Capítulo

3

Congruencias de Grado Superior

3.1 Introdución

En el capítulo anterior vimos cómo resolver congruencias del tipo

$$ax \equiv b \; mod \; m$$

donde a, b y m son enteros $m > 1$, y $(a, b) = 1$.

En este capítulo discutiremos un nuevo enfoque de este problema, al considerar esta ecuación dentro del anillo de enteros módulo m. Sabemos que a posee un inverso multiplicativo, a^*, con la propiedad

$$a \cdot a^* = 1$$

y por lo tanto se puede multiplicar la ecuación original por a^*, a fin de resolver en términos de x, esto es

$$x \equiv a^* b \; mod \; m$$

Veremos cómo se pueden obtener inversos multiplicativos, mediante el teorema de Euler, lo cual nos permite resolver una gran cantidad de problemas relativos a las congruencias lineales y de grado superior. Como consecuencia del Teorema de Euler, se obtiene el famoso Teorema de Fermat (Pequeño teorema), que establece la identidad

$$x^{p-1} \equiv 1 \; mod \; p$$

válida para todo entero x, con $(x, p) = 1$

Finalmente, se estudian las congruencias polinomiales módulo un entero m. En el caso de ser m un primo se dan una serie de resultados interesantes sobre la factorización y el cálculo de raíces de polinomios.

3.2 La función φ de Euler

Definición 3.2.1 *Sea m un entero positivo. Un* **sistema reducido de residuos** *módulo m, es un conjunto de enteros $a_1, \cdots, a_n$ tales que:*

i) Los a_i son incongruentes módulo m.

ii) Para todo i se tiene $(a_i, m) = 1$.

iii) Si a es un entero cualquiera, tal que $(a, m) = 1$, entonces existe un a_i, tal que $a \equiv a_i \ mod \ m$.

Ejemplo 1:

Un sistema reducido módulo 6, viene expresado por $\{1, 5\}$.

Notemos que las propiedades *i)* y *ii)* ciertamente se satisfacen. Si a es un entero tal que $(a, 6) = 1$, entonces aplicando el algoritmo de la división, se tiene enteros q y r, tales que $a = 6q + r$, donde $0 \leq r < 6$. Por otro lado, $(a, 6) = (6q + r, 6) = (r, 6) = 1$. Luego $r = 1$ ó $r = 5$, lo cual implica

$$a \equiv 1 \ mod \ 6 \quad \text{ó} \quad a \equiv 5 \ mod \ 6$$

Luego *iii)* también se cumple en este ejemplo.

Utilizando un razonamiento análogo, en el caso general, se puede probar:

Teorema 3.2.1 *El conjunto de enteros*

$$A = \{x \mid 0 \leq x < m \ \text{ y } \ (x, m) = 1\}$$

es un sistema reducido de residuos módulo m.

Observación: El teorema anterior demuestra la existencia de un sistema reducido de residuos, para cualquier entero m. Sin embargo existen otros sistemas, además de este dado arriba. Por ejemplo $\{1, 5\}$ y $\{7, 11\}$ son ambos sistemas de residuos módulo 6.

Una pregunta natural es la siguiente: ¿Todo sistema reducido posee el mismo número de elementos? La respuesta a esto es afirmativa, como se verá más adelante.

Definición 3.2.2 *La función φ de Euler, aplicada al entero positivo m se define por*

$$\varphi(m) = |A|$$

En otras palabras, $\varphi(m)$ es el número de enteros positivos mayores o iguales a uno, y menores que m, los cuales son primos relativos con m.

Teorema 3.2.2 *Todo sistema reducido de residuos módulo m, posee $\varphi(m)$ elementos.*

Demostración:

Sea $r_1, \cdots, r_n$ un sistema reducido de residuos módulo m. Probaremos que existe una correspondencia biyectiva entre el conjunto B formado por los r_i y el conjunto A definido previamente.

En efecto, si $x \in A$, se tiene que $(x, m) = 1$ y por ser B un sistema reducido, existe un elemento r_i en B, tal que $x \equiv r_i \ mod \ m$. Por lo tanto definimos

$$\begin{aligned} f : A &\longrightarrow B \\ x &\longrightarrow r_i \end{aligned}$$

Es claro que la función f está bien definida, pues a cada x en A se le puede asignar mediante esta regla un único elemento en B. Seguidamente, probaremos que f es inyectiva y sobreyectiva, con lo cual habremos demostrado que A y B tienen el mismo número de elementos.

Para demostrar la inyectividad, supóngase que x_1 y x_2 son dos elementos en A que satisfacen $f(x_1) = f(x_2)$.

Luego existe un j, $(1 \leq j \leq n)$, tal que

$$\begin{aligned} x_1 &\equiv r_j \ mod \ m \\ x_2 &\equiv r_j \ mod \ m, \end{aligned}$$

lo cual implica $x_1 \equiv x_2 \ mod \ m$. Esto último sucede si y sólo si $x_1 = x_2$.

Para demostrar la sobreyectividad, sea r_i un elemento cualquiera de B. Luego se verifica $(r_i, m) = 1$. Por ser A un sistema reducido, existe un x en A tal que $r_i \equiv x \ mod \ m$, por lo cual $f(x) = r_i$. ♠

Veamos a continuación una tabla con algunos valores de la función φ de Euler.

m	$\varphi(m)$
2	1
3	2
4	2
5	4
6	2

m	$\varphi(m)$
7	6
8	4
9	6
10	4
11	10

m	$\varphi(m)$
12	4
13	12
14	6
15	8
16	8

m	$\varphi(m)$
17	16
18	6
19	18
20	8
21	12

Observando la presente tabla, notamos que $\varphi(m)$ es par, para todo $m \geq 3$. Esto será probado de manera general más adelante. También es evidente que si p es primo, entonces $\varphi(p)$ es igual a $p - 1$. Nuestra próxima meta, será obtener una fórmula para calcular la función de Euler de un número compuesto, la cual va a depender de la factorización de dicho número. Es decir, si m se expresa como un producto de primos $p_1 \cdots p_n$, entonces $\varphi(m)$ se expresará en función de $p_1, \cdots, p_n$.

El primer paso en este proceso viene dado por el siguiente:

Teorema 3.2.3 *Si p es primo y $\alpha \geq 1$, entonces*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}.$$

Demostración:

Recordemos que $\varphi(p^\alpha)$ es el número de enteros positivos menores o iguales que p^α, y que son primos relativos con p^α. Podemos contar los enteros positivos menores que p^α que no son primos relativos con el. Una lista de estos enteros es la siguiente:

$$p, 2p, 3p, \cdots, (p-1)p, p^2, 2p^2, \cdots, p^{\alpha-1}p$$

vemos que hay entonces $p^{\alpha-1}$ de ellos, luego restando este número del total de enteros positivos menores que p^{α}, obtenemos por lo tanto $\varphi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1}$. ♠

Ejemplo 2:

Por intermedio del teorema anterior podemos calcular la función de Euler sobre una cantidad infinita de números, por ejemplo

$$\varphi(81) = \varphi(3^4) = 3^4 - 3^3 = 34.$$

Teorema 3.2.4 *Sean m y n son dos enteros positivos tales que $(m, n) = 1$. Se tiene entonces $\varphi(mn) = \varphi(m)\varphi(n)$.*

Demostración:

Definimos los siguientes conjuntos

$$\begin{aligned} A_n &= \{x | 1 \leq x < n | (x, n) = 1\} \\ A_m &= \{x | 1 \leq x < m | (x, m) = 1\} \\ A_{mn} &= \{x | 1 \leq x < mn | (x, mn) = 1\} \end{aligned}$$

La razón de definir estos tres conjuntos se debe a que $|A_n| = \varphi(n)$, $|A_m| = \varphi(m)$ y $|A_{mn}| = \varphi(mn)$. La idea de la demostración consiste en probar

$$|A_{mn}| = |A_m \times A_n| = |A_n||A_m|,$$

de lo cual se deduce $\varphi(mn) = \varphi(m)\varphi(n)$.

Comenzaremos por definir una función

$$f : A_{mn} \longrightarrow A_n \times A_m$$

de la forma siguiente:

Para cada $x \in A_{mn}$, se cumple $(x, mn) = 1$, de donde $(x, m) = 1$ y $(x, n) = 1$. Luego, existen elementos únicos $r \in A_n$ y $h \in A_m$ tales que $x \equiv r \ mod \ n$ y $x \equiv h \ mod \ m$.

Definimos entonces $f(x) = (r, h) \in A_n \times A_m$. Es claro que f está bien definida.

Además, f es inyectiva, si $f(x) = f(y)$ para algunos enteros x, y en A_{mn}, se tendrá que existen enteros r, h tales que x e y son ambos soluciones del sistema:

$$Z \equiv r \ mod \ n,$$
$$Z \equiv h \ mod \ m.$$

De acuerdo al teorema 3.2.3, el cual afirma la unicidad módulo mn de la solución de este sistema, se tendrá entonces:

$$x \equiv y \ mod \ mn$$

lo cual implica que $x = y$. Por lo tanto f es inyectiva.

Finalmente, para probar la sobreyectividad de f, tomemos un elemento $(i, j) \in A_n \times A_m$. Nuevamente, usamos el teorema 3.2.3 para garantizar la existencia de una solución del sistema

$$Z \equiv i \ mod \ n,$$
$$Z \equiv j \ mod \ m.$$

la cual denotaremos por x. De las dos condiciones $(i, n) = 1$ y $(j, m) = 1$ se deduce que $(x, mn) = 1$, luego $x \in A_{mn}$ y además $f(x) = (i, j)$. Como consecuencia de esto, se ha demostrado que f es sobreyectiva.

Al ser f biyectiva queda probado que

$$|A_{mn}| = |A_n \times A_m|$$

y de esto se deduce:

$$\varphi(mn) = \varphi(m)\varphi(n).$$

♠

Ejemplo 3:

A la luz de los resultados anteriores, nos es permitido ahora calcular la función de Euler para cualquier entero, una vez que se conozca su factorización prima.

Por ejemplo:

$$\begin{aligned}\varphi(600) &= \varphi(2^3 \cdot 3 \cdot 5^3) \\ &= \varphi(2^3)\varphi(3)\varphi(5^3) \\ &= (2^3 - 2^2)(3-1)(5^3 - 5^2) \\ &= 4 \cdot 2 \cdot 20 \\ &= 160\end{aligned}$$

Corolario 3.2.1 *Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, donde los p_i son primos distintos se tendrá entonces:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right)$$

Demostración:

Ejercicio.

3.3 Funciones Multiplicativas

Existen muchas funciones en teoría de números que satisfacen propiedades similares a la función de Euler, como la establecida en el teorema 3.2.4, esto es $\varphi(mn) = \varphi(m)\varphi(n)$ cuando m y n son primos relativos. En esta sección se estudiaran una serie de funciones que cumplen estas y otras propiedades interesantes.

A lo largo de este capítulo, $\mathbb{Z}^+$ denotará el conjunto de los enteros positivos.

Definición 3.3.1 *Una función* $f : \mathbb{Z}^+ \longrightarrow \mathbb{Z}$ *se llama* **función aritmética**.

Definición 3.3.2 *Una función aritmética* f *se dice* **multiplicativa**, *si satisface*

$$f(mn) = f(m)f(n),$$

cada vez que $(m, n) = 1$.

Definición 3.3.3 *Una función aritmética se dice* **totalmente multiplicativa** *si satisface*

$$f(mn) = f(m)f(n),$$

para cualquier par de enteros m *y* n.

Ejemplo 4:

Las funciones siguientes son multiplicativas:
a) La función φ de Euler.
b) La función constante $f(n) = 1$, para todo $n \in \mathbb{Z}^+$.
c) La función idéntica $f(n) = n$, para todo $n \in \mathbb{Z}^+$.
Las dos últimas son totalmente multiplicativas, pero la primera no lo es.

Existen otras funciones multiplicativas, de gran utilidad, como lo son:
$d(n)$ = número de divisores positivos de n.
$\sigma(n)$= suma de los divisores positivos de n.

Ejemplo 5:

Podemos calcular algunos valores de estas funciones y expresarlos mediante una tabla:

n	$d(n)$	$\sigma(n)$
2	2	3
3	2	4
4	3	7
5	6	6
6	4	12
7	2	8
8	4	15
9	3	13
10	4	18
11	2	12

n	$d(n)$	$\sigma(n)$
12	6	28
13	2	14
14	4	24
15	4	24
16	5	31
17	2	18
18	6	39
19	2	20
20	6	42
21	4	32

Notación Si f es una función aritmética, y n es un entero positivo, entonces el símbolo

$$\sum_{d/n} f(d)$$

indica la suma de todos los términos $f(d)$, donde d es un divisor de n.

Teorema 3.3.1 *Sea f una función multiplicativa y*

$$F(n) = \sum_{d/n} f(d)$$

entonces F es multiplicativa.

Demostración:

Sean m y n enteros positivos tales que $(m, n) = 1$. Debemos demostrar entonces $F(mn) = F(n)F(m)$, para lo cual supondremos que m y n tienen descomposición en factores primos de la forma

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \quad , \quad m = q_1^{\delta_1} q_2^{\delta_2} \cdots q_t^{\delta_t}.$$

Entonces los divisores de mn son todos de la forma

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s} q_1^{\lambda_1} q_2^{\lambda_2} \cdots q_t^{\lambda_t},$$

donde $0 \leq \gamma_i \leq \alpha_i$, $0 \leq \lambda_j \leq \beta_j$.

Por lo tanto

$$\begin{aligned} F(m,n) &= \sum_{d/mn} f(d) \\ &= \sum_{0\leq\gamma_i\leq\alpha_i\leq \ 0\leq\lambda_j\leq\beta_j} f(p_1^{\gamma_1}\cdots p_s^{\gamma_s} q_1^{\lambda_1}\cdots q_t^{\lambda_t}) \\ &= \sum_{0\leq\gamma_i\leq\alpha_i} \ \sum_{0\leq\lambda_j\leq\beta_j} f(p_1^{\gamma_1}\cdots p_s^{\gamma_s)} f(q_1^{\lambda_1}\cdots q_t^{\lambda_t}) \\ &= \sum_{d_1/n} \sum_{d_2/m} f(d_1) f(d_2) \\ &= \left(\sum_{d_1/n} f(d_1)\right)\left(\sum_{d_2/m} f(d_2)\right) \\ &= F(n)F(m). \end{aligned}$$

♠

Teorema 3.3.2 *La función $d(n)$= número de divisores de n, es multiplicativa.*

Demostración:

Usamos el resultado anterior, haciendo $f(n) = 1$. Luego

$$d(n) = \sum_{d/n} 1$$

es multiplicativa. ♠

Teorema 3.3.3 *La función $\sigma(n)$= suma de los divisores de n, es multiplicativa.*

Demostración:

Nuevamente, por intermedio del teorema 3.3.2 se obtendrá el resultado. Tomando $f(n) = n$, nos produce:

$$\sigma(n) = \sum_{d/n} d.$$

Claramente σ es multiplicativa en virtud del teorema 3.3.2. ♠

Una vez que hemos demostrado este par de teoremas, nos resulta relativamente fácil calcular los valores de las funciones $d(n)$ y $\sigma(n)$ cuando se conoce la descomposición prima de n. Unicamente falta obtener fórmulas para estas funciones en el caso de ser n una potencia de un primo, lo cual no es muy difícil; como se verá a continuación.

Si p es primo, entonces los divisores de una potencia de p, digamos p^α, son $1, p, p^2, \cdots p^{\alpha-1}, p^\alpha$. Luego se tiene

$$d(p^\alpha) = \alpha + 1,$$

y

$$\begin{aligned} \sigma(p^\alpha) &= 1 + p + \cdots + p^\alpha \\ &= \frac{1 - p^{\alpha+1}}{1 - p^\alpha}. \end{aligned}$$

Podemos resumir todas estas observaciones en el siguiente corolario.

Corolario 3.3.1 *Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, con p_i primos, se tiene:*

$$\begin{aligned} &a) \quad d(p) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1) \\ &b) \quad \sigma(n) = \left(\frac{1 - p_1^{\alpha_1+1}}{1 - p_1^{\alpha_1}}\right) \cdots \left(\frac{1 - p_s^{s+1}}{1 - p_s^{\alpha_s}}\right) \end{aligned}$$

Ejercicios

1) Construir una tabla con los valores de n, $1 \leq n \leq 100$ para las funciones
a) $\varphi(n)$
b) $d(n)$
c) $\sigma(n)$.

2) Hallar un sistema reducido de residuos módulo 25.

3) Sea n un entero positivo fijo. Demostrar que la ecuación $\varphi(x) = n$ posee un número finito de soluciones.

4) Hallar el menor entero x para el cual $\sigma(2x) = 2\varphi(x)$.

5) **Números perfectos:** un entero positivo n se dice perfecto si n es igual a la suma de sus divisores, diferentes de n (divisores propios). Por ejemplo: $6 = 3+2+1$ = suma de sus divisores propios.

Pregunta: ¿Existen números perfectos? La respuesta es sí, 28 y 496 también son perfectos (verficarlo!).

Pregunta: ¿Existen infinitos números perfectos? No se sabe hasta el presente.

Probar:
a) n es perfecto, si y sólo si $\sigma(n) = 2n$.
b) Usando el resultado anterior, probar lo siguiente: si $2^\alpha - 1$ es primo, entonces $2^{\alpha-1}(2^\alpha - 1)$ es perfecto.

6) **Primos de Mersene:** Un número primo de la forma $2^\alpha - 1$, se llama un primo de Mersene, por ejemplo: $3 = 2^2 - 1$, $31 = 2^5 - 1$.

Pregunta: ¿Existen infinitos primos de Mersene? No se conoce la respuesta. Se sabe que $2^{19937} - 1$ es un primo de Mersene que contiene 6002 dígitos!. Hallar otro primo de Mersene distinto de los dados como ejemplos.

7) **Función de Mobius:** Considerese la función aritmética

$$\mu(n) = \begin{cases} 1, & \text{si} \quad n = 1 \\ 0, & \text{si} \quad n \text{ es divisible por un cuadrado } d \neq 1 \\ (-1)^r, & \text{si} \quad n = p_1 p_2 \cdots p_r,\ p_i \text{ primos diferentes.} \end{cases}$$

a) Probar que μ es multiplicativa
b) Probar

$$\sum_{d/n} \mu(d) = 0, \quad \text{si } n > 1$$

8) Halle un sistema reducido de residuos módulo 10 en el conjunto $\{11, 12, \ldots, 20\}$

9) Calcular $\mu(429)$, $\mu(400)$ y $\mu(505)$.

10) Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, donde los p_i son primos distintos. Probar la fórmula:

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right)$$

3.4 Teoremas de Euler y Fermat

En esta sección, m será un número entero positivo mayor que 1.

Teorema 3.4.1 *Sea $x_1, \cdots, x_n$ un sistema reducido de residuos módulo m, y sea a un entero tal que $(a, m) = 1$. Luego $ax_1, \cdots, ax_n$ es también un sistema reducido módulo m.*

Demostración:

En primer lugar, debemos probar que los ax_i son incongruentes módulo m. En efecto, supongamos que para algunos i, j se tiene

$$ax_i \equiv ax_j \, mod \, m.$$

Esto implica que m divide a $(ax_i - ax_j)$ y de esto se deduce $m|x_i - x_j$, pues $(a, m) = 1$ por hipótesis. Por lo tanto se tiene que

$$x_i \equiv x_j \ mod \ m,$$

con lo cual $x_i = x_j$, porque los x_i son incongruentes entre sí. Con esto queda probada la primera parte de la demostración.

En segundo lugar, es claro que para todo i se tiene que $(ax_i, m) = 1$, pues $(x_i, m) = 1$ y además $(a, m) = 1$. Es decir, x_i y a no poseen factores primos comunes con m y en consecuencia ax_i tampoco tiene factores en común con m.

Por último, resta probar que si c es un entero con $(c, m) = 1$, entonces existe un i tal que

$$ax_i \equiv c \ mod \ m.$$

Notemos que la ecuación lineal de congruencia

$$ax \equiv c \ mod \ m \tag{3.1}$$

siempre se puede resolver, con las hipótesis que tenemos sobre a, c y m. Por lo tanto, sea y_0 una solución de (3.1), la cual debe cumplir

$$ay_0 = c + mt,$$

para algún t entero. Si m divide a y_0, entonces m divide a c, lo cual es imposible. Por lo tanto debe ser $(y_0, m) = 1$, con lo cual obtenemos

$$y_0 \equiv x_i \ mod \ m,$$

para algún i, y de aquí se deduce:

$$ay_0 \equiv ax_i \ mod \ m.$$

Sustituyendo este resultado en la ecuación (3.1) nos da:

$$c \equiv ay_0 \equiv ax_i \ mod \ m,$$

y con esto termina la demostración. ♠

Teorema 3.4.2 *(Teorema de Euler) Si a es un entero, con $(a, m) = 1$, entonces se tiene*

$$a^{\varphi(m)} \equiv 1 \ mod \ m.$$

Demostración:

Sea $x_1, \cdots, x_n$ un sistema reducido de residuos módulo m, luego $n = \varphi(m)$. En virtud del teorema anterior: $ax_1, \cdots, ax_n$ es también un sistema reducido, y en particular obtenemos que para todo i existe un j tal que

$$x_i \equiv ax_j \ mod \ m \tag{3.2}$$

donde $1 \leq i \leq n$, $1 \leq j \leq n$.

En realidad, para cada i se tiene una ecuación del tipo (3.2). Luego multiplicando $x_1 x_2 \cdots x_n$ y usando las ecuaciones dadas para cada x_i, obtenemos

$$\prod_{i=1}^{n} x_i \equiv a^n \prod_{j=1}^{n} x_j \, mod \, m \tag{3.3}$$

Observemos que cada uno de los términos x_i es primo relativo con m, luego el producto de todos ellos también lo es, y en consecuencia podemos dividir ambos miembros de (3.3) entre este producto, para obtener

$$a^n \equiv a^{\varphi(m)} \equiv 1 \ mod \ m.$$

Con lo cual se da fin a la prueba. ♠

Teorema 3.4.3 *(Teorema de Fermat) Si p es primo, entonces*

$$a^{p-1} \equiv 1 \ mod \ p$$

Demostración:

Notemos que la condición $p|a$ implica $(a, p) = 1$, y de acuerdo al teorema anterior se debe tener

$$a^{\varphi(p)} \equiv a^{p-1} \equiv 1 \ mod \ p$$

♠

El teorema de Euler posee el siguiente corolario, muy importante:

Corolario 3.4.1 *Sean a y b dos enteros, con $(a, m) = 1$. Entonces la ecuación lineal de congruencia*

$$ax \equiv b \; mod \; m \tag{3.4}$$

posee solución

$$x \equiv a^{\varphi(m)-1} b \; mod \; m$$

Demostración:

De acuerdo al teorema 3.4.3 se tiene que $a^{\varphi(m)} \equiv 1 \; mod \; m$. Luego multiplicando (3.4) por $a^{\varphi(m)-1}$ se obtiene el resultado deseado. ♠

Ejemplo 6:

Resolver la congruencia

$$3x \equiv 2 \; mod \; 5$$

Solución: Usando el teorema anterior se tiene:

$$\begin{aligned} x &\equiv 3^{\varphi(5)-1} 2 \, mod \, 5 \\ &\equiv 3^3 2 \, mod \, 5 \\ &\equiv 54 \, mod \, 5 \end{aligned}$$

Luego $x \equiv 4 \; mod \; 5$.

Observación 1: El teorema de Fermat se puede generalizar a cualquier grupo de manera siguiente:

Si G es un grupo de n elementos, entonces para todo elemento $a \in G$ se tiene

$$a^n = e,$$

donde e es el elemento neutro de G.

Observación 2: En el capítulo 2, sección 4, vimos que si p es primo, entonces el conjunto de enteros módulo p, denotado por $\mathbb{Z}_p$, es un cuerpo. Por lo tanto, todo elemento distinto de cero en $\mathbb{Z}_p$ posee un inverso multiplicativo.

Por ejemplo si $p = 7$ en $\mathbb{Z}_7$ tenemos

$$2 \cdot 4 \equiv 1 \ mod\ 7 \quad ; \quad 3 \cdot 5 \equiv 1 \ mod\ 7 \quad ; \quad 6 \cdot 6 \equiv 1 \ mod\ 7$$

Luego se tiene

$$\begin{aligned} 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 &\equiv 6 \, mod\, 7 \\ 6! &\equiv -1 \, mod\, 7 \end{aligned}$$

Teorema 3.4.4 *(Teorema de Wilson)*

$$p \text{ es primo} \iff (p-1)! \equiv -1 \ mod\ p$$

Demostración:

Si $p = 2$ el resultado es evidente. Supongamos que $p > 2$

Sea $A = \{1, 2, \cdots, p-1\}$. De acuerdo a la observación anterior, cada elemento x en A, posee un inverso multiplicativo en A. En otras palabras, para cada x, $1 \leq x \leq p-1$, existe un y, $1 \leq y \leq p-1$, tal que

$$xy \equiv 1 \ mod\ p$$

Posiblemente suceda que $x = y$, en algunos casos, pero veamos cuando puede ocurrir esto. Si $x^2 \equiv 1 \ mod\ p$, entonces p divide a $(x+1)(x-1)$, y como p es primo se tendrá:

i) $p|x+1$, y en este caso

$$x \equiv -1 \equiv p-1 \ mod\ p,$$

o bien

ii) $p|x-1$, y en este caso se tiene

$$x \equiv 1 \ mod \ p.$$

Así pues, los únicos elementos de A que satisfacen la condición $x^{-1} = x$ son $x = 1$ y $x = p-1$. Por lo tanto cada x de A, distinto de 1 y $p-1$, se puede agrupar con su inverso $y \neq x$, y al multiplicar ambos obtenemos uno. Si multiplicamos ahora todos los elementos de A, y los agrupamos en pares (x, y) donde y es el inverso de x, obtendremos $(p-3)/2$ parejas de la forma (x, y) con $xy = 1$, lo cual produce $(p-3)/2$ unos, y por lo tanto

$$\begin{aligned} (p-1)! = 1 \cdot 2 \cdot 3 \cdots (p-1) &\equiv \overbrace{1 \cdot 1 \cdot 1 \cdots 1}^{(p-3)/2 \text{ veces}}(p-1) \, mod \, p \\ &\equiv p-1 \, mod \, p \\ &\equiv -1 \, mod \, p \end{aligned}$$

Recíprocamente, si

$$(p-1)! \equiv -1 \ mod \ p,$$

entonces de esta congruencia se deduce lo siguiente: ningún x, con $1 \leq x \leq p-1$ divide a p, luego p es primo.

♠

Ejercicios

1) Verifique el teorema de Euler para $m = 7$ y a tomando los valores $2, 3, 4, 5$ y 6.

2) Verifique el teorema de Fermat para $p = 11$ y $a = 3$.

3) Hállese el mínimo valor de n para el cual $5^n \equiv 1 \ mod \ 7$.

4) Si p es primo, impar y $x \equiv -1 \ mod \ p$, demuéstrese que

$$x^{p-2} + x^{p+3} + \cdots + x + 1 \equiv 0 \ mod \ p$$

5) Resolver la congruencia: $6x \equiv 2 \ mod \ 7$.

6) Resolver $x^{80} \equiv 2 \ mod \ 5$.

7) En $\mathbb{Z}_{11}$, hallar los inversos multiplicativos de 3,5 y 9.

8) ¿Es $2^{100} - 1$ un número primo?.

9) Demuestre que 35 divide a $6^{24} - 1$. *Ayuda* : $\varphi(35) = 24$.

10) Demuestre que $(p-1)! \equiv -1 \ mod \ p$, entonces p es primo.

11) Demuestre que si $p \equiv 1 \ mod \ 4$ entonces la congruencia

$$x^2 \equiv -1 \ mod \ p$$

posee solución.

12) Hallar las soluciones de
a) $x^2 \equiv -1 \ mod \ 13$,
b) $x^2 \equiv -1 \ mod \ 17$

13) Demuestre que si $p \equiv 1 \ mod \ 4$, se puede resolver

$$x^2 + y^2 \equiv 0 \ mod \ p$$

14) Hallar una solución de $x^2 + y^2 \equiv 0 \ mod \ 13$.

15) Probar que $x^5 - x$ es divisible por 5,8 y 10, para todo entero x.

16) Probar que $x^{16} - x$ es divisible por 32, para todo x entero.

17) Si p es primo, hallar el inverso multiplicativo de $(p-1)!$ en $\mathbb{Z}_p$.

18) Hallar las soluciones de
a) $15x \equiv 2 \ mod \ 17$,
b) $8x \equiv 3 \ mod \ 15$.

19) En $\mathbb{Z}_{11}$, hallar todos los elementos y tales que $y = x^2$ para algún x en $\mathbb{Z}_{11}$.

20) Hallar todas las soluciones de $x^3 \equiv 1 \ mod \ 11$.

21) Verificar el teorema de Fermat para el grupo de los enteros módulo m con la adición.

22) Construir un ejemplo de un grupo finito de 6 elementos, y verifíquese el teorema de Fermat, en el mismo.

3.5 Congruencias Polinomiales

En el capítulo 2, vimos como se resolvía una congruencia lineal

$$ax \equiv b \; mod \; m$$

en donde a y b son enteros.

En esta sección y las siguientes, nos ocuparemos de resolver congruencias del tipo

$$f(x) \equiv 0 \; mod \; m, \tag{3.5}$$

donde $f(x)$ es un polinomio con coeficientes enteros. Es decir

$$f(x) = a_n x^n + \cdots + a_1 x + a_0,$$

con a_i entero, $1 \leq i \leq n$.

Notemos que x_1 es solución de (3.5), entonces todo entero b que satisface $b \equiv x_1 \; mod \; m$, también es solución (verificarlo!), luego consideramos solo aquellas soluciones distintas módulo m.

Observación: La teoría de polinomios módulo m, difiere un poco de la teoría general de polinomios sobre $\mathbb{Q}$.

Sabemos que en $\mathbb{Q}[x]$ todo polinomio de grado n, posee a lo sumo n raíces. Esto es falso en general para polinomios módulo m. Por ejemplo el polinomio de grado 2 en los enteros módulo 6,

$$f(x) = x^2 - x$$

tiene 4 raíces las cuales son 0,1,3 y 4.

En el ejemplo 9 se estudia el polinomio

$$x^3 - 2x^2 - 9 \, mod \, 125,$$

el cual tiene 11 raíces.

Sin embargo si p es un número primo, veremos que todo polinomio sobre $\mathbb{Z}_p$ de grado n, posee a lo sumo n raíces.

Existe una relación importante entre los polinomios en $\mathbb{Z}[X]$ y polinomios en $\mathbb{Z}_m[x]$.

Teorema 3.5.1 *Sea $f(x)$ un polinomio con coeficientes enteros, Si $f(x)$ es irreducible módulo m para algún m, entonces $f(x)$ es irreducibles en $\mathbb{Z}[x]$.*

Ejemplo: El polinomio $f(x) = x^2 + 1$, es irreducible en $\mathbb{Z}_3$. Luego $f(x)$ es irreducible en $\mathbb{Z}[x]$ y por lo tanto en $\mathbb{Q}[x]$, pues $f(x)$ es mónico.

En lo sucesivo y hasta el resto de este capítulo, todos los polinomios considerados, son de coeficientes enteros.

A fin de simplificar los cálculos en las congruencias polinomiales, introduciremos la siguiente definición.

Definición 3.5.1 *Dos polinomios f y g de grados m y n, con $m \geq n$*

$$f(x) = a_m x^m + \cdots + a_1 x + a_0$$
$$g(x) = b_n x^n + \cdots + b_1 x + b_0$$

se dicen **congruentes módulo** m **polinomio**, *y lo denotamos por*

$$f(x) \equiv_x g(x) \, mod \, m$$

Si $a_i \equiv 0 \; mod \; m$, para $i > n$, y $a_i \equiv b_i \; mod \; m$, y para todo i, $1 \leq i \leq n$.

Ejemplo 7:

$$10x^{13} + 17x^2 + 25x - 6 \equiv_x 2x^2 - 1 \, mod \; 5$$

Vemos con este ejemplo, la importancia de la definición anterior en lo que respecta a la simplificación de las operaciones. Es evidente que el polinomio de la derecha es mucho fácil de manipular que el de la izquierda.

Observación: Si $f(x)$ es un polinomio, entonces la congruencia normal

$$f(x) \equiv 0 \; mod \; p$$

no implica necesariamente que

$$f(x) \equiv_x 0 \, mod \, p.$$

Por ejemplo, si p es un número primo, entonces por el teorema de Fermat se tiene

$$x^p - x \equiv 0 \; mod \; p$$

para todo x entero.

Luego el polinomio $f(x) = x^p - x$ es congruente módulo p al polinomio 0. Si embargo $f(x)$ no es congruente a 0 módulo polinomio, pues los coeficientes de $f(x)$ no son congruentes módulo p a los coeficientes del polinomio 0.

El primer paso que daremos en la resolución de una ecuación del tipo (3.5), será reducir el tamaño del módulo, el cual puede ser un número muy grande. Supongamos que m se factoriza

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

entonces usando el mismo razonamiento empleado en las ecuaciones lineales en el capítulo 2, se tiene el siguiente resultado:

Teorema 3.5.2 *Sea f un polinomio. Entonces toda solución de*

$$f(x) \equiv 0 \; mod \; m \tag{3.6}$$

es solución del sistema

$$\begin{aligned} f(x) &\equiv 0 \; mod \; p_1^{\alpha_1} \\ f(x) &\equiv 0 \; mod \; p_2^{\alpha_1} \\ &\cdots \\ f(x) &\equiv 0 \; mod \; p_s^{\alpha_s} \end{aligned} \tag{3.7}$$

Recíprocamente, toda solución del sistema (3.7) es solución de (3.6).

De acuerdo a este teorema, el problema de resolver congruencias polinomiales, módulo un número compuesto se reduce a resolver congruencias polinomiales módulo potencias de primos.

Ejemplo 8:

Resolver:

$$2x^2 + x - 1 \equiv 0 \, mod \, 20$$

Solución:

De acuerdo al teorema anterior, esta ecuación es equivalente al sistema

$$\begin{aligned} 2x^2 + x - 1 &\equiv 0 \ mod \ 4 \\ 2x^2 + x - 1 &\equiv 0 \ mod \ 5. \end{aligned}$$

Por inspección directa, vemos que las soluciones módulo 20 de la primera y segunda ecuación, son respectivamente:

$$x = 3, 7, 11, 15, 19 \quad \text{y} \quad y = 4, 9, 14, 19$$

Luego la solución de la ecuación original (módulo 20), será la solución común a ambos sistemas, es decir, $x \equiv 19 \ mod \ 20$

Seguidamente, haremos un estudio de la congruencia

$$f(x) \equiv 0 \ mod \ p^{\alpha} \tag{3.8}$$

donde p es primo. Probaremos que esta ecuación se puede resolver cuando se conoce la solución de

$$f(x) \equiv 0 \ mod \ p \tag{3.9}$$

Antes de entrar de lleno en la demostración de esto, necesitamos algunas herramientas del álgebra de polinomios. Supondremos que el lector conoce el concepto de derivada de orden i de una función la cual denotaremos por $f'(x)$.

Teorema 3.5.3 *Sean x e y y números enteros, y f un polinomio de grado n, entonces*

$$f(x+y) = f(x) + \frac{f'(x)}{1!}y + \frac{f''(x)}{2!}y^2 + \cdots + \frac{f^n(x)}{n!}y^n$$

y además los coeficientes $\dfrac{f^i(x)}{i!}$ son todos enteros, $1 \leq i \leq n$.

Demostración:

Observamos en primer lugar que el grado de f es n, y por lo tanto todas las derivadas de órdenes superiores a n, son nulas, y en consecuencia la serie de Taylor es finita. En particular el resto de orden $n+1$ es cero, luego la fórmula anterior es correcta. Solo falta probar que los términos $f^i(x)/i!$ son todos enteros, lo cual probaremos en el caso de ser $f(x) = ax^k$ un monomio (¿Por qué ?).

Luego tenemos

$$\frac{f^i(x)}{i!} = \frac{ak(k-1)(k-2)\cdots(k-i+1)}{1\cdot 2\cdot 3\cdots i}x^{k-i}, \qquad 1 \leq i \leq k.$$

Nótese que

$$\left(\begin{array}{c} k \\ i \end{array}\right) = \frac{k!}{(k-i)!i!} = \frac{k(k-1)\cdots(k-i-1)}{1\cdot 2\cdots i}$$

es un entero, y por lo tanto

$$\frac{f'(x)}{i!} = a\left(\begin{array}{c} k \\ i \end{array}\right)x^{k-i}$$

es también un número entero. ♠

Consideremos ahora el par de congruencias

$$f(x) \equiv 0 \ mod\ p^{\alpha+1} \tag{3.10}$$
$$f(x) \equiv 0 \ mod\ p^{\alpha} \tag{3.11}$$

Sea a una solución de (3.10), entonces necesariamente se sigue que a es solución de (3.11). Luego podemos hacer $a = b + kp^{\alpha}$, donde b es una solución de (3.11), y k es un entero a determinar. Veremos a continuación, que es posible obtener todas las soluciones de (3.10) a partir de las soluciones de (3.11), en la forma indicada, imponiendo ciertas condiciones sobre el entero k.

Teorema 3.5.4 *Sea b solución de (3.11), entonces $b + kp^{\alpha}$ es solución de (3.10), si y sólo si*

$$kf'(b) \equiv -\frac{f(b)}{p^{\alpha}} \, mod \, p \tag{3.12}$$

Demostración:

Usando la fórmula de Taylor tenemos

$$f(b + kp^{\alpha}) = f(b) + \frac{f'(b)kp^{\alpha}}{1} + \cdots \frac{f^{n}(b)(kp^{\alpha})^{n}}{n!}$$

Nótese que los términos

$$\frac{f'(b)}{1}, \frac{f''(b)}{2!}, \cdots, \frac{f^{n}(b)}{n!}$$

son todos enteros, y por lo tanto los términos del lado derecho en la serie de Taylor, son todos enteros. Luego

$$f(b + kp^{\alpha}) \equiv f(b) + f'(b)kp^{\alpha} \, mod \, p^{\alpha+1}$$

Si $b + kp^{\alpha}$ es solución de (3.10), se tendrá:

$$f(b + kp^{\alpha}) \equiv 0 \, mod \, p^{\alpha+1},$$

y por consiguiente

$$f'(b)kp^{\alpha} \equiv f(b) \, mod \, p^{\alpha+1} \tag{3.13}$$

Como b es solución de (3.11) se tiene que:

$$f(b) \equiv 0 \ mod \ p^{\alpha}$$

luego p^{α} divide a $f(b)$ y por lo tanto podemos dividir la ecuación de congruencia (3.13) entre p^{α} para obtener

$$f'(b)k \equiv \frac{f(b)}{p^{\alpha}} \, mod \, p$$

con lo cual queda probado el teorema ♠

A continuación, haremos un estudio detallado de la ecuación de congruencia (3.12), en donde analizaremos los posibles valores de $f'(b)$ módulo p

Teorema 3.5.5 *Sean $a = b + kp^{\alpha}$, como en el teorema 3.5.4. Entonces se presentan dos casos:*

i) Si $f'(b) \equiv 0 \, mod \, p$, a es solución de (3.10) si y sólo si b es solución de (3.11) (no hay restricción sobre k).

ii) Si $f'(b) \not\equiv 0 \ mod \ p$, existe un único valor k para el cual a es solución de (3.10).

Demostración:

Caso I): Si $f'(b) \equiv 0 \ mod \ p$, entonces (3.12) se puede resolver si y sólo si $f(b) \equiv 0 \, mod \, p^{\alpha+1}$, lo cual implica que b es solución de (3.10). El recíproco también es cierto.

Caso II): Si $f'(b) \not\equiv 0 \ mod \ p$ se tiene $(f'(p), p) = 1$ y por lo tanto, $f'(p)$ tiene un inverso bajo el producto módulo p. Sea t este inverso y multipliquemos la ecuación (3.12) por t para obtener

$$k \equiv -\frac{tf(b)}{p^{\alpha}} \, mod \, p.$$

Al evaluar $f(b)$ no debe hacerse la reducción módulo p.

Luego existe un único valor de k módulo p, que hace a a solución de (3.10). ♠

Ejemplo 9:

Resolver:

$$f(x) = x^3 - 2x^2 - 9 \equiv 0 \, mod \, 125 \tag{3.14}$$

Solución:

En primer lugar resolvemos.

$$f(x) = x^3 - 2x^2 - 9 \equiv 0 \; mod \; 5$$

esto es

$$x^3 - 2x^2 + 1 \equiv 0 \; mod \; 5. \tag{3.15}$$

Podemos hallar una solución, si existe, por intermedio de la tabla siguiente:

tabla módulo 5

x	x^2	x^3	$x^3 - 2x^2 + 1$
0	0	0	1
1	1	1	0
2	4	3	1
3	4	2	0
4	1	4	3

Luego las soluciones son $x \equiv 1, 3 \; mod \; 5$
Tomemos $x = 1$ y consideremos aquellas soluciones del tipo

$$a = 1 + 5k \tag{3.16}$$

y veamos cuál de éstos es solución de

$$x^3 - 2x^2 - 9 \equiv 0 \; mod \; 25 \tag{3.17}$$

Para tal fin, calculamos las cantidades involucradas en el teorema anterior

$$f'(x) = 3x^2 - 4x$$

luego

$$f'(1) = 3 - 4 \equiv -1 \equiv 4 \, mod \, 5$$

luego despejamos k de la ecuación

$$f'(1)k \equiv \frac{-f(1)}{p} \, mod \, p,$$

teniendo cuidado que $f(1)$ se calcula de acuerdo (3.14) sin hacer la reducción módulo 5.

Así pues, tenemos

$$4k \equiv \frac{+10}{5} \, mod \, 5$$

o sea

$$4k \equiv +2 \; mod \; 5$$

de donde

$$k = 3.$$

Sustituyendo en (3.16) tenemos que

$$a = 1 + 3 \cdot 5 = 16$$

es la única solución de (3.17) proveniente de $x = 1$.

Repetimos el mismo argumento para la ecuación (3.17), haciendo ahora

$$a = 16 + 25 \cdot k. \tag{3.18}$$

donde k es un nuevo valor a determinar

Nótese que

$$f'(16) = 3(16)^2 - 4(16) = 704 \equiv 4 \, mod \, 5$$

Luego despejamos el valor de k en la ecuación

$$f'(16)k \equiv \frac{-f(16)}{p^2} \, mod \, p,$$

de donde

$$\begin{aligned} 4 \cdot k &\equiv \frac{-3575}{25} \, mod \, 5 \\ &\equiv -143 \, mod \, 5 \\ &\equiv -3 \, mod \, 5 \\ &\equiv 2 \, mod \, 5 \end{aligned}$$

de donde

$$k = 3.$$

Luego

$$a = 16 + 25 \cdot 3 = 91$$

es una solución de (3.14).

Veamos qué sucede si volvemos hacia atrás y tomamos $x = 3$ como solución de (3.15).

Consideremos soluciones del tipo

$$a = 3 + 5 \cdot k$$

Para determinar el valor de k admisible, en la ecuación (3.17) usamos el teorema

$$f'(3) = 3(3)^2 - 4(3) \equiv 15 \equiv 0 \, mod \, 5.$$

Además

$$f(3) = 0 \equiv 0 \, mod \, 25$$

y por lo tanto todos los valores de k son admisibles. Así pues tenemos: x = 3,8,13,18 y 23 soluciones de (3.17).

Podemos repetir el proceso para cada uno de estos valores. Esto se expresa en la siguiente

tabla módulo 5

x	$f(x)$	$f'(x)$	$f(x) \, mod \, 125$	$f'(x) \, mod \, 5$
3	0	15	0	0
8	375	160	0	0
13	1850	455	60	0
18	5175	900	50	0
23	11100	1495	100	0

De acuerdo a la tabla se tiene que $x = 3$ y $x = 8$ aportan nuevas soluciones. Los valores restantes de x: 13, 18 y 23 no generan solución alguna.

Luego

$$3 + 25 \cdot k$$

es solución de (3.14) para todo $k = 0, 1, 2, 3, 4$. Esto genera las 5 soluciones

$$\{3, 28, 53, 78, 103\}$$

Igualmente, se deduce que

$$8 + 25 \cdot k$$

es solución de (3.14) para todo $k = 0, 1, 2, 3, 4$, lo cual genera las soluciones

$$\{8, 33, 58, 83, 108\}$$

Resumiendo entonces, la ecuación (3.14) posee 11 soluciones dadas por

$$\{3, 8, 28, 33, 53, 58, 78, 83, 91, 103, 108\}$$

Ejemplo 10:

Resolver:

$$x^3 - 2x^2 + 2 \equiv 0 \, mod \, 125$$

Solución:

En primer lugar resolvemos

$$x^3 - 2x^2 + 2 \equiv 0 \, mod \, 5$$

Por simple inspección, vemos que no posee solución. Luego la ecuación dada tampoco posee solución.

3.6 Congruencias Módulo Primo

En esta sección se continua con el estudio de las congruencias polinomiales del tipo visto en la sección anterior, pero tomando como módulo un número primo p. Bajo esta condición, se tienen muy buenos resultados, algunos de ellos provenientes del álgebra de los polinomios, como por ejemplo el teorema de Lagrange que establece: Todo polinomio de grado n posee a lo sumo n raíces. Finalmente, haremos un estudio particular de las ecuaciones cuadráticas módulo p.

Teorema 3.6.1 *Sea $f(x)$ un polinomio de grado n, con coeficientes enteros, y sea a un entero cualquiera. Entonces existe un polinomio $q(x)$ con coeficientes enteros, tal que*

$$f(x) = (x-a)q(x) + f(a)$$

y además, grado $(q(x)) = n-1$.

Demostración:

Podemos aplicar la división de polinomios entre $f(x)$ y $x-a$, para obtener

$$f(x) = (x-a)q(x) + r,$$

donde el grado de $r <$grado $(x-a) = 1$.

Por lo tanto grado $r = 0$ y así pues r es una constante, que se puede determinar al sustituir x por a en la ecuación de arriba. Esto nos da

$$f(a) = (a-a)q(a) + r = r.$$

Solo resta probar que q posee coeficientes enteros, lo cual es fácil ver pues en el proceso de división de f entre $x-a$, no es necesario dividir en ningún momento. Para reafirmar lo dicho $q(x)$ se expresa por

$$q(x) = a_n x^{n-1} + (a_{n-1} + aa_n)x^{n-2} + \cdots + (-a_1 x),$$

si

$$f(x) = a_n x^n + \cdots + a_1 x + a_0.$$

Con esto termina la demostración ♠

Ejemplo 11:

Sea

$$f(x) = x^4 - 3x^3 + 2x^2 + 5$$

y $a = 1$.

Luego $f(1) = 5$ y así pues, se tiene

$$f(x) = (x-1)q(x) + 5$$

donde $q(x)$ es el polinomio de grado 3: $q(x) = x^3 - 2x^2$.

Teorema 3.6.2 *(Teorema de Lagrange) Sea p un número primo y sea f un polinomio de grado n $(n \leq p)$ con coeficientes enteros. Entonces la congruencia*

$$f(x) \equiv 0 \, mod \, p \tag{3.19}$$

posee a lo sumo n soluciones distintas.

Demostración:

Sean $r_1, \cdots, r_s$ soluciones distintas módulo p de (3.19). Entonces $f(r_i) \equiv 0 \, mod \, p$, $1 \leq i \leq s$. Por el teorema 3.6.1 existe un polinomio $q_1(x)$ de grado menor n tal que

$$f(x) \equiv (x - r_1)q_1(x) \ mod \ p \tag{3.20}$$

Tomando $x = r_2$ en (3.20) obtenemos

$$0 \equiv f(r_2) \equiv (r_2 - r_1)q_1(r_2) \, mod \, p,$$

y por lo tanto p divide a $(r_2 - r_1)q_1(r_2)$. Como p es primo se tiene que

$$r_2 - r_1 \equiv 0 \, mod \, p, \quad \text{ó} \quad q_1(r_2) \equiv 0 \, mod \, p.$$

Lo primero no puede ocurrir, pues por hipótesis las soluciones r_1, $r_2, \cdots, r_s$ son distintas módulo p y por lo tanto se obtiene

$$q_1(r_2) \equiv 0 \, mod \, p.$$

Por un razonamiento análogo al anterior, se deduce que las restantes $s - 1$ soluciones de (3.19), $r_2, r_3, \cdots r_s$ satisfacen la ecuación

$$q_1(x) \equiv \ 0 \, mod \, p.$$

Como el grado de $q_1(x)$ es menor que n, podemos usar inducción sobre n, para afirmar que $q_1(x)$ posee a lo sumo $n - 1$ raíces.

Luego el conjunto $\{r_2, r_3, \cdots, r_s\}$ posee a lo sumo $n-1$ elementos. Es decir, $s-1 \leq n-1$, lo cual implica que $s \leq n$. ♠

Ejemplo 12:

Resolver la congruencia:

$$12x^{17} + 68x^8 + 393 \equiv 0 \, mod \, 7 \tag{3.21}$$

Solución:

En primer lugar podemos reducir los coeficientes del polinomio dado. Esto es:

$$12x^{17} + 68^8 + 393 \equiv_x 5x^{17} + 5x^8 + 1 \, mod \, 7$$

Luego la ecuación original (3.21) se transforma en

$$5x^{17} + 5x^8 + 1 \equiv 0 \, mod \, 7 \tag{3.22}$$

Observamos que en la ecuación anterior, algunas potencias de x son de grado superior a 7. Es posible simplificar esto también, mediante la utilización del teorema de Fermat, el cual establece:

$$x^6 \equiv 1 \; mod \; 7 \tag{3.23}$$

para todo x.

Usando la ecuación anterior, se puede reducir las potencias de x, de grado mayor que 7. Por ejemplo

$$\begin{gathered} x^7 \equiv x \; mod \; 7 \\ x^8 \equiv x^2 \; mod \; 7 \\ \cdots \\ x^{6k+t} \equiv x^t \, mod \, 7 \end{gathered}$$

para todo entero k, y $1 \leq t \leq 5$.

Luego, (3.22) se transforma en

$$5x^5 + 5x^2 + 1 \equiv 0 \, mod \, 7 \tag{3.24}$$

Podemos eliminar el coeficiente principal 5, multiplicando por el inverso módulo 7 del mismo, el cual es igual 3 (verificarlo!). Haciendo esto nos queda la siguiente ecuación, la cual no admite más simplificación

$$x^5 + x^2 + 3 \equiv 0 \, mod \, 7 \tag{3.25}$$

Por inspección directa, vemos que la única solución es $x = 4$.

3.7 Ecuación Cuadrática

Finalmente, concluimos este capítulo con un estudio detallado de la ecuación polinomial cuadrática módulo un primo p, es decir una ecuación del tipo

$$ax^2 + bx + c \equiv 0 \, mod \, p \tag{3.26}$$

Recordemos que en el caso de las ecuaciones cuadráticas sobre el cuerpo de los números reales se tenía una fórmula explícita para x:

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \tag{3.27}$$

En el cuerpo de los enteros módulo p, podemos hacer muchas operaciones similares a las efectuadas en los números reales, aunque desafortunadamente existen algunas limitaciones. En primer lugar no hemos hablado de "extraer raíces cuadradas módulo p". En segundo lugar si $p = 2$ entonces

$$2a \equiv 0 \; mod \; 2$$

y por lo tanto la fórmula anterior carece de sentido en esta situación.

Podemos solventar este y otros inconvenientes con los elementos que tenemos en nuestras manos, sin necesidad de crear nuevos entes matemáticos.

Se puede tratar el caso $p = 2$ como un caso especial, dentro de la teoría que vamos a desarrollar.

La ecuación

$$ax^2 + bx + c \equiv 0 \, mod \, 2$$

se reduce a uno de los cuatros casos

$$\begin{aligned} x^2 &\equiv 0 \ mod \ 2 \\ x^2 + 1 &\equiv 0 \ mod \ 2 \\ x^2 + x &\equiv 0 \ mod \ 2 \\ x^2 + x + 1 &\equiv 0 \ mod \ 2 \end{aligned}$$

y cada uno de estos casos se pueden resolver por tanteo.

De ahora en adelante, supondremos que p es un primo distinto de 2.

En primer lugar, asumiremos que en la ecuación (3.26) el coeficiente a es primo relativo con p (caso contrario se tendría una ecuación lineal, la cual fue estudiada en el capítulo 2). Por lo tanto se tiene $4a \not\equiv \ 0 \ mod \ p$, y al multiplicar la ecuación (3.26) por $4a$, nos queda la siguiente ecuación:

$$4a^2x^2 + 4abx + 4ac \equiv 0 \, mod \, p$$

o sea

$$(2ax + b)^2 + 4ac - b^2 \equiv 0 \, mod \, p$$

y por lo tanto

$$(2ax + b)^2 \equiv b^2 - 4ac \, mod \, p.$$

Haciendo el cambio de variables

$$2ax + b = X \tag{3.28}$$
$$b^2 - 4ac = B \tag{3.29}$$

se tendrá

$$X^2 \equiv B \ mod \ p \tag{3.30}$$

Obsérvese que si resolvemos la ecuación anterior (3.30) para X, entonces el valor de x se puede hallar en (3.28), pues $(2a, p) = 1$ y por lo tanto la ecuación lineal

$$2ax \equiv X - b \, mod \, p$$

siempre posee solución.

Hemos probado entonces:

Teorema 3.7.1 *Sea p un número primo, $p \neq 2$ entonces, toda ecuación cuadrática*

$$ax^2 + bx + c \equiv 0 \, mod \, p$$

es equivalente a una del tipo

$$X^2 \equiv b^2 - 4ac \, mod \, p,$$

donde $B \equiv b^2 - 4ac \, mod \, p$

Observación: En el capítulo 4, nos dedicaremos a estudiar en detalle las ecuaciones cuadráticas del tipo $x^2 \equiv b \ mod \ p$ con $(b, p) = 1$, con p un primo. Si esta ecuación posee solución, entonces diremos que b es un resto cuadrático módulo p

Ejemplo 13:

Resolver:

$$3x^2 + 2x - 1 \equiv 0 \, mod \, 7 \tag{3.31}$$

Solución:

En primer lugar, resolvemos

$$X^2 \equiv b^2 - 4ac \, mod \, p$$

esto es

$$\begin{aligned} X^2 &\equiv 4 - 4(3)(-1) \, mod \, 7 \\ X^2 &\equiv 2 \, mod \, 7 \end{aligned} \tag{3.32}$$

A fin de resolver la ecuación anterior, examinamos todos los posibles restos cuadráticos módulo 7, mediante una tabla. Esto nos da las soluciones $X = 3$ y $X = 4$. Resolvemos ahora el cambio de variable

$$2ax + b \equiv X \, mod \, p,$$

para cada valor de X independientemente. Haciendo esto obtenemos

i)$X = 3$

$$6x + 2 \equiv 3 \; mod \; 7,$$

lo cual nos da

$$x \equiv 6 \; mod \; 7$$

ii)$X = 4$

$$6x + 2 \equiv 4 \; mod \; 7,$$

lo que produce

$$x \equiv 5 \; mod \; 7$$

Claramente estas son las soluciones, únicas módulo 7, de la ecuación original (3.31).

Ejercicios

1) Sea $f(x) = 25x^4 + 36^2 - 163x + 2$. Hallar un polinomio $g(x)$ con coeficientes mínimos tal que

$$g(x) \equiv_x f(x) \, mod \, m,$$

para $m = 5, 10$ y 12.

2) Demuestre que $x^7 \equiv x \ mod \ 7$ para todo x, pero sin embargo, no se tiene $x^7 \equiv_x x \, mod \, 7$.

3) Sea $f(x)$ un polinomio de grado n, tal que

$$f(1) \equiv f(2) \equiv \cdots \equiv f(n+1) \equiv 0 \ mod \, p$$

Probar que $f(x) \equiv 0 \ mod \ p$, para todo x.

4) Probar que lo anterior no se cumple, en general, si p no es primo.

5) Resolver las ecuaciones

a)$x^2 + 15x - 6 \equiv 0 \ mod \ 25$

b)$x^2 + 2x - 15 \equiv 0 \ mod \ 8$

c)$x^3 - 7x^2 + 6 \equiv 0 \ mod \ 27$

6) Aplicando el método de división sintética, hallar el cociente y el resto de dividir

$$(x^4 + 5x^3 - 9x + 16)/(x - 6)$$

7) Resolver las congruencias

a)$2x^2 + x - 1 \equiv 0 \ mod \ 13$

b)$x^2 - 3x + 6 \equiv 0 \ mod \ 7$

c)$5x^2 + 2x - 1 \equiv 0 \ mod \ 11$

8) Demostrar que si x_1 es solución de la congruencia

$$a_n x^n + \cdots + a_1 x + a_0 \equiv 0 \ mod \ m \qquad (*)$$

y si b es otro entero, $b \equiv x_1 \ mod \ m$, entonces b es también solución de la congruencia $(*)$.

9) Resuelva las ecuaciones

a)$6x^2 + 3x - 5 \equiv 0 \ mod \ 21$

b)$9x^3 + 14x^2 - 5x \equiv 0 \ mod \ 15$

10) Reducir los siguientes polinomios

a) $27x^4 + 25x^2 - 31x \, mod \, 3$

b) $71x^{113} + 44x^{22} - x - 102 \, mod \, 11$

11) Resolver:

a)$x^3 + 3x^2 + 3x \equiv 0 \ mod \ 7$

b)$x^3 + 3x^2 + 3x \equiv 0 \ mod \ 11$

c)$127x^8 + 6x - 78 \equiv 0 \ mod \ 5$

d)$x^4 + x^3 + x^2 + x + 1 \equiv 0 \ mod \ 5$

12) Probar el teorema 3.5.2 en el caso $m = pq, p$ y q dos primos distintos.

13) Probar que si B es el número de soluciones de la congruencia

$$f(x) \equiv 0 \ mod \ p^\alpha$$

se tiene que $p|B$.

14) Hallar mediante tablas, todos los restos cuadráticos módulo p, para $p = 5, 7, 11$ y 13.

15) Demuestre que en $\mathbb{Z}_p$, el número de restos cuadráticos es igual al número de restos no cuadráticos. Halle una fórmula para calcular el número de restos cuadráticos módulo p.

16) Resuelva:

a)$x^2 + x + 1 \equiv 0 \ mod \ 2$

b)$x^2 + x \equiv 0 \ mod \ 2$

c)$x^2 + 1 \equiv 0 \ mod \ p$

17) Resolver:

$$3x^{16} + 128x^{10} + 640 \equiv 0 \; mod \; 9$$

18) Factorizar $x^5 - x$ en $\mathbb{Z}_5$ *Ayuda* : Usar el teorema de Fermat.

19) Factorizar $x^4 - 3x^2 + 2x - 1$ en $\mathbb{Z}_2$.

20) Demuestre que si $f(x)$ se puede factorizar de la forma $g(x)h(x)$ en $\mathbb{Z}[x]$, entonces admite la misma factorización en $\mathbb{Z}_p[x]$, para todo p primo. Usando lo anterior, probar $x^2 - 25x + 1$ es irreducible. *Ayuda* : Probar el caso $p = 2$