Lista Vacacional Teoría de Números

Myriam Hernández Ketchul

22 de Diciembre de 2018

1. Teorema Chino del Residuo

Teorema 1.1 Si $mcd(a, m) = 1$ entonces existe un x tal que $ax \equiv 1(\text{mód } m)$. Cualesquiera dos de esos x son congruentes módulo m. Si $(a, m) > 1$ entonces no existe dicho x.

Demostración Si $(a, m) = 1$, entonces existen x, y tales que $ax + my = 1$. Esto es, $ax \equiv 1(\text{mód } m)$. Por otro lado, si $ax \equiv 1(\text{mód } m)$, se sigue que existe y tal que $ax + my = 1$, así $mcd(a, m) = 1$. Además si $ax_i \equiv ax_2 \equiv 1(\text{mód } m)$, ya que $mcd(a, m) = 1$, se tiene que $x_1 \equiv x_2(\text{mód } m)$■

Teorema 1.2 Sean $m_1, m_2, m_3, ..., m_r,\ r$ enteros poitivos primos relativos por parejas. Entonces el siguiente sistema de congruencias tiene soluciones comunes. Si x_0 es una de esas soluciones, entonces el entero x es solución si y sólo si x es de la forma $x = x_0 + km$ para algún entero k. Donde $m = m_1 m_2 \cdots m_r$.

$$\begin{aligned} x &\equiv a_1(\text{mód } m_1) \\ x &\equiv a_2(\text{mód } m_2) \\ &\vdots \\ x &\equiv a_r(\text{mód } m_r) \end{aligned}$$

Demostración Escribimos $m = m_1 m_2 \cdots m_r$, notemos que m/m_j es entero y que $mcd(m/m_j, m_j) = 1$. Por el Teorema 1.1 para cada j existe un entero b_j tal que $(m/m_j)b_j \equiv 1(\text{mód } m_j)$. Claramente $(m/m_j)b_j \equiv 0(\text{mód } m_i)$ si $i \neq j$. Hacemos

$$x_0 = \sum_{j=1}^{r} \frac{m}{m_j} b_j a_j. \tag{1}$$

Consideramos este número módulo m_i, y tenemos que

$$x_0 \equiv \frac{m}{m_i} a_i b_i \equiv a_i(\text{mód } m_i)$$

Así x_0 es solución del sistema de congruencias.
Si x_0 y x_1 son dos soluciones del sistema, entonces $x_0 \equiv x_1(\text{mód } m_i)$ para $i = 1, 2, ..., r$, de esta forma $x_0 \equiv x_1(\text{mód } m)$, completando la prueba■

Es importante recalcar que esta demostración, además de demostrar la existencia de la solución te da un algoritmo para la construcción de la misma. Haciendo que sea más sencillo encontrarla. Aquí hay un ejemplo de como hacerlo.

Ejemplo 1 Encuentra el menor entero positivo x tal que $x \equiv 5(\text{mód } 7)$, $x \equiv 7(\text{mód } 11)$, y $x \equiv 3(\text{mód } 13)$.

Solución Siguiendo la demostración del teorema, tomamos $a_1 = 5, a_2 = 7, a_3 = 3, m_1 = 7, m_2 = 11, m_3 = 13$ y $m = 7 \cdot 11 \cdot 13 = 1001$. Ahora $\text{mcd}(m_2m_3, m_1) = 1$, y por el algoritmo de Euclides tenemos que $(-2) \cdot m_2m_3 + 41 \cdot m_1 = 1$, así tomamos $b_1 = -2$. Similarmente, encontramos que $4 \cdot m_1m_3 + (-33) \cdot m_2 = 1$, así $b_2 = 4$. Por el algoritmo de Euclides aplicado una tercera vez encontramos que $(-1) \cdot m_1m_2 + 6 \cdot m_3 = 1$, así tomamos $b_3 = -1$. Entonces por (1) tenemos que $11 \cdot 13 \cdot (-2) \cdot 5 + 7 \cdot 13 \cdot 4 \cdot 7 + 7 \cdot 11 \cdot (-1) \cdot 3 = 887$ es una solución. Como esta solución es única módulo m, esta es la única solución entre los números $1, 2, ..., 1001$. Así 887 es el menor entero positivo■

La hipótesis de que los m_j sean primos relativos por pares es escencial. Cuando esta hipótesis falla, no se puede asegurar la existencia de la solución x del sistema, si existe, esta será única módulo $\text{mcm}[m_1, m_2, ..., m_r]$, no módulo m. Si el sistema no tiene solución, decimos que es *inconsistente*.

Ejemplo 2 Demuestra que no existe solución para el sistema $x \equiv 29(\text{mód } 52)$ y $x \equiv 19(\text{mód } 72)$.

Solución Como $52 = 4 \cdot 13$, entonces $x \equiv 29(\text{mód } 4)$ y $x \equiv 29(\text{mód } 13)$ simultáneamente, lo que se reduce a $x \equiv 1(\text{mód } 4)$ y $x \equiv 3(\text{mód } 13)$.
Similarmente, $72 = 8 \cdot 9$, y la segunda congruencia dada es equivalente al sistema simultáneo de congruencias $x \equiv 19(\text{mód } 8)$ y $x \equiv 19(\text{mód } 9)$. Esto se reduce a $x \equiv 3(\text{mód } 8)$, $x \equiv 1(\text{mód } 9)$. Las congruencias dadas son inconsistentes ya que no existe x tal que $x \equiv 1(\text{mód } 4)$ y $x \equiv 3(\text{mód } 8)$.

1.1. Problemas

1. Determina si el sistema $x \equiv 3(\text{mód } 10)$, $x \equiv 8(\text{mód } 15)$, $x \equiv 5(\text{mód } 84)$ tiene solución, encuentrálas todas, si existen.

2. Encuentra el menor entero positivo tal que deje residuos 1, 2, 3, 4, y 5 cuando lo divides entre 3, 5, 7, 9, y 11, respectivamente.

3. Determina si las congruencias $5x \equiv 1(\text{mód } 6)$, $4x \equiv 13(\text{mód } 15)$ tienen una solución común, y en caso afirmativo, encuéntralas todas.

4. Sean $m_1, m_2, ..., m_r$ son primos relativos por pares. Asumiendo que cada una de las congruencias $b_ix \equiv a_i(\text{mód } m_i)$, $i = 1, 2, ..., r$, tiene solución, demuestra que las congruencias tienen una solución común.

5. Sean m_1 y m_2 dos enteros positivos arbitrarios, y sean a_1 y a_2 enteros arbitrario. Muestra que existe una solución simultánea para las congruencias $x \equiv a_1(\text{mód } m_1)$, $x \equiv a_2(\text{mód } m_2)$, si y sólo si $a_1 \equiv a_2(\text{mód } g)$, donde $g = mcd(m_1, m_2)$. Muestra que si se cumple esta condición, entonces la solución es única módulo $\text{mcm}[m_1, m_2]$.

6. * Sea p un número primo, y supón que $m_j = p^{\alpha_j}$ en el sistema de congruencias del enunciado del teorema, donde $1 \leq \alpha_1 \leq \alpha_2 \leq ... \leq \alpha_r$. Muestra que el sistema tiene una solución simultánea si y sólo si $a_i \equiv a_r(\text{mód } p^{\alpha_r})$ para $i = 1, 2, ..., r$.

2. Órdenes

Definición Dado un número entero a y un entero positivo n coprimo con a (es decir, tal que $\text{mcd}(a, n) = 1$), el órden multiplicativo de a módulo n es el menor entero positivo k que cumple

$$a^k \equiv 1(\text{mód } n) \tag{2}$$

El órden de $a(\text{mód } n)$se suele denotar $\text{ord}_n(a)$, o bien $O_n(a)$.
Por ejemplo el órden de 2 módulo 5, $O_5(2) = 4$, ya que $2^4 = 16 \equiv 1(\text{mód } 5)$.

Lema 2.1 Si a tiene órden h módulo n, entonces los enteros tales que $a^k \equiv 1(\text{mód } n)$ son aquellos tales que $h \mid k$.

Corolario 2.2 Sea n un entero positivo, para todo entero a se tiene que $\text{ord}_n(a) \mid (n-1)$.

Corolario 2.3 Si $(a, n) = 1$, entonces el órden de a módulo n divide a $\phi(n)$.

Lema 2.4 Si a tiene órden h módulo n, entonces a^k tiene órden $h/(h, k)$ módulo n.
Demostración Por el Lema 2.1, $(a^k)^j \equiv 1(\text{mód } n)$ si y sólo si $h \mid kj$. Pero $h \mid kj$ si y sólo si $\{h/(h, k)\} \mid \{k/(h, k)\}j$. Como el divisor es primo relativo con el primer factor del dividendo, esta relación se cumple si y sólo si $\{h/(h, k)\} \mid j$. Entonces el menor entero positivo j tal que $(a^k)^j \equiv 1(\text{mód } n)$ es $j = h/(h, k)$■

Lema 2.5 Si a tiene órden $h(\text{mód } n)$, b tiene órden $k(\text{mód } n)$, y si $(h, k) = 1$, entonces ab tiene órden $hk(\text{mód } n)$.
Demostración Sea r el órden de $ab(\text{mód } n)$. Ya mostramos que $r \mid hk$. Para completar la prueba basta demostrar que $hk \mid r$. Notemos que $b^{rh} \equiv (a^h)^r b^{rh} = (ab)^{rh} \equiv 1(\text{mód } n)$. Entonces $k \mid rh$, por el Lema 2.1. Como $(h, k) = 1$, se sigue que $k \mid r$. Por un argumento similar, podemos demostrar que $h \mid r$. Usando nuevamente la hipótesis $(h, k) = 1$, concluimos que $hk \mid r_b lacksquare$

Definición Si g tiene órden $\phi(m)(\text{mód } m)$, entonces g es llamada raiz primitiva módulo m.

2.1. Problemas

1. Demuestra el Lema 2.1.

2. Encuentra una raiz primitiva de los primos 3, 7, 5, 11, y 13.

3. Sea p un primo impar. Prueba que a tiene órden $2(\text{mód } p)$ si y sólo si $a \equiv -1(\text{mód } p)$.

4. Si a tiene órden $h(\text{mód } m)$, prueba que ningún par de $a, a^1, a^2, ..., a^h$ tienen la misma congruencia módulo m.

5. Si p es un primo impar, Â¿Cuántas soluciones hay para $x^{p-1} \equiv 1(\text{mód p})$ y para $x^{p-1} \equiv 2(\text{mód p})$?

3. Residuos Cuadráticos

Definición Para todo a tal que $(a, m) = 1$, a es llamado residuo cuadrático módulo m si la congruencia $x^2 \equiv a(\text{mód } m)$ tiene solución.

Definición Si p denota un primo impar, entonces el *Símbolo de Legendre* $\left(\frac{a}{p}\right)$ es definido como 1 si a es un residuo cuadrático, -1 si no es residuo cuadrático módulo p, y 0 si $p \mid a$.

Teorema 3.1 Sea p un primo impar. Entonces

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}(\text{mód } p)$.
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.
3. $a \equiv b(\text{mód } p)$ implica que $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
4. Si $(a, p) = 1$ entonces $\left(\frac{a^2}{p}\right) = 1$, $\left(\frac{a^2 b}{p}\right) = \left(\frac{b}{p}\right)$.
5. $\left(\frac{1}{p}\right) = 1, \left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Demostración Si $p \mid a$, entonces (1) es claro. Si $(a, p) = 1$ entonces (1) se sigue del criterio de Euler. Las demás partes son consecuencia de (1).
La parte 1, también puede ser probada sin usar el criterio de Euler, como sigue: Si $\left(\frac{a}{p}\right) = 1$, entonces $x^2 \equiv a(\text{mód } p)$ tiene una solución, digamos x_0. Entonces, por la congruencia de Fermat, $a^{(p-1)/2} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right)(\text{mód } p)$. Por otro lado, si $\left(\frac{a}{p}\right) = -1$, entonces $x^2 \equiv a(\text{mód } p)$ no tiene solución, y procedemos como la demostración del teorema de Wilson.
Para cada j que satisface $1 \leq j < p$, elegimos $j', 1 \leq j' < p$, tal que $jj' \equiv a(\text{mód } p)$. Emparejamos j con j'. Notamos que $j \not\equiv j'(\text{mód } p)$, porque la congruencia $x^2 \equiv a(\text{mód } p)$ no tiene solución. La combinación de la contribución de j con j' en $(p-1)!$ es $jj' \equiv a(\text{mód } p)$. Como hay $(p-1)/2$ pares j, j', se sigue que $a^{(p-1)/2} \equiv (p-1)!\ (\text{mód } p)$, y por el teorema de Wilson se demuestra (1).
La última parte del teorema se sigue inmediatamente de la primera■

Teorema (Lema de Gauss) Para todo primo impar p sea $(a, p) = 1$. Consideramos los enteros $a, 2a, 3a, ..., \{(p-1)/2\}a$ y sus menores residuos positivos módulo p. Si n denota el número de residuos que exceden $\frac{p}{2}$, entonces $\left(\frac{a}{p}\right) = (-1)^n$.

Demostración Sean $r_1, r_2, ..., r_n$ denotan los residuos que exceden $p/2$, y sean $s_1, s_2, ..., s_k$ los demás residuos. Los r_i y s_i son todos distintos, y ninguno es cero. Más aún, $n + k = (p-1)/2$. Ahora $0 < p - r_i < p/2, i = 1, 2, ..., n$, y los números $p - r_i$ son distintos. Además ningún $p - r_i$ es un s_j, si lo fuera entonces $p - r_i = s_j$ implica $r_i \equiv \rho a$, $s_j \equiv \sigma a(\text{mód } p)$ para algúnos $\rho, \sigma; 1 \leq \rho \leq (p-1)/2$; $1 \leq \sigma \leq (p-1)/2$, y $p - \rho a \equiv \sigma a(\text{mód } p)$. Ya que $(a, p) = 1$ esto implica $a(\rho + \sigma) \equiv 0, \rho + \sigma \equiv 0(\text{mód}$

p), lo cual es imposible. Ya que $p-r_1, p-r_2, ...p-r_n, s_1, s_2, ..., s_k$ son todos distintos, son al menos 1 y menores que $p/2$, y son $n+k=(p-1)/2$ en número. Esto implica que son los enteros $1, 2, ..., (p-1)/2$ en algún órden. Multiplicándolos todos juntos tenemos

$$(p-r_1)(p-r_2)\cdots(p-r_n)s_1s_2\cdots s_k = 1\cdot 2\cdots\frac{p-1}{2}$$

y así

$$\begin{aligned}(-r_1)(-r_2)\cdots(-r_n)s_1s_2\cdots s_k &\equiv 1\cdot 2\cdots\frac{p-1}{2}(\text{ mód } p)\\ (-1)^n r_1r_2\cdots r_ns_1s_2\cdots s_k &\equiv 1\cdot 2\cdots\frac{p-1}{2}(\text{ mód } p)\\ (-1)^n a\cdot 2a\cdot 3a\cdots\frac{p-1}{2}a &\equiv 1\cdot 2\cdots\frac{p-1}{2}(\text{ mód } p)\end{aligned}$$

cancelamos los factores $2, 3, \cdots, (p-1)/2$ para obtener $(-1)^n a^{(p-1)/2} \equiv 1(\text{mód } p)$ lo que nos da $(-1)^n \equiv a^{(p-1)/2} \equiv \left(\frac{a}{p}\right)(\text{mód } p)$ por Teorema 3.1■

3.1. Problemas

1. Prueba que 3 es residuo cuadrático de 13 pero no lo es de 7.
2. Prueba que los residuos cuadráticos de 11 son 1, 3, 4, 5, 9, y enlista todas las soluciones para cada una de las 10 congruencias $x^2 \equiv a(\text{mód } 11)$ y $x^2 \equiv a(\text{mód } 11^2)$ donde $a = 1, 3, 4, 5, 9$.
3. Enlista los residuos cuadráticos de cada uno de los primos $7, 13, 17, 29, 37$.
4. * Sea p un primo impar. Prueba que toda raiz primitiva de p no es residuo cuadrático. Prueba que todo no residuo cuadrático es una raiz primitiva si y sólo si p es de la forma $2^{2^n}+1$ donde n es un entero no-negativo, esto es, si y sólo si $p=3$ o es un número de Fermat

4. Para leer más

Esta guía fue basada en su mayoría en las secciones 2.3, 2.8, 3.1 del libro *An Introduction to the Theory of Numbers* de Ivan Niven. Puedes revisarlo para mayores detalles y más ejercicios. Si gustas que te envie la versión digital en inglés envíame un correo a myriam.hernandez@cimat.mx.