Ecuaciones Diofánticas

Ezra Guerrero Alvarez

1 de enero del 2023

1 Introducción

Las ecuaciones diofánticas son ecuaciones donde las variables involucradas son enteros. Esto puede hacer que preguntas que en los reales son extremadamente aburridas, se vuelvan interesantes al restringirnos solo a los enteros. Hay muchos tipos de Ecuaciones Diofánticas y estas aparecen por todas partes al lidiar con problemas de teoría de números.
A través de este folleto, denotamos por $m \perp n$ que los enteros m y n son coprimos.

2 Diofánticas Lineales

Primero, nos enfocamos en ecuaciones diofánticas de aspecto lineal. Cuando solo tenemos una variable, estas son aburridas, pues encontrar la solución es immediate. Veamos que sucede cuando tenemos dos variables.

Ejemplo 1

Encuentra una solución entera a la ecuación

$$3x + 7y = 89.$$

Solución. Un ejemplo es $(x, y) = (11, 8)$, pero hay muchos ejemplos que funcionan. ■

Ejemplo 2

Demuestra que

$$3x + 6y = 89$$

no tiene solución entera.

¿Cuál es la diferencia entre este problema y el anterior? La clave es que $\gcd(3, 6) = 3$, así que $3 \mid 3x + 6y$. Sin embargo, $3 \nmid 89$, así que es imposible que ambos lados sean iguales. ■

Esto ilustra como resolveremos ecuaciones de este tipo en general. Consideremos la ecuación

$$ax + by = c,$$

donde a, b, c son enteros fijos. Nos preguntamos cuando esta ecuación tiene soluciones enteras (x, y) y cuando las tiene, si podemos caracterizarlas todas. Con este fin, recordemos el Lema de Bezout:

Lema 1: Lema de Bezout

Sean a y b enteros. Su máximo común divisor, $\gcd(a, b)$ es el menor entero positivo del conjunto $\{ax + by \mid x, y \in \mathbb{Z}\}$.

Ejercicio 1. Demuestra este lema.

Lema 2: ¿Cuando tiene $ax + by = c$ soluciones?

La ecuación $ax + by = c$ tiene soluciones enteras si y solo si $\gcd(a, b) \mid c$. Si tiene soluciones, sea (x_0, y_0) una de ellas. Todas las soluciones tienen la forma $(x_0 + \frac{b}{\gcd(a,b)}t, y_0 - \frac{a}{\gcd(a,b)}t)$, donde t es un entero cualquiera.

Demostración. Primero, si $\gcd(a, b) \nmid c$, es claro que la ecuación no tiene solución. En caso contrario, sea $d = \gcd(a, b)$. Por el lema de Bezout, sabemos que existen enteros x', y' tales que $ax + by = d$. Entonces, si dejamos $(x, y) = (\frac{c}{d}x', \frac{c}{d}y')$, vemos que $ax + by = \frac{c}{d} \cdot d = c$ y la ecuación tiene solución.

Ahora, cuando hay soluciones, las caracterizamos todas. Sea (x_0, y_0) una solución cualquiera. Primero, veamos que $(x_0 + \frac{b}{\gcd(a,b)}t, y_0 - \frac{a}{\gcd(a,b)}t)$ es una solución:

$$a\left(x_0 + \frac{b}{\gcd(a,b)}t\right) + b\left(y_0 - \frac{a}{\gcd(a,b)}t\right) = ax_0 + \frac{ab}{\gcd(a,b)}t + by_0 - \frac{ab}{\gcd(a,b)}t = ax_0 + by_0 = c.$$

Procedemos a demostrar que todas las soluciones tienen esta forma. Sea (x, y) una solución. Sabemos que $ax + by = ax_0 + by_0 = c$, así que $a(x - x_0) = -b(y - y_0)$. Sea $a' = \frac{a}{\gcd(a,b)}$ y $b' = \frac{b}{\gcd(a,b)}$. Dividiendo entre $\gcd(a, b)$, vemos que $a'(x - x_0) = -b'(y - y_0)$. Por ende, $a' \mid -b'(y - y_0)$. Como $a' \perp b'$, esto implica que $a' \mid y_0 - y$, así que existe un entero t tal que $y_0 - y = a't$. Sustituyendo, esto implica que $x - x_0 = b't$, así que $(x, y) = (x_0 + b't, y_0 - a't)$ como queríamos demostrar. ■

Ejercicio 2. Encuentra las soluciones enteras para las siguientes ecuaciones: $3x + 4y = 0$, $2x + 7y = 3$, $21x + 36y = 6$.

Lema 3: Soluciones Pequeñas

Sean a y b enteros coprimos. Hay exactamente una solución (x, y) a la ecuación $ax + by = c$ tal que $0 \leq y < a$.

Ejercicio 3. Demuestra este lema reduciendo módulo a.

Ahora, notarán que varias de estas soluciones requieren que al menos uno de x, y sea negativo. ¿Qué pasa si restringimos a enteros no negativos?

Teorema 1: Teorema de Chicken McNugget

Sean a y b dos enteros positivos coprimos mayores a 1. El número más grande que no puede expresarse de la forma $ax + by$ con x, y enteros no negativos es $ab - a - b$ y hay $\frac{(a-1)(b-1)}{2}$ enteros positivos que no se pueden expresar de esta forma.

Demostración. Sabemos por el **Lema 2** que para todo entero positivo N existen enteros x, y tales que $ax + by = N$. Sea (x_0, y_0) la solución única con $0 \leq y_0 < a$, la cual sabemos existe por el **Lema 3**. Veremos que N se puede expresar de la forma $ax + by$ con x, y no negativos si y solo si $x_0 \geq 0$. Primero, si $x_0 \geq 0$, como $y_0 \geq 0$, entonces N se puede expresar de la forma deseada. Ahora, si $x_0 < 0$, sabemos que todas las soluciones tienen la forma $(x_0 + bt, y_0 - at)$. Si $t \leq 0$, entonces $x_0 + bt < 0$ y si $t > 0$ entonces $y_0 - at < 0$. Esto implica lo que deseábamos. Entonces, los enteros positivos que no se pueden expresar de la forma deseada tienen la forma $ax_0 + by_0$ con $x_0 < 0$ y $0 \leq y_0 < a$. El mayor de estos será cuando $x_0 = -1$ y $y_0 = a - 1$, es decir

$$a(-1) + b(a - 1) = ab - a - b.$$

Para contar cuantos hay, notamos que $ax_0 + by_0 > 0$, así que $x_0 > -\frac{b}{a}y_0$. Como $a \perp b$ y $y_0 < a$, sabemos que $\frac{b}{a}y_0$ nunca es un entero, dando que $x_0 \geq -\left\lfloor \frac{b}{a}y_0 \right\rfloor$. Entonces, para cada y_0, hay $\left\lfloor \frac{b}{a}y_0 \right\rfloor$ opciones para x_0. Entonces, en total hay

$$\sum_{y_0=0}^{a-1} \left\lfloor \frac{b}{a}y_0 \right\rfloor$$

enteros positivos que no pueden expresarse de la forma $ax + by$ con x, y no negativos. Se puede demostrar que esta suma es igual a $\frac{(a-1)(b-1)}{2}$, concluyendo la demostración. ■

3 Diofánticas No Lineales

A veces también nos toca lidear con ecuaciones en los enteros que no son ecuaciones lineales. Estas por lo general contienen nuestras variables en los exponentes, son polinomios de grado más alto, tienen factoriales o alguna combinación de las tres. Para todas, la clave es usar todas las herramientas de teoría de números que conocemos para llegar a un resultado.

Talvez el ejemplo más sencillo de una diofántica no lineal es cuando tenemos un producto igual a un entero.

Ejemplo 3

Encuentra todos los pares de enteros (a, b) tales que $(a + 1)(b - 3) = 10$.

Solución. La clave es que como $a + 1$ y $b - 3$ son enteros, deben ser factores de 10. Listando los factores de 10, tenemos las siguientes opciones:

$a+1$	$b-3$
-10	-1
-5	-2
-2	-5
-1	-10
1	10
2	5
5	2
10	1

Resolviendo para a y b en cada uno de estos casos, encontramos que las soluciones son $(-11, 2), (-6, 1), (-3, -2), (-2, -7), (0, 13), (1, 8), (4, 5)$ y $(9, 4)$. ■

Para poder resolver ecuaciones, a veces nos interesa llevarlas a esta forma, pues una vez lo hacemos terminar el problema se simplifica grandemente. Para esto, podemos usar un truco de factorización, conocido en inglés como SFFT (Simon's Favorite Factoring Trick).

Lema 4: Simon's Favorite Factoring Trick

Se cumple que $(xa + m)(yb + n) = xy \cdot ab + xn \cdot a + ym \cdot b + mn$. La forma más común en la que se ve esta factorización es cuando $x = y = 1$ y $m = n$, en cual caso

$$ab + n \cdot a + n \cdot b + n^2 = (a + n)(b + n).$$

Ejercicio 4. Demuestra esto.

Lo útil del truco es que podemos forzar la factorización cuando vemos expresiones del tipo $ab + n \cdot a + n \cdot b$. Veamos un ejemplo con un problema de la Olimpiada Hondureña de Matemáticas (OHM) del 2022.

Ejemplo 4 (OHM 2022 Nivel Básico P5)

Encuentre todos los números primos p, q, r tales que

$$pqr = 101(p + q + r).$$

Solución. Primero, como $101 \mid pqr$ y 101 es primo, sabemos que 101 divide a uno de p, q, r. Sin perdida de generalidad, supongamos que divide a r. Como r es un primo divisible entre 101, sigue que $r = 101$. Sustituyendo y simplificando, tenemos que $pq = p + q + 101$. Escribamos esto de forma que podramos reconocer SFFT:

$$pq - p - q = 101.$$

La expresión de la izquierda nos recuerda a la factorización, así que sumamos 1 a ambos lados para obtener

$$pq - p - q + 1 = 102.$$

Podemos factorizar ahora, obteniendo $(p - 1)(q - 1) = 102$ y con esto podemos terminar el problema. ■

Ejercicio 5. Termina el problema y encuentra todas las soluciones usando la factorización ya encontrada.

Finalmente, quiero terminar con un ejemplo de una diofántica que involucra exponentes:

Ejemplo 5

Encuentra todos los primos p tales que $5^p + 4p^4$ es un cuadrado perfecto.

Solución. Aunque inicialmente no suene como una ecuación diofántica, el problema nos pide encontrar todas las parejas de enteros (p, a) con p primo tal que $5^p + 4p^4 = a^2$. Restando $4p^4$ de ambos lados, reconocemos una diferencia de cuadrados, por lo cual

$$5^p = (a - 2p^2)(a + 2p^2).$$

Ahora, cada factor del lado derecho debe ser una potencia de 5, pues su producto es una potencia de 5. Por ende, existen enteros no negativos x, y tales que $a - 2p^2 = 5^x$ y $a + 2p^2 = 5^y$. Restando, encontramos que

$$4p^2 = 5^y - 5^x.$$

Primero, concluimos que $y > x$. Ahora, si $x > 0$, entonces 5 divide el lado derecho, por lo cual $5 \mid 4p^2$. Concluimos que $5 \mid p$, así que $p = 5$. Podemos revisar que $5^5 + 4 \cdot 5^4$ en efecto es un cuadrado perfecto, dando una solución. En caso contrario, $x = 0$ y como $x + y = p$, tenemos $y = p$. En este caso $4p^2 = 5^p - 1$. Reduciendo módulo p y usando el Pequeño Teorema de Fermat, vemos que

$$0 \equiv 4p^2 \equiv 5^p - 1 \equiv 5 - 1 \equiv 4 \pmod{p},$$

por lo cual $p \mid 4$. Concluimos que $p = 2$. Sin embargo, $5^2 + 4 \cdot 2^4$ no es un cuadrado perfecto, por lo cual esto no nos da una solución. Por ende, el único tal primo es $p = 5$. ■

4 Conclusión

Las ecuaciones diofánticas vienen en distintas formas y sabores. Poder atacarlas y resolverlas cuando aparecen es crucial para poder resolver diversos problemas. Es útil tener en mente las estrategias más frecuentes para lidiar con las diofánticas más comunes y reconociendo estos patrones se podrán resolver ecuaciones similares.