lineales por aplicación de las congruencias lineales

Vamos a resolver ejemplos en los cuales comparamos las congruencias lineales, la solución general y el método de Euler para la solución particular.

Resolver la ecuación diofántica $5x + 2y = 9$.

Transformamos la ecuación en una congruencia lineal de módulo -2
La ecuación $5x + 2y = 9$ equivale a $5x = 9 - 2y$ y esto significa que: $5x \equiv 9$ (mód (-2)) y esto a su vez se puede escribir $(4x + x) \equiv (4 \cdot 2 + 1)$ (mód (-2)), así que $x \equiv 1$ (mód (-2)) de donde $x = 1 + (-2)k;\ k \in \mathbb{Z}$.

Una solución es $x = 1$ que ocurre cuando $k = 0$.

Si $x = 1$ entonces $5 + 2y = 9$ lleva a que $y = 2$. De manera general si $x = 1 - 2k; 2y = 9 - 5(1 - 2k) = 4 + 10k$ así que $y = 2 + 5k$.

Resolvamos de nuevo esta ecuación usando ahora el teorema de la solución general y el método de Euler:

Solución general: Tomando $x_0 = 1, y_0 = 2$ tenemos que $x = x_0 - \frac{bt}{d} = 1 - 2t;\ y = y_0 - \frac{at}{d} = 2 + 5t$.

Usamos el método de Euler

Aplicando el Algoritmo de Euclides, tenemos que: $5 = 2 \cdot 2 + 1 = 2(2 \cdot 1 + 0) + 1$, así que $1 = 5 - 2 \cdot 2$, luego una solución particular puede ser $x = 1$, y, $y = -2$.

Ahora buscamos la solución general, puesto que $5 = 2 \cdot 2 + 1$, y $9 = 4 \cdot 2 + 1$, y $5x + 2y = 9$ tenemos que

$$y = \frac{9 - 5x}{2} = \frac{4 \cdot 2 + 1 - (2 \cdot 2 + 1)x}{2} = 4 - 2x + \frac{1 - x}{2}$$

Si hacemos $t = \frac{1-x}{2}$, esto equivale a tener $x = 1 - 2t$, tenemos $y = 4 - 2(1 - 2t) + t = 2 + 5t$, y, así la solución general es $(x, y) = (1 - 2t, 2 + 5t)$ para todo t.

Resolver la ecuación diofántica $3x - 7y = 5$.

De $3x - 7y = 5$ tenemos que $3x \equiv 5 \pmod 7$, así que $15x \equiv 25 \pmod 7$ de donde $x \equiv 4 \pmod 7$ y una solución particular es $x_0 = 4$, así que $x = x_0 + \frac{7}{1}t = 4 + 7t$.

Con este valor encontramos que $y = \frac{3x-5}{7} = \frac{3(4+7t)-5}{7} = \frac{7+21t}{7} = 1 + 3t$, una solución particular es $y_0 = 1$, luego la solución general es $(x, y) = (4 + 7t, 1 + 3t)$, $t \in \mathbb{Z}$.

Mediante el teorema de solución general y Euler:

Solución general: Tenemos que $x = x_0 - \frac{b}{d}t = 4 - \frac{-7}{1}t = 4 + 7t$, y, $y = y_0 + \frac{a}{d}t = 1 + \frac{3}{1}t = 1 + 3t$, puesto que $7 = 3 \cdot 2 + 1$, y, $5 = 2 \cdot 2 + 1$, tenemos que $3x = 5 + 7y = (2 \cdot 2 + 1) + (2 \cdot 3 + 1)y$, así que, $x = \frac{(2\cdot 2+1)+(2\cdot 3+1)y}{3} = 1 + 2y + \frac{2+y}{3}$.

Puesto que $\frac{2+y}{3} \in \mathbb{Z}$, uno de los valores de y es 1, así que $y_0 = 1$, y, $x_0 = 1+2+1 = 4$, y la solución general es $(4 + 7t, 1 + 3t)$.

Capítulo 6
ECUACIONES DIOFÁNTICAS PITAGÓRICAS

6.1. Las ternas pitagóricas

Las ternas $(x; y; z)$ tales que $x^2 + y^2 = z^2$ se denomina ternas pitagóricas y originan triángulos rectángulos con lados enteros. Estudiaremos ecuaciones más generales del tipo

$$ax^2 + by^2 = cz^2; a, b, c \in \mathbb{Z}$$

En general esta ecuación no tiene por qué tener soluciones, pero si encontramos una solución $(x_0; y_0; z_0)$ vamos a poder hallar otras soluciones de la ecuación lo cual lo observamos al buscar las soluciones enteras de $ax^2+by^2 = cz^2$ es equivalente a buscar las soluciones racionales de $ax_1^2 + by_1^2 = c$, donde $x_1 = \frac{x}{z}, y_1 = \frac{y}{z}$.

Es decir, hemos de encontrar los puntos (x, y) de coordenadas racionales sobre la elipse $ax_1^2 + by_1^2 = c$. Supongamos que mediante una simple inspección hemos encontrado un punto (x_0, y_0) de coordenadas racionales sobre la elipse. Ahora trazamos una recta que pase por dicho punto y con pendiente dada $r \in \mathbb{Q}$. Esta recta cortará a la elipse en otro punto $(x_0^{'}; y_0^{'})$.

La ecuación de la recta que pasa por (x_0, y_0) y tiene pendiente r es $y-y_0 = r(x-x_0)$, si la sustituimos en la ecuación de la elipse, $ax^2 + b(y_0 + r(x - x_0))^2 = c$ obtenemos una ecuación de segundo grado que tendría como soluciones x_0 y $x_0^{'}$.

Ahora bien, la suma de las soluciones de una ecuación de segundo grado con coeficientes racionales es racional. Por lo tanto, si x_0 es racional, $x_0^{'}$ debe ser racional y sustituyendo en la ecuación de la recta anterior tenemos que $y_0^{'}$ también es racional.

Por otra parte, dos puntos de coordenadas racionales sobre la circunferencia nos determinan una recta de pendiente racional. Es decir, existe una biyección entre las soluciones enteras de la ecuación original y los puntos $x_0^{'}; y_0^{'}$ obtenidos según el método anterior.

Ahora teniendo esta información podemos demostrar el siguiente teorema.

6.1.1. Teorema

Las soluciones positivas de $x^2 + y^2 = z^2$, con x par son:

$$\begin{cases} x &= 2rs \\ y &= r^2 - s^2 \\ z &= r^2 + s^2 \end{cases}$$

donde r, s son enteros arbitrarios de paridad distinta (es decir, que uno es par y el otro impar), con $r > s > 0$ y el $m.c.d.(r, s) = 1$. Estas soluciones suelen llamarse soluciones primitivas.

Demostración 1.

Se desea resolver la ecuación $x^2 + y^2 = z^2$ en los enteros positivos, donde $m.c.d.(x, y, z) = 1$. Por tanto los tres números no pueden ser pares, porque si lo fueran el $m.c.d.(x, y, z,) \neq 1$. Tampoco dos de ellos ya que si por ejemplo x, y, y son pares z^2 seria par, así que el $m.c.d.(x, y, z) \neq 1$. Los tres no pueden ser impares, ya que $x^2 + y^2$ seria par, y habria una contradicción ya que z es impar. Así que digamos x es par y y, y, z impares.

Reescribimos la ecuación así: $x^2 = z^2 - y^2 = (z - y)(z + y)$ como los números x, $z - y$, $z + y$ son todos pares, se tiene que existen enteros positivos u, v, w tal que $x = 2u$, $z + y = 2v$, y, $z - y = 2w$. Entonces $(2u)^2 = (2v)(2w)$, simplificando obtenemos $u^2 = vw$. Además el $m.c.d.(v, w) = 1$, es decir son primos relativos ya que un divisor común de v, y, w tambien lo serian de y, y, z lo cual es imposible porque estos son primos relativos.

Tenemos entonces $u^2 = vw$, si el producto de dos enteros positivos, primos relativos v, y, w es igual a un cuadrado entonces tanto v como w son cuadrados, por tanto existen enteros positivos r, s tal que $v = r^2$, y, $w = s^2$. Además r, y, s son primos relativos, al serlos v, y, w entonces:

$$z = v + w = r^2 + s^2$$

$$y = v - w = r^2 - s^2$$

Esto nos dice que $r > s$, y que r, y, s son de paridad distinta (es decir, que uno es par y el otro impar), ya que y, y, z son impares.

Usando ahora la primera expresión podemos expresar x facilmente en terminos de r, y, s.

$$\begin{aligned} x^2 = (z^2 - y^2) &= (r^2 + s^2)^2 - (r^2 - s^2)^2 \\ &= r^4 + 2r^2s^2 + s^4 - r^4 + 2r^2s^2 - s^4 \\ &= 4r^2s^2 \\ &= (2rs)^2 \end{aligned}$$

Es decir, $x = 2rs$.

Lo que hemos obtenido es lo siguiente: dado una terna pitagórica primitiva x, y, z existen enteros positivos primos relativos r, y, s tal que $r > s$, r, y, s son de paridad distinta y la terna $(2rs, r^2 - s^2, r^2 + s^2)$ es un terna pitagórica.

6.2. Ecuaciones de la forma $x^2 - y^2 = a$

Sea $a = bc$ entonces: $bc = a = x^2 - y^2 = (x + y) \cdot (x - y)$. Aquí $x + y = b$ y $x - y = c$, o, $x + y = c$ y $x - y = b$. En cualquiera de los dos casos $2x = b + c$, y, $2y = b - c$ o $2y = c - b$, lo que significa que $b + c$ y $b - c$ son números pares y de esto podemos decir que b y c son ambos pares o ambos impares. Así que $x = \frac{b+c}{2}$, y $y = x - c = \frac{b+c}{2} - c = \frac{b-c}{2}$.

Ejemplo

Encontrar todos los valores enteros x y y en la ecuación:

$$x^2 - y^2 = 36$$

Aquí tenemos que: $(x+y)(x-y) = 36 = 1 \cdot 36 = 2 \cdot 18 = 4 \cdot 9 = 6 \cdot 6$, por el anterior analisis: $x+y = 18$, y, $x-y = 2$; $x+y = 6$, y, $x-y = 6$; $x+y = -18$, y, $x-y = -2$; $x+y = -6$, y, $x-y = -6$; son los valores que nos sirven.
De $x+y = 18$, y, $x-y = 2$, tenemos que $x = 10$, y, $y = 8$; de $x+y = 6$, y, $x-y = 6$, tenemos que $x = 6$, y, $y = 0$; de $x+y = -18$, y, $x-y = -2$, tenemos que $x = -10$, y, $y = -8$; de $x+y = -6$, y, $x-y = -6$, tenemos que $x = -6$, y, $y = 0$;
Asi las parejas (x, y) que satisfacen la ecuación son:

$$(10, 8); (6, 0); (-10, 8); (-6, 0) \text{ y } (-10, -8)$$

Capítulo 7
CONCLUSIONES

El trabajo realizado es muy importante porque permitió aplicar nuestro conocimiento, a la vez que brinda la oportunidad de darlo a conocer a todo aquel que quiera saber e investigar sobre las Ecuaciones Diofánticas.

Las Ecuaciones Diofánticas son de gran utilidad en la vida del estudiante porque permite repasar distintos temas y operaciones que manejan a través de todos los conocimientos que se desarrollan en nuestra carrera

En conclusión podemos decir que el tema fue interesante y muy agradable porque nos brindo la oportunidad de conocer a cerca de las Ecuaciones Diofánticas y nos ayudo ampliar y reforzar nuestras ideas para poderlas aplicar con más propiedad en un futuro.

Bibliografía

[1] *Christiam Huertas R.*, ECUACIONESDIOFANTICASWeb.pdf, 2008

[2] *Francisco José González Gutiérrez*, Apuntes de Matemática Discreta, Universidad de Cádiz

[3] *Francisco Javier García Capitán*, Un Pequeño Manual para la Resolución de Problemas, Priego de Córdoba, 9 de Noviembre de 2002

[4] *Carlos S. Chinea*, Artículo Sobre Ecuaciones Diofánticas Lineales, 2009

[5] *Burton W. Jones*, Teoría de los Números, Editorial Trillas, México,1969

[6] *Williams Le Veque*, Teoría Elemental de los Números, Herrero Hermanos, 1968

[7] *Goldfrey Harold Hardy; Edward Maitland Wright;* An Introduction to the Theory of Numbers, Oxford University Press, 2008