Ecuaciones Diofantinas I

Ecuación de Legendre

Nicolle Escobar

Universidad del Valle de Guatemala

esc20647@uvg.edu.gt

13 de octubre de 2023

Tabla de contenido

Recordatorio

Definición

Se llama ecuación diofantina a cualquier ecuación algebraica de dos o más incógnitas, cuyos coeficientes recorren el conjunto de los números enteros, de las cuales se buscan soluciones que pertenezcan a los números enteros.
Un tipo particular son las ecuaciones pitagóricas. Si (x, y, z) con $x, y, z \in \mathbb{Z}$, es una terna pitagórica, también lo serán

- (y, x, z)
- (ky, kx, kz)
- $(-x, y, z), (x, -y, z), (y, x, -z)$
- cualquier otra terna mediante una combinación de las anteriores

Recordatorio

Proposición

Las ternas pitagóricas primitivas (x, y, z) son de la forma

$$x = uv, \quad y = \frac{v^2 - u^2}{2}, \quad z = \frac{v^2 + u^2}{2}$$

Se dice que una terna es primitiva si (x,y,z) = 1.

Las primeras ternas pitagóricas primitivas (x, y, z) con $z \leq 100$ son

x	y	z
3	4	5
5	12	13
8	15	17
7	24	25
9	40	41
11	60	61
12	35	37
13	84	85
16	63	65
20	21	29
28	45	53
65	72	97

Cuadro: Ternas pitagóricas primitivas

Recordatorio

Teorema chino del residuo

Sea $b_1, b_2, \ldots, b_k$ tal que $a_1, a_2, \ldots, a_k$ son coprimos a pares (dos en dos), el sistema de ecuaciones

$$\begin{aligned} x &\equiv b_1 \pmod{a_1} \\ x &\equiv b_2 \pmod{a_2} \\ &\vdots \\ x &\equiv b_k \pmod{a_k} \end{aligned}$$

admite una solución que es única módulo $A = a_1 a_2 \ldots a_k$

Recordatorio

Principio de las casillas

Sea $k, m \in \mathbb{Z}$. Si $n = km + 1$ objetos son distribuidos en m conjuntos, entonces por el principio de casillas se afirma que al menos uno de los conjuntos contendrá al menos $k + 1$ objetos.

Ternas Pitagóricas

Las triplas de números enteros positivos (x, y, z) que satisfacen la ecuación $x^2 + y^2 = z^2$ se llaman triplas o ternas pitagóricas. Nótese que $x^2 + y^2 = z^2$ admite soluciones triviales de la forma $(\pm x, 0, \pm x)$ y $(0, \pm y, \pm y)$ para $x, y \in \mathbb{Z}$. Podemos suponer que x, y, z son primos relativos en pares.
Si queremos encontrar todas las ternas pitagóricas (x, y, z) entonces $x = dx', y = dy', z = dz'$, entonces

$$\begin{aligned} x^2 + y^2 = z^2 &\implies (dx')^2 + (dy')^2 = (dz')^2 \\ &\implies d^2((x')^2 + (y')^2) = d^2(z')^2 \\ &\implies (x')^2 + (y')^2 = (z')^2 \end{aligned}$$

Una terna pitagórica cuyos términos son primos relativos es una terna pitagórica primitiva.

Ternas Pitagóricas

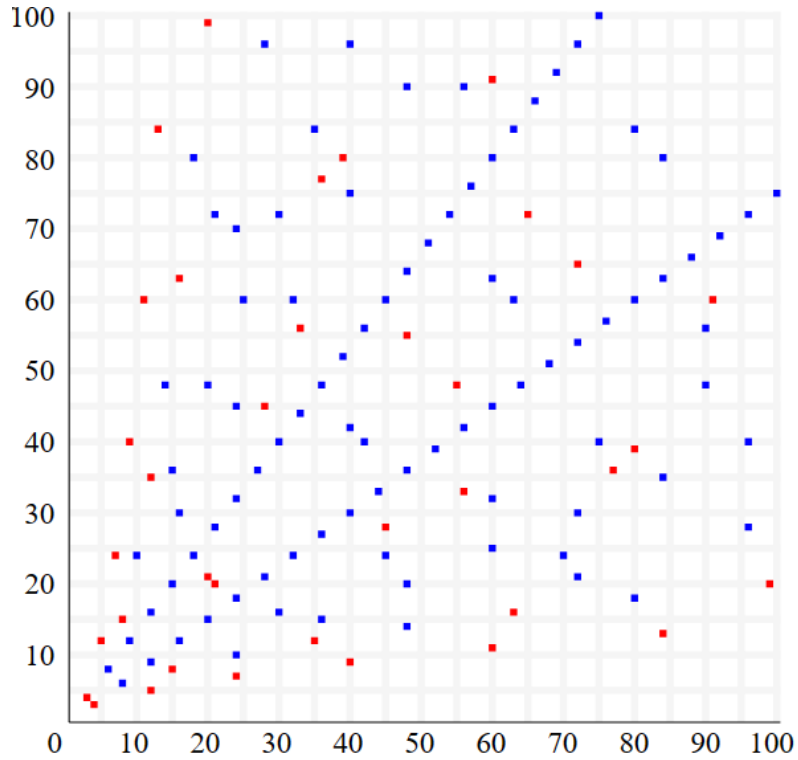

Figura: Distribución de ternas pitagóricas sobre $\mathbb{R}^2_+$. Los puntos rojos representan ternas primitivas.

Teorema de Legendre

Teorema 4.4

Sean $a, b, c \in \mathbb{Z}$, enteros libres de cuadrados, primos relativos entre sí, dos a dos, y de signos distintos. La ecuación $ax^2 + by^2 + cz^2 = 0$ tiene solución no trivial $(x, y, z) \neq (0, 0, 0)$, con $x, y, z \in \mathbb{Z}$ si, y sólo si, $-bc$ es un cuadrado módulo a, $-ca$ es cuadrado módulo b y $-ab$ es cuadrado módulo c.

Prueba. ($\Longrightarrow$) Por hipótesis, podemos suponer que x, y y z son primos relativos dos a dos, pues $d|x, d|y$, entonces $d^2|x^2, d^2|y^2$ $\Longrightarrow$

Teorema de Legendre

Demostración

$\implies d^2|ax^2+by^2 = -cz^2$. Por lo tanto, $d^2|cz^2$ y como c es libre de cuadrados, $d|z$. Esto también puede escribirse de forma que $x = dx', y = dy', z = dz'$, con $x', y', z' \in \mathbb{Z}$, y sustituyendo en la ecuación inicial,

$$\begin{aligned} ax^2 + by^2 + cz^2 = 0 &\implies a(dx')^2 + b(dy')^2 + c(dz')^2 = 0 \\ &\implies a(x')^2 + b(y')^2 + c(z')^2 = 0 \end{aligned}$$

Por otro lado, como $by^2 + cz^2 \equiv 0 \pmod{a} \implies b^2y^2 \equiv -bcz^2 \pmod{a}$. Nótese que z y a deben ser primos relativos, pues si p es primo tal que $p|a, p|z$, entonces tendremos que $p|by^2$. Sin embargo, como $p|y$, se contradice que y y z son primos relativos.

Teorema de Legendre

Demostración

Por lo tanto, a, z son primos relativos entre sí. De esta forma, z es invertible módulo a y se obtiene $(byz^{-1})^2 \equiv -bc \pmod{a}$. Entonces queda demostrado que $-bc$ es residuo cuadrático módulo a.
Nótese que por simetría de la ecuación, puede generalizarse el resultado para demostrar que $-ca$ es cuadrado módulo b y que $-ab$ es cuadrado módulo c.
$(\Longleftarrow)$ Podemos suponer sin pérdida de generalidad que $a < 0, b < 0$ y $c > 0$. Por hipótesis, $\exists u \in \mathbb{Z}$ tal que $u^2 \equiv -bc \pmod{a}$. Entonces tenemos que

$$ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv b^{-1}((by)^2 + bcz^2)$$
$$b^{-1}((by)^2 - u^2z^2) \equiv b^{-1}(by - uz)(by + uz)$$

Teorema de Legendre

Demostración

$$\equiv (y - b^{-1}uz)(by + uz)$$
$$\equiv L_1(x, y, z)M_1(x, y, z)$$

donde $L_1(x, y, z) = d_1x + e_1y + f_1z$ y $M_1(x, y, z) = g_1x + h_1y + i_1z$ son funciones lineales con $d_1 = g_1 = 0, e_1 = 1, f_1 = -b^{-1}u, h_1 = b$ y $i_1 = u$, de forma similar

$$ax^2 + by^2 + cz^2 \equiv L_2(x, y, z)M_2(x, y, z) \pmod{b}$$
$$ax^2 + by^2 + cz^2 \equiv L_3(x, y, z)M_3(x, y, z) \pmod{c}$$

con $L_k(x, y, z) = d_kx + e_kyf_kz$ y $M_k(x, y, z) = g_kx + h_k + i_kz$, $k = 2, 3$. Como a, b, c son primos relativos entre sí, dos en dos, por el Teorema Chino,

Teorema de Legendre

Demostración

podemos hallar dos funciones lineales $L(x, y, z) = dx+ey+fz$, $M(x, y, z) = gx + hy + iz$ tal que

$$\begin{array}{ccc} L \equiv L_1 \pmod{a}, & L \equiv L_2 \pmod{b}, & L \equiv L_3 \pmod{c} \\ M \equiv M_1 \pmod{a}, & M \equiv M_2 \pmod{b}, & M \equiv M_3 \pmod{c} \end{array}$$

es el resultado del sistema de congruencias. Luego,

$$ax^2 + by^2 + cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}$$

Ahora, considerando todas las triplas $(x, y, z) \in \mathbb{Z}^3$ con $0 \leq x \leq \sqrt{|bc|}, 0 \leq y \leq \sqrt{|ca|}, 0 \leq z \leq \sqrt{|ab|}$. Tenemos $(\lfloor\sqrt{|bc|}\rfloor + 1)(\lfloor\sqrt{|ca|}\rfloor + 1)(\lfloor\sqrt{|ab|}\rfloor + 1) > abc$.

Teorema de Legendre

Demostración

De estas triplas, por el principio de Dirichlet, existen dos triplas distintas entre estas,
(x_1, y_1, z_1) y (x_2, y_2, z_2) con $L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc}$ $\iff$ $L(x_1 - x_2, y_1 - y_2, z_1 - z_2) \equiv 0 \pmod{abc}$, donde, haciendo $\tilde{x} = x_1 - x_2, \tilde{y} = y_1 - y_2, \tilde{z} = z_1 - z_2$ tenemos

$$a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \equiv L(\tilde{x}, \tilde{y}, \tilde{z})M(\tilde{x}, \tilde{y}, \tilde{z}) \equiv 0 \pmod{abc}$$

Nótese que $(\tilde{x}, \tilde{y}, \tilde{z}) \neq (0, 0, 0)$. Además, $|\tilde{x}| < \sqrt{|bc|}, |\tilde{y}| < \sqrt{|ac|}$ y $|\tilde{z}| < \sqrt{|ab|}$. Por hipótesis, a, b, c son primos relativos dos a dos y libres de cuadrados, entonces no procede la igualdad. Como $a, b < 0$ y $c > 0$ tenemos,

Teorema de Legendre

Demostración

$-2abc = a|bc| + b|ac| < a\tilde{x}^2 + b\tilde{y}^2 \leq a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 \leq c\tilde{z}^2 < |ab|\, c = abc$. Como $abc | a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2$, entonces se tiene que $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = 0$. En el caso que $a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 = -abc$ se tiene

$$\begin{aligned} 0 &= (a\tilde{x}^2 + b\tilde{y}^2 + c\tilde{z}^2 + abc)(\tilde{z}^2 + ab) \\ &= a(\tilde{x}\tilde{z} + b\tilde{y})^2 + b(\tilde{z}\tilde{y} - a\tilde{x})^2 + c(\tilde{z} + ab)^2 \end{aligned}$$

lo cual tiene como resultado $(\tilde{x}\tilde{z} + b\tilde{y}, \tilde{y}\tilde{z} - a\tilde{x}, \tilde{z}^2 + ab)$ con $\tilde{z}^2 + ab \neq 0$. $\square$

Ejemplo

Considérese la ecuación

$$x^2 + 3y^2 - 7z^2 = 0$$

con $(1,3) = 1, (1,-7) = 1, (3,-7) = 1$. Se tiene

$$\begin{aligned} -ac &= -(1)(-7) = 7 \equiv 1 \pmod 3 \\ -ab &= -(1)(3) = -3 \equiv 4 \pmod 7 \\ -bc &= -(3)(-7) = 21 \equiv 0 \pmod 1 \end{aligned}$$

References


Fabio E. Brochero Martinez, Carlos G. Moreira, Nicolau Saldanha, Eduardo Tengan (1999)
Teoria dos Números
Um passeio com primos e outros números familiares pelo mundo inteiro
148-153


Pablo Soberón (2014)
Revista Tzaloa, año 2
El Principio de las Casillas