Academia Sabatina de Jóvenes Talento

Ecuaciones Diofánticas
Clase #7

Encuentro: 22 **Nivel:** 5
Curso: Ecuaciones Diofánticas **Semestre:** II
Fecha: x de octubre (prob) de 2024 **Instructor:** Kenny Jordan Tinoco
Instructor Aux: Gema Tapia

Contenido: Ecuaciones diofánticas lineales

En esta ocasión abordaremos el tema de ecuaciones Lineales el primero de la tercera unidad ecuaciones diofánticas clásicas. Primero recordaremos algunos hechos básicos y luego veremos un poco teoría de las ecuaciones lineales clásicas, los teoremas y técnicas más comunes, ejemplos y problemas.

1. Desarrollo

Antes de empezar recordemos lo siguiente.

Definición 1.1 (El máximo común divisor)**.** de dos enteros positivos a y b es el mayor entero positivo que divide a ambos y podemos denotarlo como $mcd(a,b)$ o simplemente como (a,b).

Definición 1.2 (El Algoritmo de la división)**.** tomando $a \geq b > 0$, $a = bq + r$, donde r es conocido como residuo y satisface $0 \leq r < b$.

Ahora, observemos que si $d \mid a$ y $d \mid b$ entonces $d \mid r$. De igual forma, si $d \mid r$ y $d \mid b$ entonces $d \mid a$. Esto implica que el conjunto de divisores comunes de a y b es igual al conjunto de divisores comunes de b y r. En particular $(a,b) = (b,r)$. Sean a y b dos enteros positivos tal que $(a,b) = 1$ entonces diremos que a y b son coprimos o primos entre sí.

Teorema 1.1. Sean $a, b, c \in \mathbb{Z}$ con $a, b \neq 0$ la ecuación $ax + by = c$ cumple lo siguiente.

1. La ecuación tiene solución si y sólo si $d = mcd(a,b)$ divide a c. Aún más, dicha ecuación es equivalente a otra donde los coeficientes son coprimos.

2. Si (x_0, y_0) es una solución particular, entonces todas las soluciones enteras son de la forma
$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t, \quad t \in \mathbb{Z}.$$

3. Si $c = mcd(a,b)$ y $|a|$ y $|b|$ es diferente de 1, entonces una solución particular (x_0, y_0) para la solución general. Puede ser encontrada tal que $|x_0| < |b|$ y $|y_0| < |a|$.

Ejemplo 1.1. ¿Tiene la ecuación $24x + 18y = 12$ soluciones enteras?

Solución. Por supuesto, ya que $(24, 18) = 6$ y $6 \mid 12$, por el teorema anterior podemos afirmar que sí tiene soluciones enteras. ■

En notación de congruencias, el problema de resolver una ecuación lineal de dos incógnitas equivale a resolver la congruencia:

$$ax \equiv c \ (\text{mód } b)$$

ya que si $ax \equiv c \ (\text{mód } b)$ entonces $ax - c = -by$. O sea $ax + by = c$.

Ejemplo 1.2. Resolver la ecuación $5x - 3y = 52$ en enteros positivos.

Solución. Primero, verificamos que la ecuación tiene soluciones enteras. Como 5 y 3 son coprimos o que $mcd(5, 3) = 1$ y $1 \mid 52$, entonces por el teorema anterior sí hay soluciones enteras. Ahora, buscamos un múltiplo de 3 que, cuando se sume a 52, dé un número divisible por 5. Esto es

$$52 + 3y \equiv 0 \ (\text{mód } 5) \implies 2 - 2y \equiv 0 \ (\text{mód } 5) \implies y \equiv 1 \ (\text{mód } 5)$$

Notamos que una solución a esta congruencia es, efectivamente, $y = 1$. Y que $52+3\cdot 1 = 55 = 5 \cdot 11$ es, en efecto, un múltiplo de 5. De donde es fácil ver que la ecuación tiene como solución para x a 11.

Ya con la solución $(x_0, y_0) = (11, 1)$ y con teorema anterior llegamos a que

$$(x, y) = (11 + 3t, 1 - 5t), \text{ donde } t \in \mathbb{Z}.$$ ■

Ejemplo 1.3. Resolver la siguiente ecuación $8c + 7p = 100$.

Solución. Análogamente al ejemplo anterior, verificamos que la ecuación tiene soluciones enteras. Como 8 y 7 son coprimos claramente sí hay soluciones enteras. Ahora, buscamos un múltiplo de 7 que, cuando se reste a 100, dé un número divisible por 8. Esto es

$$100 - 7p \equiv 0 \ (\text{mód } 8) \implies 4 + p \equiv 0 \ (\text{mód } 8) \implies p \equiv -4 \ (\text{mód } 8)$$

Y rápidamente, podemos decir que $p = -4$ es una solución para dicha congruencia. Al sustituirlo en la ecuación original obtenemos $c = 16$. Luego, con la solución $(x_0, y_0) = (16, -4)$ y con anterior llegamos a que

$$(c, p) = (16 + 7t, -4 - 8t), \text{ donde } t \in \mathbb{Z}.$$ ■

1.1. Aplicando el algoritmo de Euclides

Usando el algoritmo de euclides podemos resolver ecuaciones lineales de la siguiente forma. Dada la ecuación $ax + by = c$ y $d = mcd(a, b)$, entonces:

1. Obtener d, si $d \nmid c$, entonces no hay solución.

2. Si $d \mid c$, dividimos ambos términos de la ecuación por d.

3. Consideremos la ecuación $ax + by = c$, tal que $d = 1$. Podemos suponer esto en virtud del paso 2.

   a) Si $a \mid c$, existe c_0 tal que $ac_0 = c$. Luego, hay una solución $x = c_0, \quad y = 0$.

   b) Si $a \nmid c$ podemos suponer que $0 < |a| < |b|$, por el algoritmo de la división

$$\begin{aligned} b &= aq_1 + r_1, \quad 0 < r_1 < |a| \\ c &= aq_2 + r_2, \quad 0 < r_2 < |a| \end{aligned}$$

4. Si sustituimos estas igualdades en la ecuación original, entonces

$$\begin{aligned} ax + (aq_1 + r_1)y &= aq_2 + r_2, \\ a(x + q_1y - q_2) + r_1y &= r_2, \end{aligned}$$

   si tomando $z = x + q_1y - q_2$, entonces la ecuación anterior se transforma en $az + r_1y = r_2$.

   a) Si $r_1 \mid r_2$, caemos en 3.a.

   b) Si $r_1 \nmid r_2$ caemos en 3.b y continuamos el proceso.

Ejemplo 1.4. Resuelva la siguiente ecuación $350x + 425y = 1200$.

Solución. Como $(350, 425) = 25$ y $25 \mid 1200$, dividimos ambos lados de la ecuación por 25 y tenemos

$$14x + 17y = 48$$

Por el algoritmo de euclides se tiene que $17 = 1 \cdot 14 + 3$ y $48 = 3 \cdot 14 + 6$. Sustituyendo y agrupando, tenemos $14(x + y - 3) + 3y = 6$. Haciendo $z = x + y - 3$ y sustituyendo en esta última ecuación se tiene $14z + 3y = 6$. Como $3 \mid 6$, para esta ecuación tenemos una solución de la forma $z = 0$ y $y = 2$. Escribiendo z en términos de x y $y = 2$, obtenemos el valor de $x = 1$. Luego, la solución general de la ecuación inicial es:

$$x = 1 + 17k, \quad y = 2 - 14k, \quad k \in \mathbb{Z}. \qquad \blacksquare$$

Ejemplo 1.5. Resuelva la ecuación diofántica $125x - 25y = 28$.

Ejemplo 1.6. Resuelva la ecuación $69x + 123y = 3000$.

Comentario. Esta ecuación es un ejemplo perfecto en donde se utiliza la recursividad del método.

Hasta el momento sólo hemos trabajado en ecuaciones lineales de dos variables, pero en realidad la ecuación $ax + by = c$ no es más que un caso particular de la ecuación

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = c,$$

donde $a_1, a_2, \ldots, a_n$, y c son coeficientes.

Teorema 1.2. La ecuación $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ tiene solución si y sólo sí $mcd(a_1, a_2, \cdots, a_n) \mid c$.

Ejemplo 1.7. Resuelva la ecuación $3x + 4y + 5z = 6$

Solución. Primero garantizamos que $(3, 4, 5) = 1$ efectivamente divide a 6. Trabajando con módulo 5 tenemos que $3x + 4y \equiv 1 \pmod 5$, y de esto que $3x + 4y = 1 + 5s, \quad s \in \mathbb{Z}$. Una solución para esta ecuación es $x = -1 + 3s$, $y = 1 - s$. Usando el resultado anterior, obtenemos $x = -1 + 3s + 4t$, $y = 1 - s - 3t$, con $t \in \mathbb{Z}$, y sustituyendo en la ecuación original $z = 1 - s$. Por lo que todas las soluciones son

$$(x, y, z) = (-1 + 3s + 4t, 1 - s - 3t, 1 - s), \quad s, t \in \mathbb{Z}. \qquad \blacksquare$$

Definición 1.3. Sean $a_1, a_2, \ldots, a_n$ enteros positivos con $mcd(a_1, a_2, \ldots, a_n) = 1$ se define a $g(a_1, a_2, \ldots, a_n)$ como el mayor entero positivo N para el cual

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n = N,$$

no tiene soluciones enteras.

El problema de determinar $g(a_1, a_2, \ldots, a_n)$ es conocido como el problema de las monedas de Frobenius. Fue este quien planteó el problema de encontrar la mayor cantidad de dinero que no se puede pagar con monedas de $a_1, a_2, \ldots, a_n$ centavos. El ejemplo clásico de este problema es que con monedas de 3 y 5 centavos nunca se podrá llegar a la cantidad de 7 centavos.

Teorema 1.3 (Sylvester)**.** Sean $a, b \in \mathbb{Z}+, (a, b) = 1$, entonces $g(a, b) = ab - a - b$.

Para el caso de $n = 2$, existe el Teorema de Sylvester el cual nos brinda el valor de N (rápidamente podemos verificar el ejemplo anterior con 3 y 5), pero para $n \geq 2$ no se conoce ninguna fórmula explicíta, aunque sí se han encontrado rangos en donde N puede estar. Estos caso para $n \geq 2$ sobre pasan los objetivos de este escrito, se invita al lector investigar este tema por su cuenta.

Finalmente por el **Teorema 1.1** podemos entender de mejor manera el siguiente teorema.

Teorema 1.4 (Chicken McNugget)**.** Sean $a, b \in \mathbb{Z}+$; $(a, b) = 1$, entonces

1. $ax + by = n$ es insoluble $\forall x, y \in \mathbb{Z}^+$, si $n = ab - a - b$.
2. Si $n > ab - a - b$, entonces la ecuación es soluble.

Como recomendación general, se deja que siempre se verifique que una ecuación diofántica lineal de dos variables cumpla con el **Teorema 1.1** punto 2.

1.2. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

2. Problemas propuestos

Se asigna como **tarea** los problemas de esta sección, el estudiante debe entregar sus soluciones en la siguiente sesión de clase, en caso de no resolverlos se pueden entregar borradores. Recordar realizar un trabajo claro, ordenado y limpio.

3. Extra

Problemas para **puntos extras en la nota final** del curso, estos se califican distinto a los problemas propuestos.

Referencias

[BDMS98] Hugo Barrantes, Pedro Díaz, Manuel Murillo, and Alberto Soto. *Introducción a la Teoría de Números.* Universidad Estatal a Distancia. Costa Rica, 1998.

[Tin22] Kenny Tinoco. V Nivel. Ecuaciones diofánticas. Clase 10. Ecuaciones diofánticas clásicas. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Octubre 2022.

En caso de consultas

Instructor: Kenny J. Tinoco
Teléfono: +505 7836 3102 *(Tigo)*
Correo: kenny.tinoco10@gmail.com

Instructor: Gema Tapia
Teléfono: +505 8825 1565 *(Claro)*
Correo: gematapia97@gmail.com

4. Plan de clase

4.1. ¿Qué?

4.2. ¿Cómo?

4.3. Comentarios

Preguntas claves: ¿me entendieron? ¿me salté algún tema? ¿di tiempo suficiente para pensar los problemas? ¿participaron? ¿problemas muy fáciles o muy difíciles, demasiados o muy pocos? ¿las explicaciones/ejemplos fueron suficientes y buenos?