Academia Sabatina de Jóvenes Talento

Ecuaciones Diofánticas
Clase #4

Encuentro: 19 **Nivel:** 5
Curso: Ecuaciones Diofánticas **Semestre:** II
Fecha: 31 de agosto de 2024 **Instructor:** Kenny Jordan Tinoco
Instructor Aux: Gema Tapia

Contenido: Método de Congruencia

En esta sesión de clase se sigue con los métodos básico para la resolución de ecuaciones diofánticas, en concreto con el método de congruencia, el cual nos permite utilizar las propiedades de divisibilidad para hallar posibles soluciones de una ecuación.

1. Desarrollo

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 1.1 (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 1.2 (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 $a \equiv b \pmod{m} \iff (a - b) \mid m$. Con esto, podemos demostrar el siguiente teorema.

Teorema 1.1 (Propiedades de Congrencia)**.** 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 1.1. 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 1.3 (Función phi de Euler)**.** Para cualquier entero n se denota a $\varphi(n)$ como cantidad de números de coprimos menores a n.

Teorema 1.2 (Teorema de Euler)**.** Si a y n son dos enteros positivos primos relativos entre si, entonces $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Teorema 1.3 (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.

$$x^2 \equiv 0, 1 \pmod{3} \qquad x^2 \equiv 0, 1, 4 \pmod{8} \qquad x^3 \equiv 0, \pm 1 \pmod{7}$$

$$x^2 \equiv 0, 1 \pmod{4} \qquad x^2 \equiv 0, 1, 4, 9 \pmod{16} \qquad x^4 \equiv 0, 1 \pmod{16}$$

$$x^2 \equiv 0, \pm 1 \pmod{5} \qquad x^3 \equiv 0, \pm 1 \pmod{9} \qquad x^5 \equiv 0, \pm 1 \pmod{11}$$

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 1.2. 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 1.3. 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. ■

[1] ¿Podés justificar por qué?

1.1. Ejercicios y problemas

Ejercicios y problemas para el autoestudio.

Ejercicio 1.1. Demostrar que 7 divide a $3^{2n+1} + 2^{n+2}$ para todo natural n.

Ejercicio 1.2. Hallar los restos cuadráticos en módulo 13.

Ejercicio 1.3. Probar que no existen enteros positivos a, b tales que $a^2 - 3b^2 = 8$.

Ejercicio 1.4. ¿Existen enteros positivos x, y tal que $x^3 = 2^y + 15$?

Ejercicio 1.5. Probar que la ecuación $x^2+3xy-2y^2 = 122$ no tiene soluciones enteras

Ejercicio 1.6. Demostrar que la ecuación $x^2 - 7y = 3$ no tiene soluciones enteras.

Ejercicio 1.7. Demostrar que no hay enteros para los cuales $800000007 = x^2+y^2+z^2$.

Ejercicio 1.8. Hallar las soluciones enteras de la ecuación $x^2 - 5y^2 = 2$.

Ejercicio 1.9. Si se cumple que $n \equiv 4 \pmod 9$, probar que la ecuación $x^3+y^3+z^3 = n$ no tiene soluciones enteras.

Ejercicio 1.10. Probar que la ecuación $(x+1)^2 + (x+2)^2 + \cdots + (x+2001)^2 = y^2$ no es soluble en enteros x, y.

Ejercicio 1.11. Hallar las soluciones de enteros tal que $a^3 + 2b^3 + 4c^3 = 9d^3$.

Ejercicio 1.12. Encontrar todas las soluciones (p, q) de números primos tales que $p^3 - q^5 = (p+q)^2$.

Ejercicio 1.13. 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).

Ejercicio 1.14. Probar que la ecuación $(x+1)^2 + (x+2)^2 + \cdots + (x+99)^2 = y^z$ no tiene soluciones enteras (x, y, z) con $z > 1$.

Ejercicio 1.15. Probar que la ecuación $x^5 - y^2 = 4$ es insoluble en los enteros.

Ejercicio 1.16. 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 1.17. 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 $n = 2891$.

2. Problemas propuestos

Los problemas de esta sección es la **tarea**. El estudiante tiene el deber de entregar sus soluciones en la siguiente sesión de clase (también se pueden entregar borradores). Recordar realizar un trabajo claro, ordenado y limpio.

3. Extra

Problemas para **puntos extras en la nota final** del curso. Los problemas extras se califican de manera distinta a los problemas propuestos.

Problema 3.1. Hallar los pares (a, b) de enteros positivos tales que satisfacen la ecuación $a^{b^2} = b^a$.

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. Notas de clase

4.1. ¿Qué?

4.2. ¿Cómo?