# Funciones aritméticas, Fermat,Euler, Wilson y teorema chino del residuo

Entrenamiento #3 para el nacional
1-4 de Octubre del 2015
Por: Argel

**Resumen**

Bienvenidos sean de nuevo al mágico mundo de la teoría de números, en esta sesión vamos a recordar lo visto con respecto a congruencias y funciones aritméticas, además, les presentaremos una serie de resultados relacionados a congruencias que les pueden ser útiles para realizar diversas demostraciones relacionadas a divisibilidad, también se hará mención de los sistemas de congruencias y un teorema muy importante relacionado a esto, el teorema chino del residuo. Espero que les agrade la lista y mucho éxito.

## 1. Un pequeño repaso

Primero vamos a recapitular lo que se ha visto con respecto a congruencias y funciones aritméticas

### 1.1. Congruencias

Primero, recordemos que

$$a \equiv b \pmod{m} \leftrightarrow m|a-b$$

Luego veamos las propiedades de las congruencias que nos permiten trabajar cuando usamos módulos, considerando que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$

- $a + c \equiv b + d \pmod{m}$
- $ac \equiv bd \pmod{m}$
- $a^k \equiv b^k \pmod{m}$

El caso de la división de las congruencias también es posible, sin embargo, sólo es bajo ciertas condiciones. Siendo $x$ y $m$ coprimos con $ax \equiv bx \pmod{m}$, entonces:

$$a \equiv b \pmod{m}$$

Es importante recordar el significado de una clase, cuando dos números dejan el mismo residuo bajo módulo m, se dice que ambos pertenencen a la misma clase o clase de congruencia bajo módulo m.
A continuación se presenta la notación empleada en los siguientes problemas

- $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$ será el sistema completo de residuos módulo $n$.
- $\mathbb{Z}_n^* = \{d : d \in \mathbb{Z}_n \ y \ mcd(d, n) = 1\}$ será el sistema reducido de residuos módulo $n$.

Para ejemplificar lo anterior vamos a usar módulo 6. En este módulo, el sistema completo y el sistema reducido de residuos son, respectivamente:

$$\mathbb{Z}_6 = \{1, 2, 3, 4, 5\}, \quad \mathbb{Z}_6^* = \{1, 5\}$$

.

## 1.2. El regreso de las funciones aritméticas $\tau, \sigma, \pi, \varphi$

Sea $n$ un número de la forma:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

La función $\tau$ de $n$, representa la cantidad de divisores

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

La función $\sigma$ es la suma de los divisores de $n$

$$\sigma(n) = \left(\frac{p^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\frac{p^{\alpha_2+1} - 1}{p_2 - 1}\right) \cdots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

La función $\pi$ de $n$ permite calcular el producto de los divisores

$$\pi(n) = n^{\frac{\tau(n)}{2}}$$

escrito en notación pi (como la notación sigma pero refiere a una multiplicación) se expresaría como

$$\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$$

La función $\varphi$ de $n$ es la cantidad de números coprimos con $n$ menores que $n$

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

1. Calcula $\varphi(p^n)$, donde $p$ es un primo y $n$ es un entero positivo.
2. Muestra que si $m$ y $n$ son primos relativos, entonces $\varphi(mn) = \varphi(m)\varphi(n)$.(Tip: Considera los sistemas reducidos de residuos bajo módulo $m$ y bajo módulo $n$. Luego, construye al conjunto formado por los elementos $nr + ms$, donde $r$ está en el sistema reducido de residuos módulo $m$ y $s$ está en el otro sistema reducido de residuos.)

# 2. El teorema de Fermat y el principe de fracción mixta

## 2.1. El pequeño teorema de Fermat y otros problemas introductorios

1. (Pequeño teorema de Fermat)
   a) Muestra que si $k$ es un entero tal que $0 < k < p$, entonces $\binom{p}{k}$ es divisible entre p.
   b) Muestra que si $a$ es entero, entonces $(a+1)^p \equiv a^p + 1 \pmod{p}$
   c) Muestra que si $a$ es entero, entonces $a^p \equiv a \pmod{p}$
   d) Muestra que si $a$ es un entero que no es divisible entre p, entonces $a^{p-1} \equiv 1 \pmod{p}$
2. Sean $a$ y $m$ enteros positivos con $(a, m) = 1$.Muestra que los siguientes conjuntos son iguales bajo módulo m:
$$\{a, 2a, 3a, \ldots, (m-1)a\}$$
$$\{1, 2, 3, \ldots, m-1\}$$
3. Sean $a$ y $m$ enteros positivos con $(a, m) = 1$. Muestra que existe un entero $x$ tal que $ax \equiv 1 \pmod{m}$. En este caso, se dice que $x$ es el inverso multiplicativo de $a$ bajo módulo $m$.

## 2.2. El pequeño teorema de Fermat: Otra perspectiva

1. Sea $p$ un número primo y $a$ un entero que no sea divisible entre $p$.

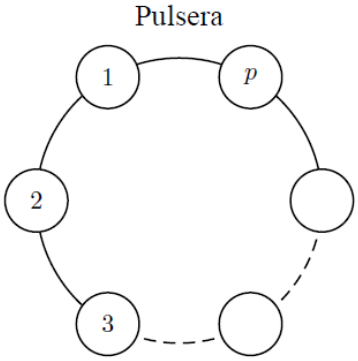
   a) Muestra que $\{a, 2a, 3a, \dots, a(p-1)\} \equiv \{1, 2, 3, \dots, p-1\} \pmod{p}$

   b) Muestra que $a \cdot 2a \cdot 3a \cdot \dots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \dots \cdot (p-1) \pmod{p}$

   c) Concluye que $a^{p-1} \equiv 1 \pmod{p}$

## 2.3. Las artes oscuras: El pequeño teorema de Fermat por combinatoria

Ahora vamos a presentarles una manera de llegar al teorema de Fermat por medio de argumentos de combinatoria.Así es, con combinatoria. Consideremos una cadena con $p$ cuentas con $a$ colores diferentes.




¿De cuántas maneras distintas se puede colorear una cadena con $p$ cuentas con $a$ colores, donde $p$ es un primo y $a \geq 2$?(Las rotaciones se consideran equivalentes mientras que las reflexiones son distintas)

# 3. El teorema de Wilson y las reliquias de la muerte

## 3.1. Teorema de Wilson

Sea $p$ un primo

1. Muestra que los elementos del conjunto de residuos $\{2, 3, \dots, p-2\}$ se pueden agrupar en parejas de inversos multiplicativos.

2. Muestra que $(p-1)! \equiv -1 \pmod{p}$

En el teorema de Wilson también su converso es cierto, es decir:

- Sea $n$ un entero positivo. Muestra que si $(n-1)! \equiv -1 \pmod{n}$, entonces $n$ es primo.

# 4. Eulers mágicos y dónde encontrarlos

## 4.1. El teorema de Euler

Sean $a$ y $m$ primos relativos.

1. Sea $\mathbb{Z}_m^* = \{r_1, r_2, \dots, r_{\varphi(m)}\}$ el conjunto de enteros positivos menores que m que son primos relativos con él. Muestra que

$$\{r_1, r_2, \dots, r_{\varphi(m)}\} \equiv \{ar_1, ar_2, \dots, ar_{\varphi(m)}\} \pmod{m}$$

2. Muestra que $a^{\varphi(m)} \equiv 1 \pmod{m}$

¿Puedes relacionar este resultado con algún otro?

# 5. Las historias del teorema chino el bardo

## 5.1. Sistemas de congruencias

Estoy seguro que en algún momento les ha tocado trabajar con sistemas de ecuaciones, ahora les presentaremos los sistemas de congruencias que pueden resultar útiles en ciertas situaciones. Un ejemplo de un sistema de congruencias podría ser

$$3x \equiv 1 \pmod{7}$$

$$x \equiv 3 \pmod{5}$$

$$2x - 12 \equiv 2 \pmod{9}$$

Una congruencia se puede transformar a un sistema de congruencias, esto considerando a $n$ en su descomposición en primos. Entonces

$$a \equiv b \pmod{n}$$

se puede transformar al sistema de congruencias

$$a \equiv b \pmod{p_1^{\alpha_1}}$$

$$a \equiv b \pmod{p_2^{\alpha_2}}$$

$$\vdots$$

$$a \equiv b \pmod{p_k^{\alpha_k}}$$

¿Y para qué nos pueden servir los sistemas de congruencias?. Un ejemplo, probar que la ecuación $x^2 - 5 = 35y$ no tiene solución para los enteros. Primero nos damos cuenta que el demostrar esto es decir que $x^2 \equiv 5 \pmod{35}$ no tiene solución, consideramos

$$x^2 \equiv 5 \pmod{7}$$

$$x^2 \equiv 5 \pmod{5}$$

Sin embargo, si consideramos la colección de residuos bajo módulo 7 (0,1,2,3,4,5,6) es posible observar que al elevar estos al cuadrado no se puede obtener 5, con esto se ha concluido. ¿Pero cómo se resuelve un sistema de congruencias?, vamos a resolver el sistema de congruencias $2x \equiv 5 \pmod{7}$ y $3x \equiv 4 \pmod{8}$. Simplificamos la primera congruencia a:

$$x \equiv 6 \pmod{7}$$

esto nos indica que $x = 6 + 7t$, sustituyendo en la congruencia siguiente

$$3(6 + 7t) \equiv 4 \pmod{8})$$

$$5t \equiv 2 \pmod{8}$$

$$t \equiv 2 \pmod{8}$$

Lo que implica $t = 2 + 8s$, sustituyendo en $x$

$$x = 6 + 7(2 + 8s) = 20 + 56s$$

Por lo tanto la solución es $x \equiv 20 \pmod{56}$, la solución de un sistema de congruencias es una congruencia.

## 5.2. El teorema chino del residuo

Un teorema importante en los sistemas de congruencias es el teorema chino del residuo.Sea $k$ un entero positivo y supongamos que $n_1, n_2, \ldots, n_k$ son $k$ números naturales primos relativos por parejas(es decir, para cada pareja $(i, j)$ con $i \neq j$ y $1 \leq i,\ j \leq k$ tenemos mcd$(n_i,n_j)$ =1). Sean $b_1, b_2, \ldots, b_k$ enteros cualesquiera. Entonces el sistema

$$\begin{aligned} x &\equiv b_1 \pmod{n_1} \\ x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ x &\equiv b_k \pmod{n_k} \end{aligned}$$

tiene solución y esta es la clase módulo el producto $N = n_1 n_2 \cdots n_k$ del entero $x_0$ que se determina de la siguiente manera: Para $i = 1, 2, \ldots, k$ sea $a_i$ el producto de todos los $n'js$ excluyendo el i-ésimo, es decir $a_i = \frac{N}{n_i}$. Como para cada $i$ se tiene que $mcd(a_i, n_i) = 1$, entonces $a_i$ tiene inverso módulo $n_i$; que denominaremos como $c_i$. Con lo anterior se puede determinar $x_0$:

$$x_0 = a_1 b_1 c_1 + a_2 b_2 c_2 + \cdots + a_k b_k c_k$$

Bueno, quizá sea un poco complicado entender todo esto en un inicio, por eso vamos a ver un ejemplo que sea ilustrativo del uso de este teorema, probablemente todo quedará un poco más claro después de esto. Encuentre las soluciones del sistema de congruencias lineales

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 1 \pmod 4 \\ x &\equiv 3 \pmod 5 \end{aligned}$$

Primero nos damos cuenta que la solución se va a encontrar bajo módulo $3 \cdot 4 \cdot 5 = 60$, para definir cada una de las $a_i$ realizamos las operaciones correspondientes, es decir

$$a_1 = \frac{60}{3} \quad a_2 = \frac{60}{4} \quad a_3 = \frac{60}{5}$$

$$a_1 = 20 \quad a_2 = 15 \quad a_3 = 12$$

Ahora ocupamos encontrar los inversos módulo $n_1$

$$20c_1 \equiv 1 \pmod 3 \quad 15c_2 \equiv 1 \pmod 4 \quad 12c_3 \equiv 1 \pmod 5$$

Pero esto es equivalente a encontrar

$$2c_1 \equiv 1 \pmod 3 \quad 3c_2 \equiv 1 \pmod 4 \quad 2c_3 \equiv 1 \pmod 5$$

De lo anterior se puede ver que $c_1 = 2$, $c_2 = 3$ y $c_3 = 3$, por lo que solo nos hace falta formar $x_0$ con lo que ya obtuvimos

$$x_0 = 20 \cdot 2 \cdot 2 + 15 \cdot 1 \cdot 3 + 12 \cdot 3 \cdot 3 = 233$$

Pero la solución es bajo módulo 60 por ende se puede decir que $x_0 = 53$.

$$x_0 \equiv 53 \pmod{60}$$

Al final el teorema chino del residuo permite hacer la solución de sistemas de congruencias en una cuestión de realizar las operaciones pertinentes.

# 6. Agregados culturales

1. La primera vez que se presentó el teorema chino del residuo fue en uno de los escritos del matemático chino Sun Tzu, aunque no es el mismo que escribió el arte de la guerra
2. Recientes reportes parecen confirmar la existencia de borrecas de limón, otra nueva especia
3. Roy's our boy!
4. En Guadalajara dos de los teatros más importantes son el teatro Degollado y el teatro Diana
5. Fernando al ser un perro robot samurai iluminati no puede encontrar la conexión a la luz.
6. Módulos are here, there and everywhere.
7. Si no conocen la razón de los nombres de los apartados referirse a la lista de funciones aritméticas pasada

# 7. Problemas

1. ¿Qué residuo deja $2^{1000006}$ al dividirse entre 101?
2. Encuentra todos los primos $p$ tales que $p|2^p + 1$.
3. Sea $p$ un primo mayor a 5. Demuestra que $p^8 \equiv 1 \pmod{240}$
4. Sea $n$ un entero mayor a 2. Prueba que entre las fracciones
$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \dots, \frac{n-1}{n}$$
una cantidad par de ellas son irreducibles.
5. Demuestra que $728|a^{27} - a^3$ para todo entero $a$.
6. Si $p$ es un primo, muestra que $x^2 \equiv 1 \pmod{p}$ tiene solución si y sólo si $x \equiv \pm 1 \pmod{p}$.
7. Muestra que $11|5^{2011} - 5$.
8. Sabiendo que $2^{29}$ es un número de nueve dígitos, siendo todos ellos distintos, determine cuál es el dígito que falta sin acudir a calculadoras o computadoras(busca el número del 0 al 9 que no aparece).
9. Si p es un primo, prueba que $(a + b)^p \equiv a^p + b^p \pmod{p}$
10. Demuestra que si $p$ es primo, entonces
$$p|ab^p - ba^p$$
.
11. Si $n$ es un entero y $p$ es un primo, entonces $p|n$ o $p|n^{p-1} - 1$
12. Al mínimo entero positivo $k$ tal que $a^k \equiv 1 \pmod{n}$ se le llama orden de $a$ módulo $n$. Sea $a$ un entero primo relativo con el número natural $n$ y sea $o$ el orden de $a$ módulo $n$. Si $a^k \equiv 1 \pmod{n}$, muestra que $o|k$. Concluye que $o|\varphi(n)$
13. Sean $p$ y $q$ primos distintos. Muestra que para todo entero $a$ se cumple que $a^{pq-p-q+2} \equiv a \pmod{pq}$
14. Sea m un número par positivo. Sean $\{a_1, a_2, \dots, a_m\}$ y $\{b_1, b_2, \dots, b_m\}$ dos sistemas completos de residuos módulo $m$. Prueba que $\{a_1 + b_1, a_2 + b_2, \dots, a_m + b_m\}$ no es un sistema completo de residuos módulo m.

15. Si $p$ es un primo distinto de 2 y de 5, prueba que existe un número entero conformado solamente de dígitos iguales a 1, que es divisible por $p$.

16. Demuestra que si $m$ y $n$ son enteros, entonces $mn(m^{60} - n^{60})$ es divisible por $56,786,730$

17. Demuestra que
$$\frac{\sigma(a)}{a} < \frac{\sigma(ab)}{ab} \leq \frac{\sigma(a)\sigma(b)}{ab}$$

18. Sea $p$ un primo impar. Prueba que $x^2 + 1 \equiv 0 \pmod{p}$ tiene solución si y sólo si $p \equiv 1 \pmod 4$

19. Demuestra que $\tau(2^n - 1) \geq \tau(n)$

20. Demuestra para todo entero $n$ no es posible partir el conjunto $\{n, n+1, n+2, n+3, n+4, n+5\}$ en dos subconjuntos tales que el producto de los miembros de uno sea igual al producto de los miembros del otro.

21. Demuestra que para $n > 1$
$$\sum_{\substack{1 \leq a < n \\ (a,n)=1}} a = \frac{n\varphi(n)}{2}$$

22. Encuentra todas las soluciones de la congruencia $304x^{303} + 204x^{202} - 104x^{101} \equiv 0 \pmod{101}$

23. Demuestra que para todo entero positivo $n$ existen dos enteros positivos $x, y$ tales que $x - y \geq n$ y $\sigma(x^2) = \sigma(y^2)$

24. Resolver el sistema de congruencias
$$2x \equiv 5 \pmod 9$$
$$x - 7 \equiv 9 \pmod{11}$$

25. Demuestra que
$$\sum_{k=1}^{n} \tau(k) = \sum_{j=1}^{n} \left\lfloor \frac{n}{j} \right\rfloor$$

26. Aplicar el teorema Chino del Residuo para resolver el sistema
$$x \equiv 2 \pmod 7$$
$$x \equiv 0 \pmod 9$$
$$x \equiv 4 \pmod{10}$$

27. Dado un número natural $n$, sea $P(n)$ el producto de todos los divisores positivo de $n$. Por ejemplo $P(12) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 12 = 1728$. Encuentra todos los valores de $n$, menores que 400, tales que $n$ tiene sólo dos divisores primos distintos y $P(n) = n^6$.

28. Diecisiete piratas se reparten un botín de $n$ monedas de oro. Acordaron partes iguales y, si hubiere un resto, se lo darían al cocinero chino. Después del reparto el chino recibió3 monedas. Pero en la borrachera nocturna 6 piratas murieron acuchillados – en la riña acostumbrada en esos casos. Al otro día los sobrevivientes se vuelven a repartir las monedas y al cocinero le tocaron 4 monedas. Posteriormente, en un naufragio, sólo se salvó el botín, el cocinero y 6 piratas. Así que se vuelven a repartir y le tocaron 5 monedas al cocinero. Encontrar el número $n$ de monedas con que se quedó el cocinero (como mínimo) después de envenenar a los piratas restantes (después de un delicioso chou main cantonés con pollo).

29. Demuestra que para todo entero positivo $n$ se cumple que

$$\sum_{d|n} \varphi(d) = n$$

30. Sean $m$ y $n$ enteros positivos con $m > 1$. Demuestra que $\phi(m^n - 1)$ es divisible entre $n$ donde $\phi$ es la función de Euler.

31. Determina el número de enteros $n > 1$ que cumplen que $a^{13} - a$ es divisible entre $n$ para todo entero $a$.

32. Determina todos los números primos $p$ tales que $5^p + 4p^4$ es un cuadrado perfecto.

33. ¿Cuál es el máximo común divisor de los números $p^4 - 1$, donde $p$ es un primo mayor que 5?

34. Determine todos los enteros $n$, con $0 \leq n \leq 50$, tales que:

$$1998^n + n^{1998}$$

sea múltiplo de 100.

35. Demuestre que existe un número entero de la forma:

$$999991999991999991 \ldots 999991$$

que es divisible por 1999.

36. Encuentre todos los números primos $p$ y $q$ tales que:

$$\frac{2^p + 2^q}{pq}$$

sea un número entero.

37. Pruebe que la ecuación:

$$a^2 + 2b^2 + 98c^2 = 77777 \ldots 77$$

no tiene soluciones enteras.(con 2006 7's)

38. Determinar todas las soluciones en enteros $x, y$ que satisfacen la ecuación

$$1998^2x^2 + 1997x + 1995 - 1998x^{1988} = 1998y^4 + 1993y^3 - 1991y^{1998} - 2001y$$

39. Muestra que si $a$ y $b$ son enteros positivos y primos relativos, entonces existen enteros $m$ y $n$ tales que $a^m + b^n \equiv 1 \pmod{ab}$

40. Muestra que la ecuación

$$x^5 + y^5 + 1 = (x + 2)^5 + (y - 3)^5$$

no tiene soluciones en enteros.

41. Encuentra el menor entero positivo $n$ tal que

$$2^{2005} | 17^n - 1$$

42. Sean $p, q, r$ números primos positivos distintos. Demostrar que si $pqr|(pq)^r + (qr)^p + (pr)^q - 1$, entonces $(pqr)^3|3((pq)^r + (qr)^p + (pr)^q - 1)$

43. Muestra que si $p$ es un primo impar, entonces el residuo al dividir $(p-1)!$ entre $p(p-1)$ es $p - 1$.

44. Si $p$ es primo, prueba que $p^{p+1} + (p+1)^p$ no es un cuadrado perfecto.

45. Demuestre que para cada entero positivo $n$ existen $n$ enteros positivos consecutivos, ninguno de los cuales es la potencia de un número primo.

46. Muestra que para todo primo $p$, se puede encontrar un entero positivo $n$ tal que

$$2^n + 3^n + 6^n - 1$$

sea divisible por $p$.

47. Demuestre que para todos los enteros positivos $n$ y $k$, existe un conjunto de $n$ enteros consecutivos tal que cada uno de los elementos de este conjunto es divisible por $k$ primos distintos ninguno de los cuales divide a los otros elementos del conjunto

48. Prueba que para todo entero positivo $s$, existe un entero positivo $n$ tal que la suma de sus dígitos es $s$, y además $s|n$

49. Demuestre que para cada entero positivo $n$, existen enteros $a$ y $b$ tales que $4a^2 + 9b^2 - 1$ es divisible entre n.

50. Sea $p$ un número primo. Demuestra que existe un número primo $q$ tal que, para todo entero $n$, el número $n^p - p$ no es divisible por $q$.