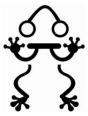

Entrenamiento Final Teoría de Números
Día 1
Olimpiada Mexicana de Matemáticas en Gto.
18 de agosto de 2019

CIMAT

1. Repaso de Congruencias

Teorema .1. *Sea f un polinomio con coeficientes enteros. Si $a \equiv b \mod m$ entonces $f(a) \equiv f(b) \mod m$.*

Teorema .2. ***SUPER IMPORTANTE***

1. *$ax \equiv ay \mod m$ si y solo si $x \equiv y \mod \frac{m}{(a,m)}$.*
2. *Si $ax \equiv ay \mod m$ y $(a,m) = 1$, entonces $x \equiv y \mod m$.*
3. *$x \equiv y \mod m_i$ para $i = 1, \ldots, r$ si y solo si $x \equiv y \mod [m_1, m_2, \ldots, m_r]$.*

Teorema .3. *Sean $(a,m) = 1$ y $r_1, r_2, \ldots, r_n$ un sistema completo o reducido de residuos módulo m. Entonces $ar_1, ar_2, \ldots, ar_n$ es un sistema completo o reducido de residuos módulo m.*

Lema .4. *Sea p un primo, entonces $x^2 \equiv -1 \mod p$ tiene solución si y solo si $p = 2$ o $p \equiv 1 \mod 4$.*

Lema .5. *Si p es un número primo y $p \equiv 1 \mod 4$, entonces existen enteros positivos a, b tales que $a^2 + b^2 = p$.*

Definición .6. Sea $r_1, \ldots, r_n$ un sistema completo de residuos módulo m. El número de soluciones de $f(x) \equiv 0 \mod m$ es el número de r_i tales que $f(r_i) \equiv 0 \mod m$.

Definición .7. Sea $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Si $a_n \not\equiv 0 \mod m$ el grado de la congruencia $f(x) \equiv 0 \mod m$ es n. Si $a_n \equiv 0 \mod m$, sea j el mayor entero tal que $a_j \not\equiv 0 \mod m$, entonces el grado de la congruencia es j. Si todos los coeficientes son múltiplos de m, la congruencia no tiene grado asignado.

Teorema .8. *Si $d \mid m$, $d > 0$, y u es una solución de $f(x) \equiv 0 \mod m$, entonces u es solución de $f(x) \equiv 0 \mod d$.*

Teorema .9. *La congruencia $f(x) \equiv 0 \mod p$ de grado n con coeficiente $a_n = 1$, tiene n soluciones si y solo si $f(x)$ tiene un factor $x^p - x$ módulo p, esto es, si y solo si $x^p - x = f(x)q(x) + ps(x)$ donde $q(x), s(x)$ tienen coeficientes enteros, $q(x)$ tiene grado $p-n$ y es mónico, y ya sea que $s(x)$ es un polinomio de grado menor a n o es 0.*

Corolario .10. *Si $d \mid (p-1)$, entonces $x^d \equiv 1 \mod p$ tiene d soluciones.*

CIMAT

1.1. Problemas

1. Demuestra que 38 no es divisor de $8n^2 + 8$ para ningún entero n.
2. Demuestra que $\frac{1}{5}n^5 + \frac{1}{3}n^3 + \frac{7}{15}n$ es entero para todo entero n.
3. Muestra que para todo primo p, si $a^p \equiv b^p \mod p$, entonces $a^p \equiv b^p \mod p^2$.
4. Si $f(x) \equiv 0 \mod m$ tiene exactamente j soluciones con p un primo, y $g(x) \equiv 0 \mod m$ no tiene soluciones, demuestra que $f(x)g(x) \equiv 0 \mod p$ tiene exactamente j soluciones.
5. Muestra que la congruencia $x^2 \equiv 1 \mod 2^\alpha$ tiene una solución cuando $\alpha = 1$, dos soluciones cuando $\alpha = 2$ y las cuatro soluciones $1, 2^{\alpha-1} - 1, 2^{\alpha-1} + 1, -1$ cuando $\alpha \geq 3$.
6. Muestra que $x^14 + 12x^2 \equiv 0 \mod 13$ tiene 13 soluciones.
7. **Teorema.** Sea $f(x)$ un polinomio fijo con coeficientes enteros, para cualquier entero positivo m denotamos $N(m)$ como el número de las soluciones de $f(x) \equiv 0 \mod m$. Si $m = m_1 m_2$ donde $(m_1, m_2) = 1$, entonces $N(m) = N(m_1)N(m_2)$. Si $m = \Pi p^\alpha$ es la factorización canónica de m entonces $N(m) = \Pi N(p^\alpha)$.
8. Resuelve la congruencia $x^3 - 9x^2 + 23x - 15 \equiv 0 \mod 503$.
9. Prueba que para un entero fijo n la ecuación $\phi(x) = n$ tiene un número finito de soluciones.
10. Encuentra todos los enteros positivos n tales que $\phi(2n) = \phi(n)$.
11. Demuestra la generalización del teorema de Euler:

$$a^m \equiv a^{m-\phi(m)} \mod m$$

para todo entero a.

12. Demuestra que si los últimos dos dígitos de un entero positivo son 33 entonces hay un primo mayor a 7 que lo divide.
13. Resuelve el siguiente sistema de ecuaciones:

$$x^2 + 2x + 5 \equiv 0 \mod 65$$
$$3^{2x} + 2(3^x) + 5 \equiv 0 \mod 65$$

CIMAT

Para entretenerse

1. (IMO Shortlist 2002) Sean $p_1, p_2, \ldots, p_n$ primos distintos mayores a 3. Demuestra que $2^{p_1 p_{2^n}} + 1$ tiene al menos 4^n divisores.

2. (IMO Shortlist 2002) Encuentra todos los pares de enteros positivos $m, n \geq 3$ para los cuales existe infinitos enteros positivos a tales que

$$\frac{a^m + a - 1}{a^n + a^2 - 1}$$

es entero.

3. (IMO Shortlist 2007) Para todos los enteros positivos n, demuestra que existe un entero positivo m tal que n divide a $2^m + m$

4. (IMO Shortlist 2011) Dado cualquier conjunto $A = \{a_1, a_2, a_3, a_4\}$ de cuatro enteros positivos distintos, denotamos $s_4 = a_1 + a_2 + a_3 + a_4$. Sea n_4 el número de pares (i, j) con $1 \leq i < j \leq 4$ para los cuales $a_i + a_j$ divide a s_4. Encuentra todos los conjuntos A de cuatro enteros positivos distintos para los cuales se alcanza el máximo valor de n_4.

5. (Chinese Mathematical Olympiad 2003) Determina el tamaño máximo del conjunto S tal que:

   - Todos los elementos de S son números naturales no mayores a 100.
   - Para cualesquiera dos elementos a, b en S, existe $c \in S$ tal que $(a, c) = (b, c) = 1$.
   - Para cualesquiera dos elementos $a, b \in S$, existe $d \in S$ tal que $(a, d) > 1, (b, d) > 1$.

6. (Olimpiada de Moscú) Demuestra que si $\frac{2^n - 2}{n}$ es un entero, entonces $\frac{2^{2^n - 1} - 2}{2^n - 1}$ también es un entero.

Entrenamiento Final Teoría de Números
Día 2
Olimpiada Mexicana de Matemáticas en Gto.
19 de agosto de 2019

CIMAT

Fuente: Capítulo 2:Introducción a la Teoría de Números de Niven, Zuckerman, Montgomery

1. Órdenes

Definición .1. Sean m un entero positivo y a cualquier entero tal que $(m, a) = 1$. Sea h el menor entero positivo tal que $a^h \equiv 1(\mod m)$. Decimos que el orden de a módulo m es h, o que a pertenece al exponente h módulo m.

Lema .2. *Si a tiene orden h módulo m, entonces los enteros positivos k tales que $a^k \equiv 1(\mod m)$ son precisamente para los cuales $h \mid k$.*

Corolario .3. *Si $(a, m) = 1$, entonces el orden de a módulo m divide a $\phi(m)$.*

Lema .4. *Si a tiene orden h módulo m, entonces a^k tiene orden $h/(h, k)$.*

Lema .5. *Si a tiene orden $h(\mod m)$, b tiene orden $k(\mod m)$, y si $(h, k) = 1$, entonces ab tiene orden $hk(\mod m)$.*

1.1. Problemas

1. Sea p un primo impar, demuestra que a pertenece al exponente 2 módulo p si y solo si $a \equiv -1(\mod p)$.

2. Si h es el orden de $a(\mod m)$, prueba que no hay dos elementos de $a, a^2, ..., a^h$ que sean congruentes módulo m.

3. Supón que $a \in \mathbb{Z}$ tiene orden $h(\mod p)$, muestra que el inverso multiplicativo de a módulo p también tiene orden $h(\mod p)$.

2. Raíces Primitivas

Definición .6. Si g tiene orden $\phi(m)(\mod m)$, entonces g es llamada raíz primitiva módulo m

Lema .7. *Sean p y q números primos, y supón que $q^\alpha \mid (p-1)$, donde $\alpha \geq 1$. Entonces existen precisamente $q^\alpha - q^{\alpha-1}$ clases de residuos $a(\mod p)$ de orden q^α.*

Teorema .8. *Si p es primo entonces existen $\phi(p-1)$ raíces primitivas módulo p.*

Definición .9. Si $(a, p) = 1$ y $x^n \equiv a(\mod p)$ tiene solución, entonces a es llamado residuo n-potencia módulo p. (n-th power residue)

Teorema .10. *Si p es un número primo y $(a,p)=1$, entonces la congruencia $x^n \equiv a(\mod p)$ tiene $(n,p-1)$ soluciones o no soluciones dependiendo si*

$$a^{(p-1)/(n,p-1)} \equiv 1(\mod p)$$

o no.

Corolario .11. ***Criterio de Euler*** *Si p es un número primo impar y $(a,p)=1$, entonces $x^2 \equiv a(\mod p)$ tiene dos o ninguna solución dependiendo si $a^{(p-1)/2} \equiv 1$ o $\equiv -1(\mod p)$.*

Teorema .12. *Si p es primo entonces existen $\phi(\phi(p^2)) = (p-1)\phi(p-1)$ raíces primitivas módulo p^2.*

Teorema .13. *Existe una raíz primitiva módulo m si y solo si $m = 1, 2, 4, p^\alpha, 2p^\alpha$, donde p es un primo impar.*

2.1. Problemas

1. *Demuestra que si p es un primo y g es una raíz primitiva módulo p^2, entonces g es raíz primitiva módulo p^α para $\alpha = 3, 4, 5, \ldots$.

2. Determina el número de soluciones de la congruencia $x^4 \equiv 61(\mod 117)$.

3. Muestra que $3^8 \equiv -1(\mod 17)$. Explica por qué esto implica que 3 es una raíz primitiva de 17.

4. Demuestra que si p es primo, $(a,p)=1$ y $(n,p-1)=1$, entonces $x^n \equiv a(\mod p)$ tiene exáctamente una solución.

5. Sean $a, \hat{a} \in \mathbb{Z}$ tales que $a\hat{a} \equiv 1(\mod p)$, para algún primo p. Supón que g es una raíz primitiva $(\mod p)$, y que $a \equiv g^i(\mod p), 0 \leq i < p-1$. Muestra que $\hat{a} \equiv g^{p-1-i}(\mod p)$.

6. Sean m, n enteros positivos. Muestra que $(2^m - 1, 2^n + 1) = 1$ si y solo si es impar.

7. Muestra que si $p \mid \phi(m)$ y $p \not| m$ entonces existe al menos un factor primo q de m tal que $q1(\mod p)$.

8. Supón que $(a,p) = 1$ y que p es un primo tal que $p \equiv 2(\mod 3)$. Muestra que la congruencia $x^3 \equiv a(\mod p)$ tiene una única solución $x \equiv a^{(2p-1)/3}$.