Academia Sabatina de Jóvenes Talento

Notas sobre Ecuaciones Diofánticas

Kenny J. Tinoco

Índice

1. Introducción a las Ecuaciones Diofánticas

La resolución de ecuaciones es un tema que se presenta en secundaria desde los primeros niveles. Paralelamente se van estudiando los diferentes conjuntos numéricos a saber: el conjunto de números Naturales ($\mathbb{N}$), el conjunto de números enteros ($\mathbb{Z}$), el conjunto de números racionales ($\mathbb{Q}$) y el conjunto de número Reales ($\mathbb{R}$).

Además, se repasan conceptos elementales de teoría de números como son: máximo común divisor, mínimo común múltiplo, números primos, etc. En este curso estudiaremos los métodos de resolución de un tipo especial de ecuaciones llamadas **Ecuaciones Diofánticas.**

1.1. Definiciones

Definición 1.1 (Ecuación Diofántica)**.** Se llama ecuación diofántica o ecuación diofantina a cualquier ecuación polinomial con coeficientes enteros cuya solución se restringe únicamente a aquellos valores enteros que la satisfacen.

Es decir, una expresión de la forma

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = b, \quad \text{con} \quad 1 \leq i \leq n,\ a_i, b \in \mathbb{Z}.$$

Donde la n-upla de números enteros $(r_1, r_2, \ldots, r_n)$ hace la igualdad. Es claro que una ecuación diofántica puede tener una o más n-upla que hagan la igualdad.

Definición 1.2. A una n-upla, con n entero, que satisface una ecuación diofántica, se le llama solución de la ecuación. Una ecuación diofántica con una o más soluciones se llama ecuación soluble, así también, una ecuación diofántica sin soluciones se llama ecuación insoluble o irresoluble.

Una ecuación diofántica se dice que tiene una familia de soluciones cuando un conjunto de estas, o todas, puede ser expresada en función de uno o más parámetros enteros. Como por ejemplo la ecuación $x^2 + 2y^2 = z^2$, vemos que tiene soluciones $(-2, 0, 2)$, $(-1, 2, 3)$, $(2, 4, 6)$, $\ldots$, las cuales podemos expresar como

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

donde r es un número entero sin ninguna restricción, por lo que la ecuación diofántica tiene infinitas soluciones de esta forma.

Ahora, nos centraremos en el conjunto de métodos elementales para la resolución de Ecuaciones Diofánticas, a lo largo del curso haremos uso de estos métodos, tales como factorización, identidades algebraicas, desigualdades, parametrización y congruencias.

2. Método de factorización

El método de factorización consiste transformar una expresión algebraica como producto de otras expresiones algebraicas, muchas veces de grado menor. Como trabajamos en números enteros esto nos permite asociar estas expresiones con los divisores de otros números enteros. Logrando así, obtener un conjunto de casos muchas veces más sencillos de resolver.

Es decir, si tenemos una expresión de la forma

$$(a_1x_1 + a_2x_2 + \cdots + a_nx_n)(b_1x_1 + b_2x_2 + \cdots + b_nx_n)\cdots(r_1x_1 + r_2x_2 + \cdots + r_nx_n) = k,$$

donde $1 \leq j \leq n$ tenemos $a_j, b_j, \ldots, r_j, k \in \mathbb{Z}$. Si $k_1, k_2, \ldots, k_m$ son los divisores de k, podemos asociar las expresiones del lado izquierdo con estos divisores, formando sistemas de ecuaciones como por ejemplo

$$\begin{cases} a_1x_1 + a_2x_2 + \cdots + a_nx_n = k_1 \\ b_1x_1 + b_2x_2 + \cdots + b_nx_n = k_2 \\ \qquad\qquad \vdots \\ r_1x_1 + r_2x_2 + \cdots + r_nx_n = k_p, \end{cases}$$

claramente, dependerá del problema como escoger estas asociaciones.

Ahora, algunas identidades algebraicas nos pueden simplificar la factorización, aquí exponemos una pequeña lista de las más comunes.

Identidades útiles

(Completación de rectángulo)	$xy + iy + jx + ij = (x + i)(y + j)$
(Diferencia de cuadrados)	$a^2 - b^2 = (a - b)(a + b)$
(Binomio al cuadrado)	$(a + b)^2 = a^2 + 2ab + b^2$
(Trinomio al cuadrado)	$(a + b + c)^2 = a^2 + b^2 + c^2 + 2(ab + bc + ca)$
(Identidad I)	$a^2 + b^2 + c^2 - ab - bc - ca = \frac{1}{2}\left[(a - b)^2 + (b - c)^2 + (c - a)^2\right]$
(Identidad de Gauss)	$a^3 + b^3 + c^3 - 3abc = (a + b + c)(a^2 + b^2 + c^2 - ab - bc - ca)$
(Identidad de Argand)	$a^4 + a^2 + 1 = (a^2 - a + 1)(a^2 + a + 1)$
(Identidad de Sophie Germain)	$a^4 + 4b^4 = (a^2 - 2ab + 2b^2)\left(a^2 + 2ab + 2b^2\right)$
(Identidad de Brahmagupta)	$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$
(Diferencia de potencias)	$a^n - b^n = (a - b)(a^{n-1} + a^{n-2}b + \cdots + b^{n-1})$
(Suma de potencias)	$a^n + b^n = (a + b)(a^{n-1} - a^{n-2}b + \cdots + b^{n-1})$ para n impar

(Binomio de Newton) $$(a+b)^n = a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{k}a^{n-k}b^k + \cdots + b^n$$

A continuación, tenemos una serie de ejercicios con los cuales podemos prácticar y aplicar el método de factorización.

2.1. Ejercicios y problemas

Ejercicio 1. Hallar la cantidad de parejas de enteros positivos x_1, x_2 tales que $x_1 \cdot x_2 = 25 \cdot 15^3$.

Ejercicio 2. Probar que la ecuación $x^2 + 2y^2 = z^2$ tiene como solución a $x = a^2 - 2b^2$, $y = 2ab$ y $z = a^2 + 2b^2$ donde $a, b \in \mathbb{Z}$.

Ejercicio 3. Hallar todos los números naturales x, y para los cuales $\dfrac{5}{x} + \dfrac{6}{y} = 1$.

Ejercicio 4. Probar que la ecuación $x^3 = 2y^3$ no tiene soluciones enteras.

Ejercicio 5. Resolver $y^2 = x^3 - x$ sobre los enteros.

Ejercicio 6. Hallar los enteros positivos x, y, z tal que $3^x + 4^y = z^2$.

Ejercicio 7. Encuentre todos los enteros positivos x, y tales que $xy - x + y = 49$.

Ejercicio 8. Encuentre todas las soluciones enteras de la ecuación

$$(x^2+1)(y^2+1) + 2(x-y)(1-xy) = 4(1+xy).$$

Ejercicio 9. Encuentre todos los enteros positivos n tales que, $n^4 + 4^n$ es primo.

Ejercicio 10. ¿Para qué valores de a y b se da la igualdad $a^2 - 4ab = -4b^2 + 9$?

Ejercicio 11. Resuelve la siguiente ecuación en enteros $x^2 + 6xy + 8y^2 + 3x + 6y = 2$.

Ejercicio 12. Para cada entero n sea $s(n)$ el número de pares ordenados (x, y) de enteros positivos para los cuales

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{n}.$$

Encuentre todos los números enteros positivos n para los cuales $s(n) = 5$.

Ejercicio 13. Hallar todas las soluciones enteras de la ecuación $x^3 + y^3 - 3xy = 3$.

Ejercicio 14. Hallar todas las soluciones enteras de $x^2(y-1) + y^2(x-1) = 1$.

Ejercicio 15. Sean p y q números primos distintos. Encuentre el número de pares de enteros positivos x, y que satisfacen la ecuación

$$\frac{p}{x} + \frac{q}{y} = 1.$$

Problema 2.1. Encuentre todos los pares de enteros (x, y) tales que $x^6+3x^3+1 = y^4$.

Problema 2.2. Encuentre todos los pares (x, y) de enteros tales que $xy + \dfrac{x^3 + y^3}{3} = 2007$.

Ejercicio 16. Probar que las triplas $\left(\frac{p+1}{3}, \frac{p+1}{3}, \frac{p-2}{3}\right)$ y $\left(\frac{p+2}{3}, \frac{p-1}{3}, \frac{p-1}{3}\right)$ son solución de la ecuación

$$(x^2 - yz)^3 + (y^2 - zx)^3 + (z^2 - xy)^3 - 3(x^2 - yz)(y^2 - zx)(z^2 - xy) = p^2.$$

Ejercicio 17. Determinar todos los enteros positivos que son solución de la ecuación

$$(xy - 7)^2 = x^2 + y^2.$$

Problema 2.3. Halla todas las triplas (x, y, z) de enteros positivos, con p primo talque

$$x^5 + x^4 + 1 = p^y.$$

3. Métodos de desigualdades

Una de las estrategias de resolución es utilizar las desigualdades. La idea principal es reducir la cantidad de casos mediante el uso de las inecuaciones.

Antes de iniciar el estudio de este método, recordemos algunas propiedades de las desigualdades numéricas. Los axiomas elementales sobre desigualdades son los siguientes

1. Dado un número real x, se tiene que $x > 0$, $x = 0$ o $x < 0$.
2. Si $a > 0$ y $b > 0$, entonces $a + b > 0$ y $ab > 0$.
3. Si $a > b$, entonces $a + c > b + c$.

Todas las demás desigualdades se derivan de estos axiomas. Como por ejemplo

1. Si $a > b$ y $c < 0$, entonces $ac < bc$.
2. Si $0 < a < 1$, entonces $a^2 < a$.
3. Si $|a| > 1$, entonces $a^2 > a$.

Cuando se tiene una desigualdad de una variable, los pasos comunes son perecidos a los de resolver una ecuación líneal. Como por ejemplo,

1. Remover denominadores.
2. Remover paréntesis y corchetes.
3. Mover términos para combinarlos.
4. Mover términos semejantes.
5. Normalizar coeficientes.

Ejemplo 3.1. Dado que $2(x-2)-3(4x-1)=9(1-x)$ y $y<x+9$, comparar las cantidades $\dfrac{y}{\pi}$ y $\dfrac{10}{31}y$.

Ahora, vemos los siguientes teoremas.

Teorema 3.1. Si x es un número real, entonces $x^2 \geq 0$. La igualdad se da si y solo si $x=0$.

Teorema 3.2 (Desigualdad Media Aritmética - Geometríca)**.** Dado n números reales positivos x_1, x_2, ..., x_n se tiene que

$$\frac{x_1+x_2+\cdots+x_n}{n} \geq \sqrt[n]{x_1x_2\cdots x_n}.$$

Donde la igualdad se da cuando $x_1=x_2=\cdots=x_n$.

Teorema 3.3 (Desigualdad Cauchy-Schwartz)**.** Dado los reales positivos $a_1, a_2, \ldots, a_n$ y $b_1, b_2, \ldots, b_n$ se tiene que

$$(a_1^2+a_2^2+\cdots+a_n^2)(b_1^2+b_2^2+\cdots+b_n^2) \geq (a_1b_1+a_2b_2+\cdots+a_nb_n)^2.$$

Donde la igualdad se da si $b_i=ka_i$ para todo $a_i \neq 0$ con $i=1,2,\ldots,n$

Finalmente, se proponen unos ejercicios para prácticar estas técnicas.

3.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 18. Sabiendo que $ac<0$, argumentar cuántas de las siguiente desiguadades pueden ser verdaderas.

$$\frac{a}{c}<0, \quad ac^2<0, \quad a^2c<0, \quad c^3a<0, \quad ca^3<0.$$

Ejercicio 19. Hay cuatro afirmaciones como se indica a continuación:

(i) Cuando $0<x<1$, entonces $\dfrac{1}{1+x}<1-x+x^2$;

(ii) Cuando $0<x<1$, entonces $\dfrac{1}{1+x}>1-x+x^2$;

(iii) Cuando $-1<x<0$, entonces $\dfrac{1}{1+x}<1-x+x^2$;

(iv) Cuando $-1<x<0$, entonces $\dfrac{1}{1+x}>1-x+x^2$.

Dar como respuesta las afirmaciones correctas.

Ejercicio 20. Dado los números reales a, b. Si $a = \dfrac{x+3}{4}$, $b = \dfrac{2x+1}{3}$ y $b < \dfrac{7}{3} < 2a$, hallar el rango de valores para x.

Ejercicio 21. Dado que $a < b < c < 0$ ordenar de manera descendiente los números $\dfrac{a}{b+c}$, $\dfrac{b}{c+a}$ y $\dfrac{c}{a+b}$.

Ejercicio 22. Probar que para reales no negativos x, y, z se cumple que

$$a^2 + b^2 + c^2 \geq ab + bc + ca.$$

Ejercicio 23. Sean a, b, c reales no negativos, probar que

$$(a+b)(b+c)(c+a) \geq 8abc.$$

Ejercicio 24. Sean $a, b, c > 0$ probar que

$$\frac{a^3}{bc} + \frac{b^3}{ca} + \frac{c^3}{ab} \geq a + b + c.$$

Ejercicio 25. Sean a, b, c reales positivos tales que $abc = 1$. Probar que

$$a^2 + b^2 + c^2 \geq a + b + c.$$

Ejercicio 26. Hallar todas las duplas positivas (x, y) tal que $x^3 - y^3 = xy + 61$.

Ejercicio 27. Resolver la siguiente ecuación en los enteros positivos x, y, z

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} = \frac{3}{5}.$$

Ejercicio 28. Hallar todas las soluciones enteras (x, y) de $x^3 + y^3 = (x+y)^2$.

Ejercicio 29. Determinar todos los números enteros positivos (x, y, z) que sean solución de

$$\left(1 + \frac{1}{x}\right)\left(1 + \frac{1}{y}\right)\left(1 + \frac{1}{z}\right) = 2.$$

Ejercicio 30. Hallar todas las soluciones en enteros de la ecuación

$$x^3 + (x+1)^3 + (x+2)^3 + \cdots + (x+7)^2 = y^3.$$

Ejercicio 31. Determinar todos los números enteros positivos (x, y, z) que sean solución de

$$xy + yz + zx - xyz = 2$$

Ejercicio 32. Halle todas las soluciones (w, x, y, z) de enteros positivos tales que

$$x^2 + y^2 + z^2 + 2xy + 2x(z-1) + 2y(z+1) = w^2$$

Ejercicio 33. Determinar todos los números enteros positivos (x, y, z) que sean solución de

$$(x+y)^2 + 3x + y + 1 = z^2$$

Ejercicio 34. Determine todas las parejas de enteros (x, y) tales que

$$1 + 2^x + 2^{2x+1} = y^2.$$

Problema 3.1. Encuentra todos los pares de números positivos (a, b) tales que $ab^2 + b + 7$ divide a $a^2b + a + b$.

Ejercicio 35. Si a, b, c son positivos y se sabe que

$$\frac{c}{a+b} < \frac{a}{b+c} < \frac{b}{a+c},$$

escribir los números a, b, c en orden descendiente.

Ejercicio 36. Resolver la siguiente ecuación en enteros positivos

$$3(xy + yz + zx) = 4xyz.$$

Problema 3.2. Resolver en enteros distintos la ecuación

$$x^2 + y^2 + z^2 + w^2 = 3(x + y + z + w).$$

4. Método de parametrización

En muchas situaciones, las soluciones enteras a una ecuación diofántica pueden ser expresadas de forma paramétrica, dónde dichos parámetros son variables enteras.

El conjunto de soluciones de algunas ecuaciones diofánticas podría tener múltiples representaciones paramétricas. Para la mayoría de ecuaciones diofánticas, no es posible encontrar todas las soluciones explícitamente. En muchos casos, el método paramétrico proporciona una prueba de la existencia de infinitas soluciones.

Ejemplo 4.1. Hallar todas las soluciones enteras (m, n) que satisfacen la ecuación

$$12m - 5n = 97 - mn.$$

Solución. Transformando la ecuación convenientemente

$$\begin{aligned} 12m + mn = 97 + 5n &\iff m(12 + n) = 97 + 5n \\ &\iff m = \frac{97 + 5n}{12 + n} \iff m = 5 + \frac{37}{n + 12}. \end{aligned}$$

Consideremos la variable $t = \frac{37}{n+12}$ con lo cual $m = t + 5$, como m es entero necesariamente t también lo es. Es fácil ver $n = \frac{37}{t} - 12$, ya que n es entero, entonces t debe ser divisor de 37. Con esta información, es claro que los posibles valores son $t \in \{\pm 1, \pm 37\}$. Finalmente, las soluciones de la ecuación están dadas por $(m, n) \in \{(4, -49), (6, 25), (-32, -13), (42, -11)\}$. ■

Como vimos en el ejemplo anterior, la idea es expresar las variables m y n en términos de un parámetro t, reduciendo el problema a solo encontrar los posibles valores de t, y puesto de que estamos trabajando en enteros y que hay ciertas condiciones con respecto a esta variable, la pudimos acotar fácilmente.

4.0.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 37. Encuentra las soluciones de la siguiente ecuación diofántica

$$2(x+y) = xy + 9.$$

Ejercicio 38. Demostrar que la ecuación $x^2 + y^2 - z^2 - x + 3y - z - 4 = 0$ posee infinitas soluciones en los números enteros.

Ejercicio 39. Determinar los números enteros x que verifican que $x^4 + 2$ es múltiplo de $x + 2$.

Ejercicio 40. Dado tres números enteros positivos x, y, z hallar el valor de su producto sabiendo que cumplen

$$x + 2y = z \quad \text{y} \quad x^2 - 4y^2 + z^2 = 310.$$

Ejercicio 41. Encontrar todas las soluciones enteras (x, y) de la ecuación

$$p(x+y) = xy,$$

donde p es un número primo.

Ejercicio 42. Hallar todas las triplas (x, y, z) de enteros positivos tales que

$$\frac{1}{x} + \frac{1}{y} = \frac{1}{z}.$$

Ejercicio 43. Probar que existen infinitas triplas (x, y, z) de enteros tales que

$$x^3 + y^3 + z^3 = x^2 + y^2 + z^2.$$

Problema 4.1. Probar que si a, b, c son enteros positivos tales que $\frac{1}{a} + \frac{1}{b} = \frac{1}{c}$, entonces

- $a + b$ es un cuadrado perfecto.
- $a^2 + b^2 + c^2$ es un cuadrado perfecto.

5. Método de Congruencia

La congruencia en enteros es una poderosa herramienta en la solución de ecuaciones diofánticas, usualmente aplicaremos este método para probar que ciertas ecuaciones son insolubles o bien deducir condiciones que las soluciones deben cumplir. Ahora, vemos algunas definiciones.

Definición 5.1 (Divisibilidad)**.** Si a y b son enteros, se dice que a divide a b o que b es múltiplo de a si $b = aq$ para algún entero q, y se denota por $a \mid b$.

Definición 5.2 (Congruencias)**.** Dados dos enteros a, b y un entero positivo m, decimos que a es congruente con b módulo m si $(a - b)$ es múltiplo de m. En este caso escribimos $a \equiv b \pmod{m}$.

Es decir, tenemos $a \equiv b \pmod{m} \iff m \mid (a - b)$. Con esto, podemos deducir y demostrar el siguiente teorema.

Teorema 5.1 (Propiedades de Congrencias)**.** Sean los enteros a, b, c, d y $m \geq 1$.

1. Si $a \equiv c \pmod{m}$ y $c \equiv d \pmod{m}$, entonces $a \equiv d \pmod{m}$.
2. Si $a \equiv c \pmod{m}$ y $b \equiv d \pmod{m}$, entonces $ab \equiv cd \pmod{m}$.
3. Si $a \equiv c \pmod{m}$, entonces $a^n \equiv c^n \pmod{m}$ para todo entero positivo n.
4. Si $ab \equiv bc \pmod{m}$, entonces $a \equiv c \pmod{\frac{m}{d}}$ donde $d = mcd(b, m)$.

Ejemplo 5.1. Hallar el resto cuando 6^{1987} es dividido por 37.

Solución. Como $6^2 = 36 = 37 - 1$ es claro que $6^2 \equiv -1 \pmod{37}$. Asi al considerar $6^{1987} = 6 \cdot 6^{1986} = 6 \cdot (6^2)^{993}$ tenemos que $6^{1987} \equiv 6(-1)^{993} \equiv -6 \equiv 31 \pmod{37}$. Por lo cual, el resto de la división de 6^{1987} por 37 es 31. ■

Definición 5.3 (Función phi de Euler)**.** Para cualquier entero n se denota a $\varphi(n)$ como cantidad de números de coprimos menores a n.

Teorema 5.2 (Teorema de Euler)**.** Si a y n son dos enteros positivos primos relativos entre si, entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Teorema 5.3 (Pequeño teorema de Fermat)**.** Si p es primo y a es un entero primo relativo con p, entonces $a^{p-1} \equiv 1 \pmod{p}$.

Es claro que el teorema de Fermat es un caso concreto del teorema de Euler, de la propia definición de números primos se deduce que un primo p tiene exactamente $(p - 1)$ primos relativos, luego el resultado es evidente.

De estas definiciones y teoremas se obtienen ciertos restos especiales, conocidos como restos potenciales respecto a un módulo, quizás los más famosos serían los restos cuadráticos, veamos algunos de ellos.

$x^2 \equiv 0, 1 \pmod{3}$	$x^2 \equiv 0, 1, 4 \pmod{8}$	$x^3 \equiv 0, \pm 1 \pmod{7}$
$x^2 \equiv 0, 1 \pmod{4}$	$x^2 \equiv 0, 1, 4, 9 \pmod{16}$	$x^4 \equiv 0, 1 \pmod{16}$
$x^2 \equiv 0, \pm 1 \pmod{5}$	$x^3 \equiv 0, \pm 1 \pmod{9}$	$x^5 \equiv 0, \pm 1 \pmod{11}$

Estos restos pueden ser probados fácilmente, algunos son resultados inmediatos de teoremas como Fermat o Euler, asi mismo, se puede considerar el conjunto de residuos

de cada módulo y luego investigar el comportamiento de las potencias. Veamos un ejemplo.

Ejemplo 5.2. Probar que para todo entero x se tiene $x^2 \equiv 0, 1 \pmod 4$.

Solución. Cuando $x = 2x_1$, entonces $x^2 = 4x_1^2 \equiv 0 \pmod 4$. Ahora, es claro que $\varphi(4) = 2$, aplicando Euler tenemos $x^2 \equiv 1 \pmod 4$. ■

Se deja como ejercicio al lector probar los demás restos potenciales.

Ejemplo 5.3. Hallar todos los enteros x, y tal que $15x^2 - 7y^2 = 9$.

Solución 1. Analizando la ecuación en módulo 3 tenemos que $-7y^2 \equiv 0 \pmod 3$, es claro que y es múltiplo de 3, es decir $y = 3y_1$. Por tanto,

$$15x^2 - 7(9y_1^2) = 9 \iff 5x^2 - 7(3y_1^2) = 3$$

donde en módulo 3 obtenemos que x también es múltiplo 3, es decir $x = 3x_1$. Esto es,

$$5(9x_1^2) - 7(3y_1^2) = 3 \iff 5(3x_1^2) - 7y_1^2 = 1 \iff 15x_1^2 - 7y_1^2 = 1.$$

Al analizar la última ecuación en módulo 3 obtenemos que $y_1^2 \equiv -1 \pmod 3$, lo cual no es resto cuadrático en módulo 3. Luego, la ecuación no tiene soluciones. ■

Solución 2. Analizando en módulo 5 tenemos que $-7y^2 \equiv 1 \pmod 5$ por lo cual[1] $y^2 \equiv 3 \pmod 5$, este resto no es posible en módulo 5. Luego, la ecuación no tiene soluciones enteras. ■

5.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 44. Hallar los restos cuadráticos en módulo 13.

Ejercicio 45. Hallar los enteros positivos a, b tales que $a^2 - 3b^2 = 8$.

Ejercicio 46. ¿Existen enteros positivos x, y tal que $x^3 = 2^y + 15$?

Ejercicio 47. Probar que la ecuación $x^2 + 3xy - 2y^2 = 122$ no tiene soluciones enteras

Ejercicio 48. Demostrar que la ecuación $x^2 - 7y = 3$ no tiene soluciones enteras.

Ejercicio 49. Demostrar que no hay enteros para los cuales $800000007 = x^2 + y^2 + z^2$.

Ejercicio 50. Hallar las soluciones enteras de la ecuación $x^2 - 5y^2 = 2$.

Ejercicio 51. Hallar las soluciones de enteros positivos tal que $a^3 + 2b^3 + 4c^3 = 9d^3$.

[1] ¿Podés justificar el porqué?

Ejercicio 52. Probar que la ecuación $x^3+3y^3+9z^3-9xyz=0$ solo tiene la solución entera $(x,y,z)=(0,0,0)$.

Ejercicio 53. Probar que las ecuaciones

1. $6x^3+3=y^6$
2. $x^3+y^3+4=z^3$

no tiene soluciones para enteros positivos x,y,z.

Ejercicio 54. Encontrar todas las soluciones (p,q) de números primos tales que

$$p^3-q^5=(p+q)^2.$$

Ejercicio 55. Demostrar que 7 divide a $3^{2n+1}+2^{n+2}$ para todo natural n.

Ejercicio 56. Hallar un número infinito de enteros n tal que $7 \mid 2^n+27$.

Ejercicio 57. Si $r_k=8^k+6^k$, hallar el resto de la división de a_{83} entre 49.

Problema 5.1. Probar que la ecuación $(x+1)^2+(x+2)^2+\cdots+(x+99)^2=y^z$ no tiene soluciones enteras (x,y,z) con $z>1$.

Problema 5.2. Determinar todos los primos p para los cuales el sistema de ecuaciones

$$\begin{cases} p+1=2x^2 \\ p^2+1=2y^2 \end{cases}$$

tiene soluciones enteras (x,y).

Problema 5.3. Probar que la ecuación $x^5-y^2=4$ es insoluble en los enteros.

Problema 5.4. Si n es un entero positivo tal que la ecuación $x^3-3xy^2+y^3=n$ tiene tres soluciones enteras (x,y). Probar que la ecuación es insoluble cuando $n=2891$.

Problema 5.5. Determinar las posibles soluciones enteras no negativas $(x_1,x_2,\ldots,x_{14})$ de la ecuación $x_1^4+x_2^4+\cdots+x_{14}^4=15999$.

Ejercicio 58. Probar que para todo entero x se tiene $x^5\equiv 0,\pm 1 \pmod{11}$.

Problema 5.6. Si se cumple que $n\equiv 4 \pmod 9$, probar que la ecuación

$$x^3+y^3+z^3=n$$

no tiene soluciones enteras.

Problema 5.7. Probar que la ecuación

$$(a+2023)^2+(a+2022)^2+\cdots+(a+1)^2=b^2$$

no es soluble en enteros a,b.

Problema 5.8. Hallar los pares (a,b) de enteros positivos tales que satisfacen la ecuación $a^{b^2}=b^a$.

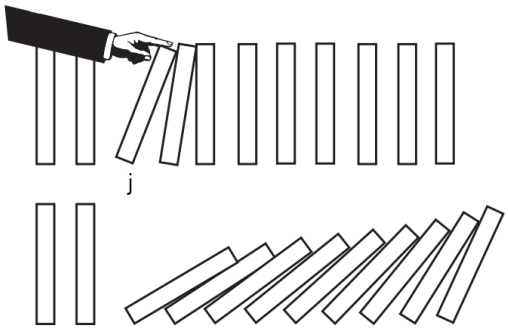

Figura 1: Fichas de dominó cayendo.

6. Inducción matemática

Inducción matemática es una técnica utilizada para probar declaraciones o proposiciones. La idea es similar a la de hacer caer varias piezas de dominó. Si cada pieza está lo suficientemente cerca de la anterior y hacemos caer la primera, entonces todas las piezas eventualmente van a caer. Cuando queremos demostrar que una proposición se cumple sobre números naturales, la idea es la misma. Dicho de otro modo, la inducción nos permite demostrar una propiedad en **infinitos números** con **pasos finitos**.

Principio 6.1 (Inducción simple)**.** Sea el entero j y $S(n)$ una proposición sobre el entero n con $n \geq j$,

i) si $S(j)$ es cierto, y

ii) para cada entero $k \geq j$, $S(k) \implies S(k+1)$,

entonces $S(n)$ es cierta para todo $n \geq j$.

Asi por ejemplo, si tenemos $j = 1$ y una proposición $T(n)$ cumple las dos condiciones anteriores, entonces $T(n)$ se cumple para todo natural n, lo más común en la mayoría de los problemas es demostrar una propiedad a partir de $j = 1$ o $j = 0$.

Es importante mencionar el vocabulario utilizado en la inducción matemática, el cual nos permite moldear una solución.

1. **Paso base:** Identificar y validar el primer entero que cumple, $S(j)$ cierto.
2. **Hipótesis de inducción:** Formular y tomar la proposición como cierta para un entero dado, $S(k)$ cierto.
3. **Tesis de inducción:** Identificar la proposición a validar, $S(k+1)$ cierto.
4. **Paso inductivo:** Demostrar por medio de argumentos que la hipótesis implica a la tesis, $S(k) \implies S(k+1)$.

Hay varias maneras de interpretar la hipótesis y la tesis, por ejemplo

- lo que sabemos y lo que buscamos,

- lo que tenemos y lo que debemos,
- entradas (input) y salidas (output),

entre otros, de cualquier modo todos siguen el objetivo de transformar la hipótesis en argumentos para demostrar la tesis.

Hay situaciones donde demostrar que una propiedad $S(n+1)$ es verdadera no basta con solo tomar a $S(n)$ como cierto, puesto que estas proposiciones a menudo dependen de la validez de más de un elemento anterior, dicho de otro modo, necesitamos más información para demostrar la propiedad, para ello utilizamos la inducción fuerte.

Principio 6.2 (Inducción fuerte)**.** Sea j un entero y $S(n)$ una proposición sobre el entero $n \geq j$. Si

$$\forall k \geq j, \quad (\forall m < k,\ S(m)) \implies S(k),$$

entonces $S(n)$ es cierta para todo $n \geq j$.

La expresión $(\forall m < k,\ S(m)) \implies S(k)$ con $k \geq j$, es equivalente a la expresión

$$(S(j) \wedge S(j+1) \wedge \cdots \wedge S(k-1)) \implies S(k).$$

Cuando $k = j$ de manera lógica obtenemos $S(j)$ cierto, lo cual es equivalente al paso base de la inducción simple, por lo tanto, no es difícil notar que la inducción fuerte es el caso general de la inducción simple.

Veamos un ejemplo, que ilustra estos principios.

Ejemplo 6.1. Hallar el $n_0 \in \mathbb{Z}^{\geq 0}$ tal que cualquier entero $n \geq n_0$ cumple $n = 3i + 5j$ para algunos $i, j \in \mathbb{Z}^{\geq 0}$.

Solución. Haciendo unas algunas pruebas, encontramos que

$0 = 3 \cdot 0 + 5 \cdot 0$	$5 = 3 \cdot 0 + 5 \cdot 1$	$10 = 3 \cdot 0 + 5 \cdot 2$
1 no cumple	$6 = 3 \cdot 2 + 5 \cdot 0$	$11 = 3 \cdot 2 + 5 \cdot 1$
2 no cumple	7 no cumple	$12 = 3 \cdot 4 + 5 \cdot 0$
$3 = 3 \cdot 1 + 5 \cdot 0$	$8 = 3 \cdot 1 + 5 \cdot 1$	$13 = 3 \cdot 1 + 5 \cdot 2$
4 no cumple	$9 = 3 \cdot 3 + 5 \cdot 0$	etc ...

Es decir, a partir de $n_0 = 8$ notamos que los enteros siguientes empiezan a cumplir la propiedad **(paso base)**. Sea la proposición $S(n)$: "existen $i, j \in \mathbb{Z}^{\geq 0}$ tales que $n = 3i + 5j$" y supongamos que para un entero $k \geq 8$, $S(8), S(9), \ldots, S(k)$ son todos ciertos **(hipótesis de inducción)**, entonces vamos a demostrar que $S(k+1)$ también es cierto **(tesis de inducción)**. Se distinguen dos casos,

- $k = 8, 9, 10$, los cuales sabemos son ciertos y
- $k \geq 11$, de donde obtenemos que $8 \leq k - 3 \leq k$.

Por la hipótesis sabemos que existen $i_0, j_0 \in \mathbb{Z}^{\geq 0}$ tales que $k - 3 = 3i_0 + 5j_0$, por lo tanto $k = 3(i_0 + 1) + 5j_0$ donde $i = i_0 + 1$ y $j = j_0$ **(paso inductivo)**. Luego, $S(n)$ se cumple para todo entero $n \geq 8$. ■

6.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 59. Hallar el $n_0 \in \mathbb{Z}^{\geq 0}$ tal que $\forall n \geq n_0,\ n = 5i + 6j$ con $i, j \in \mathbb{Z}^{\geq 0}$.

Ejercicio 60. Probar para todo $n \in \mathbb{N}$ que el número $A_n = 3^n - 2n^2 - 1$ es múltiplo de 8. Además, si $3 \nmid n$, entonces A_n es múltiplo de 24.

Problema 6.1. Probar $\forall n \in \mathbb{N}$ que las ecuaciones tienen soluciones enteras

$$1)\ x^2 + y^2 = z^n, \qquad 2)\ (x^2 + y^2)(u^2 + v^2 + w^2) = 2009^n.$$

Problema 6.2. Resolver $x_1^2 + x_2^2 + \cdots + x_{2002}^2 = 1335\,(x_1 + x_2 + \cdots + x_{2002})$ en enteros positivos distintos

7. Descenso infinito de Fermat

Sigamos con otro principio, uno bastante intuitivo.

Principio 7.1 (Buen orden)**.** Para todo subconjunto no vacío de los naturales, este debe tener un elemento mínimo.

De igual manera, es fácil pensar que un subconjunto no vacío de los números naturales debe tener un elemento máximo, por consiguiente, cualquier subconjunto no vacío de los naturales debe tener un elemento mínimo y máximo.

Al trata de problemas en específicos, a menudo utilizamos estas nociones del principio de Buen orden, lo cual podemos formalizar con el siguiente axioma.

Axioma 7.1 (Axioma del Orden)**.** Si M es un conjunto de n números reales distintos, entonces podemos escribirlo como $M = \{x_1, x_2, \ldots, x_n\}$ con $x_1 < x_2 < \ldots < x_n$.

Las demostraciones por el principio del buen orden a menudo implica realizar una prueba por contradicción, en este texto no abordaremos a detalle este principio, pero se invita a investigar más de este tema. Esta noción de orden será de útilidad con el siguiente y último principio.

El descenso infinito proviene de resolver ecuaciones diofánticas indeterminadas, el matemático Pierre de Fermat (1601-1665) utilizó este método hace unos 400 años cuando demostró que no existen soluciones enteras positivas para[2] $x^4 + y^4 = z^4$.

Principio 7.2 (Descenso infinito de Fermat)**.** Sea $k \in \mathbb{Z}^{\geq 0}$ y $S(n)$ una proposición sobre n,

i) si $S(k)$ no es cierto, y

ii) para todo $m > k$, $S(m) \implies S(r)$ con $m > r > k$,

entonces $S(n)$ no se cumple para ningún $n \geq k$.

[2]Se recomienda al lector buscar la solución de Fermat, para enrriquecer su lectura.

Podemos entender el descenso infinito de fermat metafóricamente con una escalera, si para alcanzar un escalón más alto es necesario pasar primero uno más bajo, pero no existe un escalón más bajo en la escalera, entonces es imposible subir a ningún escalón.

Veamos dos variantes o casos concretos de este principio, útiles en el estudio de las ecuaciones diofánticas.

i) No existe una secuencia $n_1 > n_2 > n_3 > \dots$ estrictamente decreciente de enteros no negativos.

ii) Si se tiene la secuencia $n_1 \geq n_2 \geq n_3 \geq \dots$ de enteros no negativos, entonces existe un $k \geq 1$ tal que $n_k = n_{k+1} = n_{k+2} = \cdots$.

Cabe destacar que los principios de Inducción matemática, Buen orden y Descenso infinito son de hecho equivalentes en el conjunto de los enteros no negativos. Con lo cual, si tomamos uno es posible demostrar con este los dos restantes[3].

Ejemplo 7.1. Probar que la ecuación $x^2 + y^2 = 3z^2$ no tiene soluciones (x, y, z) en enteros positivos cuando $z \neq 0$.

Solución. Supongamos que hay al menos una solución (x_1, y_1, z_1) con $z_1 > 0$, es claro que en módulo 3 llegamos a $x_1^2 + y_1^2 \equiv 0 \pmod 3$. Como los cuadrados perfectos solo dejan resto 0 o 1 en módulo tres, necesariamente $x_1^2 \equiv y_1^2 \equiv 0 \pmod 3$, por lo cual $x_1 = 3x_2$, $y_1 = 3y_2$ con $x_1 > x_2$ y $y_1 > y_2$.

Al reemplazar en la ecuación $9x_2^2 + 9y_2^2 = 3z_1^2 \iff 3(x_2^2 + y_2^2) = z_1^2 \iff 3 \mid z_1^2 \iff 3 \mid z_1$. Si tomamos $z_1 = 3z_2$ con $z_1 > z_2$, entonces

$$x_2^2 + y_2^2 = 3z_2^2.$$

Es decir, hemos encontrado una nueva solución (x_2, y_2, z_2) a la ecuación original. Al analizar esta solución, obtendríamos otra nueva solución (x_3, y_3, z_3), de la misma manera, aplicando este proceso obtendríamos soluciones (x_4, y_4, z_4), (x_5, y_5, z_5), (x_6, y_6, z_6) y así sucesivamente. Sin embargo, esto implica que

$$x_1 > x_2 > x_3 > \cdots, \quad y_1 > y_2 > y_3 > \cdots \quad \text{y} \quad z_1 > z_2 > z_3 > \cdots.$$

Lo cual es imposible, luego la ecuación original no tiene soluciones. ■

7.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 61. Encuentre todas las soluciones enteras de la ecuación $a^2 - 2b^2 = 0$.

Ejercicio 62. Hallar todos los números enteros a, b, c tales que $a^2 = 2b^2 + 3c^2$.

[3]Se recomienda al lector investigar cómo son esas demostraciones

Ejercicio 63. Probar que $x^2+y^2=3(m^2+n^2)$ no tiene soluciones enteras positivas.

Ejercicio 64. Hallar las soluciones $(a,b)\in\mathbb{Z}^{\geq 0}$ para $a^2+b^2+c^2=a^2b^2$.

Ejercicio 65. Resolver en enteros de la ecuación $2005x^3=y^3+25z^3$.

Ejercicio 66. Muestre que no hay enteros positivos x,y,z tal que $x^2+10y^2=z^2$.

Problema 7.1. ¿Hay soluciones racionales para $x^2+y^2+z^2+3(x+y+z)+5=0$?

Problema 7.2. Hallar las triplas $(x,y,z)\in\mathbb{N}$ que cumplen $x^3+3y^3+9z^3-3xyz=0$.

Problema 7.3. Hallar todos los enteros x,y,z para los cuales $x^2+y^2+z^2-2xyz=0$.

Problema 7.4. Resolver en enteros positivos la ecuación $m^2-mn-n^2=\pm 1$.

Ejercicio 67. Hallar el mínimo, máximo y orden, de los siguientes conjuntos.

1. $A=\{4,7,6,3,78,10,5,1,6\}$.
2. Los divisores de 121.
3. Múltiplos de 3 entre 20 y 80.
4. Los primos impares menores a 50.
5. Los primos entre 50 y 100.
6. Cubos perfectos menores de 200

Ejercicio 68. Hallar las soluciones enteras no negativas (x,y,z) tal que $x^3+2y^3=4z^3$.

Problema 7.5. Probar que $\forall n\in\mathbb{N}$, la ecuación $x^2+xy+y^2=7^n$ tiene soluciones enteras.

Problema 7.6. Todo entero $n\geq 2$ es producto de un número finito de primos (resolver por inducción y por buen orden).

Problema 7.7. Resolver en enteros positivos la ecuación

$$x^2+y^2+x+y+1=xyz.$$

8. Ecuaciones diofánticas lineales

Antes de empezar recordemos los siguientes resultados.

Definición 8.1 (Máximo divisor común)**.** Dados $a,b\in\mathbb{Z}^{\neq 0}$, el máximo $d\in\mathbb{Z}^{+}$ tal que $d\mid a$ y $d\mid b$ es el máximo divisor común, y lo denotamos por $d=\text{mcd}(a,b)$.

Definición 8.2. Si $a,b\in\mathbb{Z}^{\neq 0}$ con $\text{mcd}(a,b)=1$, entonces diremos que a y b son coprimos, primos relativos o primos entre sí.

Definición 8.3 (Combinación lineal)**.** Dados los enteros $a_1,a_2,\ldots,a_k$, definimos una combinación lineal de los números $\{a_i\}$ como un número de la forma

$$a_1x_1+a_2x_2+\ldots+a_kx_k,$$

donde los $\{x_i\}$ son enteros cualesquiera.

Teorema 8.1 (Algoritmo de la división)**.** Si $a, b \in \mathbb{Z}$ con $b \neq 0$, entonces existen enteros únicos (q, r) tales que $a = bq + r$ con $0 \leq r < |b|$.

El siguiente resultado es un teorema muy conocido e importante en la teoría de números, con él damos inicio al estudio de las ecuaciones diofánticas lineales, este resultado es utilizado tanto para la demostración de teoremas como la resolución de problemas.

Teorema 8.2 (Bezout)**.** Si $d = \text{mcd}(a, b)$, entonces d es el menor entero tal que

$$ax + by = d, \text{ con } x, y \in \mathbb{Z}.$$

Teorema 8.3. La ecuación diofántica $ax + by = c$ tendrá soluciones si y solo si $\text{mcd}(a, b) \mid c$. Además, si (x_0, y_0) es una solución particular, entonces la solución general es

$$(x, y) = \left(x_0 + \frac{b}{d}t,\ y_0 - \frac{a}{d}t\right) \quad \text{con } t \in \mathbb{Z}.$$

Ejemplos.

Ejemplo 8.1. Resolver la ecuación $5x - 3y = 52$ en enteros positivos.

Solución. Primero, como $\text{mcd}(5, 3) = 1$ y $1 \mid 52$, entonces la ecuación tiene soluciones enteras. Ahora, analizando en módulo 5 tenemos que

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

Claramente, $y = 1$ es solución a esta congruencia, sustituyendo en la ecuación original $5x - 3 \cdot 1 = 52 \iff 5x = 55$ por lo cual, la ecuación tiene una solución $(11, 1)$, luego con la solución $(x_0, y_0) = (11, 1)$ llegamos a

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

Ejemplo 8.2. Resolver la siguiente ecuación $8c + 7p = 100$.

Solución. Claramente, la ecuación tiene soluciones enteras, analizando en módulo 8,

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

Rápidamente, podemos decir que $p = 4$ es una solución para dicha congruencia, sustituyendo en la ecuación obtenemos $c = 9$. Luego, con la solución $(c_0, p_0) = (9, 4)$ tenemos

$$(c, p) = (9 + 7t, 4 - 8t), \quad \text{con } t \in \mathbb{Z}. \qquad \blacksquare$$

8.1. Aplicando el algoritmo de Euclides

Definición 8.4 (Algoritmo de Euclides)**.** Si $a, b \in \mathbb{Z}^{\neq 0}$ y $a = bq + r$ para algunos enteros q, r con $0 < r < b$, entonces

$$\text{mcd}(a, b) = \text{mcd}(b, r).$$

Podemos usar este algoritmo para resolver ecuaciones lineales de una manera iterativa, similar, a la manera en cómo se calcula el MCD de dos números grandes.

Sean $a, b, c \in \mathbb{Z}$ con $a, b \neq 0$ y $d = \text{mcd}(a, b)$, considerando la ecuación

$$ax + by = c,$$

se tienen los siguientes pasos:

1. Si $d \nmid c$, entonces no hay solución.
2. Si $d \mid c$, entonces se divide la ecuación por d obteniendo $a_1x + b_1y = c_1$.
3. Por el paso anterior la ecuación tiene coeficiente coprimos;
   3.1. Si $a_1 \mid c_1$, entonces $a_1c_0 = c_1$, luego $(x, y) = (c_0, 0)$ es solución.
   3.2. Si $a_1 \nmid c_1$, entonces tomamos el menor de $|a_1|, |b_1|$ y obtenemos[4]
   $$b_1 = a_1q_1 + r_1, \text{ con } 0 < r_1 < |a|, \quad c_1 = a_1q_2 + r_2, \text{ con } 0 < r_2 < |a|.$$
4. Sustituimos en la ecuación
   $$a_1x + (a_1q_1 + r_1)y = a_1q_2 + r_2 \iff a_1(x + q_1y - q_2) + r_1y = r_2.$$
   Haciendo $z = x + q_1y - q_2$, la ecuación anterior se transforma en $a_1z + r_1y = r_2$.
   4.1. Si $r_1 \mid r_2$, entonces terminamos con el paso 3.1.
   4.2. Si $r_1 \nmid r_2$, entonces vamos al paso 3.2 y repetimos el proceso.

Con estos pasos (o algoritmo) es posible resolver ecuaciones diofánticas lineales de coeficientes grandes, de una manera cíclica o iterativa, lo cual se reduce la complejidad. Veamos un ejemplo.

Ejemplo 8.3. Resuelva la siguiente ecuación $350x + 425y = 1200$.

Solución. Como $\text{mcd}(350, 425) = 25$ 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:

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

[4] Aquí vamos a suponer que $|a_1|$ es el menor.

8.2. Caso general de ecuaciones lineales

Hasta el momento solamente hemos trabajado en ecuaciones lineales de dos variables, pero en realidad la ecuación $ax + by = c$ es un caso concreto 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. También, cabe mencionar que el teorema de bezout se cumple para una cantidad n de números, con lo cual se podrá hacer un tratamiento similar al caso de $n = 2$.

Teorema 8.4. La ecuación diofántica $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ tiene solución si y solo si $\text{mcd}(a_1, a_2, \cdots, a_n) \mid c$.

Veamos un ejemplo.

Ejemplo 8.4. Resuelva la ecuación $3x + 4y + 5z = 6$.

Solución. Primero, notamos que $\text{mcd}(3, 4, 5) = 1$ efectivamente divide a 6. Trabajando en módulo 5 tenemos que $3x + 4y \equiv 1 \pmod 5$ por lo cual $3x + 4y = 1 + 5s$, con $s \in \mathbb{Z}$. Si tomamos a s como una constante, una solución para esta ecuación es $(x_0, y_0) = (-1 + 3s, 1 - s)$. Usando el teorema 8.3, obtenemos las soluciones generales de esta ecuación de dos variables

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

Sustituyendo esto en la ecuación original obtenemos $z = 1 - s$, por lo que todas las soluciones son

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

Como vemos en este ejemplo, una ecuación de tres variables la podemos reducir a una ecuación de dos variables, ecuación que sabemos cómo solucionarla, luego solo debemos revertir el proceso y dejar las soluciones en función de los parámetros que aparezcan. Análogamente, podemos resolver una ecuación de grado n reduciéndola sucesivamente a una de grado dos y realizar un proceso similar.

8.3. Existencia de soluciones

Para concluir, veremos algunos resultados que estudian la existencia de soluciones para una ecuación diofántica, estos resultados ya son parte de una teoría de mayor complejidad, si se tiene curiosidad se invita al lector a investigar más a fondo.

Definición 8.5. Sean $a_1, a_2, \ldots, a_n$ enteros positivos con $\text{mcd}(a_1, a_2, \ldots, a_n) = 1$ 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 $g(a_1, \ldots, a_n)$ es conocido como el problema de las monedas de Frobenius. Este problema fue planteado por Ferdinand Frobenius, quien se interesó en encontrar la mayor cantidad de dinero que no se puede representar como una combinación lineal de n denominaciones de monedas, quizás el ejemplo más sencillo es con monedas de 3 y 5 centavos con las cuales nunca se podrá pagar una deuda de 7 centavos. El siguiente teorema brinda un valor de N para el caso de $n = 2$.

Teorema 8.5 (Sylvester)**.** Sean $a, b \in \mathbb{Z}^+$, con $\text{mcd}(a, b) = 1$, entonces

$$g(a, b) = ab - a - b.$$

Con esto se puede analizar la ecuación $3x + 5y = 7$, como $g(3, 5) = 3 \cdot 5 - 3 - 5 = 7$ entonces se tiene que 7 es el mayor entero para el cual no hay soluciones. Para los casos de $n \geq 2$ hasta la fecha no se conoce ninguna fórmula explícita de g, cabe aclarar que estos temas ya son de una complejidad mayor a este curso. Finalmente, con el teorema sylvester podemos entender mejor el siguiente resultado.

Teorema 8.6 (Chicken McNugget)**.** Sean[a] $a, b \in \mathbb{Z}^+$ con $\text{mcd}(a, b) = 1$, se tiene:

i. Si $n = ab - a - b$, entonces $ax + by = n$ es insoluble $\forall x, y \in \mathbb{Z}^+$.

ii. Si $n > ab - a - b$, entonces la ecuación es soluble.

[a] Su historia es curiosa, debido a que fue enunciado en un McDonald's.

Como recomendación general, se aconseja siempre verificar que una ecuación cumpla con el segundo punto del teorema anterior.

8.4. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 69. Resolver las siguientes ecuaciones:

1. $30x - 25y = 15$
2. $2x - 3y = 5$
3. $91a - 195b = 1079$
4. $35m - 25n = 3$
5. $24x + 18y = 12$
6. $125x - 25y = 28$
7. $69x + 123y = 3000$
8. $12p + 501q = 1$
9. $97s + 98t = 1000$

Ejercicio 70. Resuelva las siguientes ecuaciones:

1. $3x + 10y + 8z = 34$
2. $5a + 20b + 5c = 13$
3. $6x + 10y + 15z = 37$
4. $m + p - q = 6$
5. $4r - 32s + 12t = 8$
6. $10x + 2y - 3z = 7$

Problema 8.1. Suponga que Fabiana gasta 40 pesos en una pulpería. Si esta paga con un billete de 100, ¿cómo puede recibir el vuelto en billetes de 10 y 25 pesos?

Problema 8.2. En el correo solo se tienen sellos de 14 y 21 céntimos. ¿De qué manera puede formar con un valor de 7.77 euros?

Problema 8.3. Queremos echar 21 litros de gasolina a un depósito. Para ello, tenemos dos bidones, de 2 y 5 litros respectivamente. Responder a las siguientes cuestiones:

1. ¿Es posible medir 21 litros con nuestros bidones? ¿Por qué?
2. En caso afirmativo, dar todas las combinaciones posibles.
3. Si suponemos que en nuestro depósito caben exactamente 22 litros, ¿cómo podemos echar 21 litros sin desbordar el depósito y sin retirar gasolina de él?

Problema 8.4. Brisa Marina le paga 143 pesos por la compra de mangos y naranjas a Gerald. Si paga 15 pesos por cada mango y 17 pesos por cada naranja, ¿cuántos mangos y naranjas le compró a Gerald?

Problema 8.5. Determinar los enteros positivos n tales que la ecuación $x+2y+z=n$ tiene exactamente 100 soluciones (x,y,z) en enteros no negativos.

9. Tripla pitagóricas

Probablemente conozca la ecuación $x^2+y^2=z^2$ por el teorema de Pitágoras, el cual describe la relación entre los lados x,y,z con respecto al ángulo recto. Si los lados son todos enteros positivos, estos forman una **tripla pitagórica** o **terna pitagórica**. Por ejemplo, $(x,y,z)=(3,4,5)$ es una terna pitagórica, asi como $(5,12,13)$ es también una terna pitagórica. También, cuando un triángulo rectángulo tiene longitudes enteras, lo llamaremos un triángulo pitagórico.

Lema 9.1. Sean x,y,z una terna pitagórica y $d=\text{mcd}(x,y,z)$. Entonces,

i) Se tiene $d=\text{mcd}(x,y)=\text{mcd}(y,z)=\text{mcd}(z,x)$.

ii) Si escribimos $x=dx_1$, $y=dy_1$ y $z=dz_1$, entonces x_1,y_1,z_1 es también una terna pitagórica.

Definición 9.1 (Terna pitagórica primitiva)**.** Se dice que una terna pitagórica es primitiva si $\text{mcd}(x,y,z)=1$ o equivalentemente cualquiera de los $\text{mcd}(x,y)$, $\text{mcd}(y,z)$ o $\text{mcd}(z,x)$ es 1.

Lema 9.2. Sea x,y,z una terna pitagórica primitiva, entonces, entre x,y,z hay exactamente un número par, que bien puede ser x o y.

Teorema 9.1. Sea x,y,z una terna pitagórica primitiva de enteros positivos, con y par. Entonces, existen enteros coprimos no negativos m,n con $m>n$ talque

$$x=m^2-n^2, \quad y=2mn, \quad z=m^2+n^2.$$

La mayoría de los problemas que implican ternas pitagóricas se reducen a utilizar las ternas ya conocidas o bien, demostrar que una ecuación no tiene soluciones porque

x	y	z	m	n
3	4	5	2	1
5	12	13	3	2
15	8	17	4	1
7	24	25	4	3
21	20	29	5	2
9	40	41	5	4
35	12	37	6	1
11	60	61	6	5
45	28	53	7	2
33	56	65	7	4

Cuadro 1: Las primeras ternas pitagóricas primitivas.

su forma es de una ecuación de Fermat, luego veremos algunos teoremas sobre este aspecto. Por lo cual es importante conocer algunas ternas pitagóricas, en el cuadro 1 se muestran las primeras diez ternas pitagóricas con lo cual se invita al lector tenerlas presente.

Lema 9.3. No existen dos enteros positivos tal que la suma y la diferencia de sus cuadrados también son cuadrados.

Demostración. El lema es equivalente a demostrar que el sistema de ecuaciones

$$\begin{cases} x^2 + y^2 = z^2 \\ x^2 - y^2 = w^2 \end{cases}$$

es insoluble en los enteros positivos. Asumamos por absurdo que dicho sistema tiene soluciones en los enteros positivos y consideremos el par (x, y) tal que $(x^2 + y^2)$ es mínimo, luego, es fácil ver que $\text{mcd}(x, y) = 1$. Sumando las dos ecuaciones obtenemos que $2x^2 = z^2 + w^2$ por lo cual z y w tienen la misma paridad. De aquí obtenemos que $(z + w)$ y $(z - w)$ son ambos pares, con esto podemos escribir

$$2x^2 = z^2 + w^2 \implies x^2 = \left(\frac{z+w}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2$$

la ecuación pitagórica de la derecha cumple con $\text{mcd}(x, \frac{z+w}{2}, \frac{z-w}{2}) = 1$, en caso contrario, es decir $\text{mcd}(x, \frac{z+w}{2}, \frac{z-w}{2}) = d \geq 2$ tendríamos que $d \mid x$ y $d \mid \frac{z+w}{2} + \frac{z-w}{2} = z$ que por el sistema original obtenemos $d \mid y$ lo cual contradice que $\text{mcd}(x, y) = 1$. Por tanto, existen enteros positivos m, n tales que

$$\frac{z+w}{2} = m^2 - n^2, \quad \frac{z-w}{2} = 2mn,$$

o bien

$$\frac{z+w}{2} = 2mn, \quad \frac{z-w}{2} = m^2 - n^2.$$

Puesto que $2y^2 = z^2 - w^2$, en cualquiera de los dos casos anteriores tenemos que $2y^2 = 2(m^2 - n^2) \cdot 4mn$ y por tanto $y^2 = 4mn(m^2 - n^2)$. De esto obtenemos que $y = 2k$, luego $k^2 = mn(m+n)(m-n)$. Ya que m, n son primos relativos $(m+n)$ es impar, así los enteros $m, n, (m+n), (m-n)$ son todos primos relativos dos a dos. Por lo cual, necesariamente $m = a^2, n = b^2, (m+n) = c^2, (m-n) = d^2$. Pero de aquí que $a^2 + b^2 = c^2$ y $a^2 - b^2 = d^2$ es decir (a, b, c, d) también es solución al sistema original, sin embargo

$$a^2 + b^2 = m + n < 4mn(m^2 - n^2) = y^2 < x^2 + y^2,$$

lo cual contradice que $x^2 + y^2$ sea mínimo. ■

La ecuación de Fermat o el último teorema de Fermat fue propuesta por el matemático francés Pierre de Fermat. En matemáticas, es un teorema famoso por su dificultad y el proceso de demostración de este teorema ha llevado a muchos descubrimientos importantes tanto en álgebra como en análisis.

Mientras estudiaba la obra del antiguo matemático griego Diofánto, Fermat escribió en el margen de su copia de un libro de Diofánto:

> "La ecuación a $a^n + b^n = c^n$ no tiene raíces enteras positivas para $n \geq 3$. He descubierto una prueba verdaderamente hermosa pero este margen es demasiado pequeño para contenerla."

Durante más de 350 años, muchos matemáticos intentaron demostrar la afirmación de Fermat o refutarla encontrando algún contraejemplo. En junio de 1993, Andrew Wiles, un matemático inglés de la Universidad de Princeton, afirmó que había demostrado el teorema. El 25 de octubre del siguiente año, Wiles envió una prueba revisada a tres colegas, después de que sus colegas la juzgaran completa, Wiles publicó su prueba.

Los siguientes teoremas son ecuaciones de la forma del teorema de Fermat.

Teorema 9.2. La ecuación $x^4 + y^4 = z^2$ no tiene soluciones enteras positivas.

Teorema 9.3. La ecuación $x^4 - y^4 = z^2$ no tiene soluciones enteras positivas.

Teorema 9.4. La ecuación $x^4 + y^2 = z^2$ no tiene soluciones enteras positivas.

Teorema 9.5. La ecuación $x^4 - 4y^2 = z^2$ no tiene soluciones enteras positivas.

Teorema 9.6. La ecuación $x^4 + 4y^2 = z^2$ no tiene soluciones enteras positivas.

Ejemplo 9.1. Hallar los números $x \in \mathbb{Z}$ tales que $81 = (2x - x^2)(x^2 - 2x + 2)$.

Solución. Operando sobre la expresión, se obtiene.

$$\begin{aligned}
(2x - x^2)(x^2 - 2x + 2) &= 81 \\
-(x^2 - 2x)(x^2 - 2x + 2) &= 9^2 \\
-(x^2 - 2x + 1 - 1)(x^2 - 2x + 1 + 1) &= 3^4 \\
-\left[(x-1)^2 - 1\right]\left[(x-1)^2 + 1\right] &= 3^4
\end{aligned}$$

$$1-(x-1)^4=3^4$$
$$3^4+(x-1)^4=1^2$$

Dicha expresión no puede tener soluciones enteras positivas, ya que esta tiene la forma del teorema 2.1, por lo cual no existe un entero x tal que se cumpla la ecuación. ■

9.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 71. Resolver las siguientes ecuaciones sobre los números naturales

1. $15y^4-z^2-2y^2z+1=0$
2. $x^4+y^4-x^2y^2-z^2-2xyz=0$
3. $x^4y^4-2x^2y^2+1=x^4+y^4$
4. $x^8+y^8-3x^4y^4=625$
5. $y^4=168x^4+338x^3y+y^2$

Ejercicio 72. Resolver las siguientes ecuaciones sobre los números naturales

1. $2x^4+2x^2+1=z^4$
2. $-14x^2+y^4=49$
3. $3x^4+y^4-102x^2+2061=0$
4. $3x^4-4x^2+1=y^4$
5. $x^4+4x^3+297x^2+4x+1=y^4$

Problema 9.1. Demostrar que el radio de la circunferencia inscrita en un triángulo pitagórico de lados enteros es siempre un número natural.

Problema 9.2. Demostrar que el área de un triángulo pitagórico no puede ser un cuadrado perfecto.

Problema 9.3. Hallar todas las soluciones en enteros positivos para el sistema de ecuaciones

$$\begin{cases} a^2+b^2=c^2 \\ b^2+c^2=d^2. \end{cases}$$

Problema 9.4. Probar que la ecuación $p=x^2+y^2$ para un primo p de la forma $p=4k+1$ con k entero, tiene una y solamente una solución en los enteros sin tomar en cuenta las permutaciones de x,y. (Pista: Usar ternas pitagóricas y luego descenso infinito)

Problema 9.5. Sea ΔABC un triángulo no equilátero con lados de longitudes enteras. Sea D y E los puntos medios de BC y CA, respectivamente, y sea G el baricentro de ΔABC. Suponga que D,C,E,G son cíclicos. Hallar el menos perimetro posible de ΔABC.

Problema 9.6. Hallar todos los $x,y\in\mathbb{N}$ tales que $x^2+y^2=2017(x-y)$.

Problema 9.7. Resolver la ecuación diofántica $x^{-2}+y^{-2}=z^{-2}$.

10. Ecuaciones de Pell

Hasta el momento solo hemos abordado ecuaciones cuadráticas, o grado par, por medio de las ternas pitagóricas y las ecuaciones de Fermat. Sin embargo, existe tipos de ecuaciones diofánticas cuadráticas muy especiales, conocidas como las ecuaciones de Pell.

Definición 10.1 (Ecuación de Pell)**.** Una ecuación diofántica de la forma

$$x^2 - dy^2 = 1, \text{ con } x, y \in \mathbb{Z},$$

donde $d \in \mathbb{N}$ no es cuadrado perfecto, es conocida como la ecuación de Pell.

¿Por qué decimos que d no es un cuadrado perfecto? Porque si esto fuera así, se formaría una diferencia de cuadrados, lo cual puede resolverse fácilmente asignado divisores a cada factor. De esta definición obtenemos.

Definición 10.2 (Ecuación de tipo Pell)**.** Una ecuación de la forma $x^2 - dy^2 = a$ para un entero a usualmente la llamaremos como ecuación del Pell.

De manera general, cualquier ecuación diofántica de dos variables puede reducirse a una ecuación del tipo Pell. Por lo cual esta ecuación diofántica resulta muy útil, con esto dicho la pregunta que surge es ¿cómo se resuelve una ecuación del tipo Pell? Resulta que estas ecuaciones tiene un tipo de solución muy sencillas de comprender, ya que a partir de una solución concreta pueden generarse una infinidad de soluciones. Similar a lo que ocurre con las soluciones de las ecuaciones diofánticas lineales. No obstante, la demostración de esto requiere conocer otros resultados en teoría de números, este escrito no abordará estos aspectos, sin embargo, se invita al lector investigarlo por su cuenta.

Definición 10.3. El conjugado del número $z = x+y\sqrt{d}$ es definido por $\overline{z} = x-y\sqrt{d}$, y su módulo está dado por $N(z) = z\overline{z} = x^2 - dy^2 \in \mathbb{Z}$.

Teorema 10.1. Para la ecuación de Pell $x^2 - dy^2 = 1$ si (x_1, y_1) es la solución más pequeña, y se tiene una solución (x_k, y_k), entonces

$$x_k + dy_k = (x_1 + dy_1)^r, \quad \text{para algún } r \in \mathbb{Z}^+.$$

Teorema 10.2. La ecuación de Pell $x^2 - dy^2 = 1$ tiene infinitas soluciones enteras no negativas y si (x_1, y_1) es la solución más pequeña, la solución general está dada por

$$x_n = \frac{(x_1 + y_1 d)^n + (x_1 - y_1 d)^n}{2}, \quad y_n = \frac{(x_1 + y_1 d)^n - (x_1 - y_1 d)^n}{2\sqrt{d}}$$

con n un natural.

Para la ecuación $x^2 - dy^2 = -1$, la situación es similar. Si (x_1, y_1) es la solución minima, entonces la solución (x_n, y_n) tiene la misma forma del teorema anterior para

n impar.

¿Qué podemos decir del conjunto de soluciones para la ecuación $x^2 - dy^2 = a$ con $a \neq 1$? A diferencia de la ecuación de Pell, la ecuación $x^2 - dy^2 = a$ no necesariamente tiene soluciones. Sin embargo, si esta tiene una solución minima, entonces tiene una infinidad de soluciones.

Teorema 10.3. La ecuación de tipo Pell $x^2 - dy^2 = a$ si tiene a (x_1, y_1) como la solución más pequeña, entonces tiene una cantidad infinita de soluciones.

En las siguientes clases abordaremos un método que nos permite encontrar las soluciones de una ecuación de Pell. Esta herramienta es conocida como fracciones continuas, se invita al lector investigar este tema.

10.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 73. Verificar que si (x_1, y_1) es la solución mínima de la ecuación de Pell $x^2 - dy^2 = 1$, entonces

$$x_n = \frac{(x_1 + y_1 d)^n + (x_1 - y_1 d)^n}{2}, \quad y_n = \frac{(x_1 + y_1 d)^n - (x_1 - y_1 d)^n}{2\sqrt{d}}$$

Ejercicio 74. Hallar todas las soluciones enteras positivas de la ecuación $x^2 - 2y^2 = 1$.

Ejercicio 75. Demostrar que la ecuación $x^2 - dy^2 = -1$ no tienes soluciones cuando $d \equiv 3 \pmod 4$.

Problema 10.1. Resolver en enteros la ecuación $x^2 + y^2 - 1 = 4xy$.

Problema 10.2. Demostrar que la ecuación $x^2 - dy^2 = -1$ no tiene solución si d es divisible por un primo de la forma $4k + 3$.

Problema 10.3. Hallar todas las soluciones x, y para la ecuación $x^2 - 3y^2 = 6$.

Problema 10.4. Hallar todas las soluciones x, y para la ecuación $x^2 - 7y^2 = 2$.

Problema 10.5. Hallar todas las soluciones x, y para la ecuación $x^2 - 7y^2 = 1$.

Problema 10.6. Demostrar que si la diferencia de dos cubos consecutivos es n^2 con $n \in \mathbb{N}$, entonces $2n - 1$ es también un cuadrado.

11. Problemas

Ejercicio 76. Resolver la ecuación diofántica $2^x + 1 = y^2$.

Ejercicio 77. Hallar todas las soluciones enteras de la ecuación

$$xy + 3x - 5y = -3.$$

Ejercicio 78. Probar que la ecuación $m^2 = n^4 + n^2 + 1$ no tiene soluciones enteras.

Ejercicio 79. Encuentra números positivos de dos cifras que sean iguales a tres veces el producto de los mismos.

Ejercicio 80. Hallar todas las soluciones enteras de la ecuación

$$x(x+1)(x+7)(x+8) = y^2.$$

Ejercicio 81. Hallar las soluciones enteras de la ecuación $13x - 7y = 0$, si las variables cumplen que $80 < x + y < 120$.

Ejercicio 82. Probar que existe infinitos pares ordenas de enteros positivos (m, n) tal que

$$\frac{m+1}{n} + \frac{n+1}{m}$$

es un entero positivo.

Ejercicio 83. Hallar los números enteros positivos x que verifican que $x^5 - 23$ es múltiplo de $x + 1$.

Ejercicio 84. Hallar todos los pares ordenados (x, y) tales que $xy = 20 - 3x + y$.

Problema 11.1. Sea p un número primo, determinar todos los números enteros k tales que $\sqrt{k^2 - kp}$ es un número natural.

Referencias

[Arr09] Enrique Arrondo. Apuntes de teoría elemental de números. *Universidad Complutense de Madrid*, Enero 2009.

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

[Gun10] David Gunderson. *Handbook of Mathematical Induction. Theory and Applications.* CRS Press, 2010.

[Lar21a] Ricardo Largaespada. Ecuaciones diofánticas. Clase 3. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Octubre 2021.

[Lar21b] Ricardo Largaespada. Ecuaciones diofánticas. Clase 4. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Abril 2021.

[Lar21c] Ricardo Largaespada. Ecuaciones diofánticas. Clase 5. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Abril 2021.

[LM24] Ricardo Largaespada and Darwing Mena. Nivel Centro. Unidad IV. Ecuaciones diofánticas. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Septiembre 2024.

[Ort17] Antonio Ortega. Estudio y discusión sobre problemas de olimpiáda. Ecuaciones diofánticas. *Universidad de Granada. España*, 2017.

[RH23a] René Rodríguez and Thomas Hernández. Ecuaciones diofánticas. Clase 1. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Julio 2023.

[RH23b] René Rodríguez and Thomas Hernández. Ecuaciones diofánticas. Clase 2. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Agosto 2023.

[Som85] I. Sominski. *Método de Inducción Matemática.* Editorial MIR, 1985.

[Tin22a] Kenny Tinoco. Ecuaciones diofánticas. Clase 6. Método de congruencias de números enteros. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Septiembre 2022.

[Tin22b] Kenny Tinoco. V Nivel. Ecuaciones diofánticas. Clase 10. Ecuaciones diofánticas clásicas. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Octubre 2022.

[Tin22c] Kenny Tinoco. V Nivel. Ecuaciones diofánticas. Clase 7. Método de Inducción matemática. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Octubre 2022.

[Tin22d] Kenny Tinoco. V Nivel. Ecuaciones diofánticas. Clase 9. Método de Descenso infinito de Fermat. *Academia Sabatina de Jóvenes Talento. Nicaragua*, Octubre 2022.