Algebra Superior 2

Grupo 4098

Soluciones y Demostraciones

Alumnos:

- Palacios Rodríguez Ricardo Rubén
- Rosas Hernandez Oscar Andres
- José Martín Panting Magaña
- Raúl Leyva Cedillo
- Angel Mariano Guiño Flores
- Gloria Guadalupe Cervantes Vidal
- David Iván Morales Campos
- Aaron Barrera Tellez
- Elias Garcia Alejandro
- Víctor Hugo García Hernández
- Oscar Márquez Esquivel

Profesor:
Leonardo Faustinos Morales

Ayudante:
Jonathan López Ruiz

Lunes 30 de Octubre

1. Ejercicio 1

Muestra un sistema reducido de residuos modulo 7 compuesto solo de potencias en 3

Solución:

Un sistema reducido de residuos módulo 7 sencillo es $Residuos = \{\ 0, 1, 2, 3, 4, 5, 6\ \}$ ahora, podemos decir que:

- $3^0 \equiv 1 \pmod 7$
- $3^2 = 9 \equiv 2 \pmod 7$
- $3^1 \equiv 3 \pmod 7$
- $3^4 = 81 \equiv 4 \pmod 7$
- $3^5 = 243 \equiv 5 \pmod 7$
- $3^3 = 27 \equiv 6 \pmod 7$

Pero... que pasa con el 0, es lo único que nos falta, pero resulta que es imposible encontrar un número tal que $3^n = 7k$ pues 3^n esta formado solo por 3, esta es su factorización prima, por lo tanto será imposible que alguna vez este número sea también divisible entre 7, pues esto significaría que podemos encontrar un 7 en su factorización prima.

2. Ejercicio 2

Probar que $n^{6k} - 1 | 7 \quad \forall k$

Solución:

Vamos a probar que $n^{6k} \equiv 1 \pmod 7$

Basta con ver que $n^6 \equiv 1 \pmod 7$ porque si esto fuera cierto, entonces elevar ese uno a la k seguira siendo uno.

Ve $n^6 \equiv 1 \pmod 7$ se puede demostrar muy facil con el Teorema de Fermat ya que $(n, 7) = 1$ (es decir, no pertenece a la clase de equivalencia del 0 módulo 7) entonces $n^{\phi(7)} \equiv 1 \pmod 7$

3. Ejercicio 3

Probar que $n^2 - a^2$ es divisible entre 91 si n y a son primos relativos con 91

Solución:

Supón que $n = 5$ pues $(91, 5) = 1$ y $(91, 5) = 1$ y que $a = 3$ pues $(91, 3) = 1$ y $(91, 3) = 1$

Pero $5^2 - 3^2$ es 16 y 16 no es divisible entre 91

Probar que $n^{12} - a^{12}$ es divisible entre 91 si n y a son primos relativos con 91

Solución:

Como n y a son primos relativos con 91 (y $91 = 13 * 7$), también son primos relativos con 13 y con 7 por lo tanto obtenemos que:

- $n^{\phi(13)} \equiv 1 \pmod{13}$ y $a^{\phi(13)} \equiv 1 \pmod{13}$
- $n^{\phi(7)} \equiv 1 \pmod{7}$ y $a^{\phi(7)} \equiv 1 \pmod{7}$

Con lo tanto tenemos que $n^6 - a^6 \equiv 0 \pmod{7}$ y si la elevamos al cuadrado tenemos que $n^{12} - a^{12} \equiv 0 \pmod{7}$ es decir $n^{12} - a^{12}$ es un multiplo de 12.

Por otro lado $n^{12} - a^{12} \equiv 0 \pmod{13}$ es decir $n^{12} - a^{12}$ es un multiplo de 13.

Y como es multiplo de ambos de sus factores, tenemos que $n^{12} - a^{12}$ es divisible entre 91

4. Ejercicio 4

Cual es el último digito de 3^{400}

Solución:

Si te das cuenta lo único que te están pidiendo es que $3^{400} \pmod{10}$ ahora como $(3, 10) = 1$ entonces podemos aplicar la el Teorema de Fermat donde $a^{\phi(n)} \equiv 1 \pmod{n}$ es decir $3^4 \equiv 1 \pmod{10}$ por lo tanto también tenemos que $(3^4)^{100} \equiv 1^{100} = 1 \pmod{10}$

Por lo tanto el último digito es uno

5. Ejercicio 5

Encontrar el número de enteros positivos $\leq$ 25200 que son primos relativos con 3600

Solución:

Ve que usando el Teorema del Ejercicio 6 (Demostrar que si m y k son enteros positivos, entonces el número de enteros positivos menos o iguales a mk que son primos relativos con m es $k\phi(m)$)

Entonces tenemos que $m = 7$ y $k = 3600$, entonces $7\phi(3600)$ son el número de enteros positivos menos o iguales a 25,200 que son primos relativos con 3600.

Y:

$$\begin{aligned} 7\phi(3600) &= 7\phi((2^4)(3^2)(5^2)) \\ &= (7)(3600)\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right) \\ &= (7)(3600)\left(\frac{1}{2}\right)\left(\frac{2}{3}\right)\left(\frac{4}{5}\right) \\ &= 6720 \end{aligned}$$

6. Ejercicio 6

$\phi(n)$ es la cantidad de naturales que son primos relativos menores que n, pero también n es la cantidad de primos relativos con n en el segmento $[n+1, 2n]$

Demostración:

Esto puede ser muy obvio o como para mi extremadamente interesante, para verlo tenemos que recordar la clave... $GCD(a, b) = GCD(a, b + ak)$.

Usando esto podemos darnos cuenta que cualquier entero k que cumpla con que $GCD(n, k) = 1 = GCD(n, k+n)$ es decir, si k es un coprimo con n entonces $k+n$ también lo será, por lo tanto puedo hacer esto con cada uno y solo con cada uno de los elementos que contaba la $phi(n)$.

Otra forma de decir lo que acabo de decir que podemos hacer una biyección entre ambos intervalos usando lo que acabo de decir, a cada elemento $a \in [1, n-1]$ tal que $(a, n) = 1$ lo vamos a relacionar con $a + n$ que pertenece a $[n + 1, 2n]$

Para cuales quiera a, b se cumple que el número de naturales menores o iguales que ab que son primos relativos con b es $a\phi(b)$

Solución:

Sea $\phi(b)$ la cantidad de naturales que son coprimos con b y que estan en el intervalo $[1, b-1]$.

Ya que sabemos que $\phi(n)$ es la cantidad de naturales que son primos relativos menores que n, pero también n es la cantidad de primos relativos con n en el segmento $[n+1, 2n]$... o incluso más general en el intervalo $[kn + 1, (k + 1)n]$.

Por lo tanto sabemos que la cantidad de primos relativos con b entre $[1, ab]$ es simplemente la suma de a intervalos, y ya sabemos que la cantidad de primos relativos con b en cada intervalo es $\phi(b)$ por lo tanto $a\phi(b)$ nos dará la cantidada de primos relativos en el intervalo $[1, ab]$.

7. Ejercicio 7

Para $n > 2$ se tiene que $\phi(n)$ es un número par

Demostración:

El caso $n = 2^k$ con $k > 1$ se sigue con facilidad

Si n no es una potencia de 2, entonces lo divide un primo impar p y entonces $n = p^\alpha m$ con $(p^\alpha, m) = 1$ por lo que: $\phi(n) = \phi(p^\alpha)\phi(m)$ y como $\phi(p^\alpha) = p^{\alpha-1}(p-1)$ y $(p-1)$ es par, el resultado se sigue.

Si n tiene k factores primos impares distintos, entonces $2^k|\phi(n)$

Solución:

Esta se ve fea, pero la verdad es que no lo esta, suponte que tenemos a n como un producto de k primos mayores que dos elevados a una potencia.

Ahora, como la Phi de Euler es una función multiplicativa (siempre que sean primos relativos, pero ya que vamos a trabajar con la factorización de n creo que doy esto por obvio) podemos ver que:

La $\phi(n)$ es el producto de las phis de cada uno de dichos factores impares, además recuerda que si $n < 2$ entonces $\phi(n)$ es par, ahí esta la clave.

Gracias a lo anterior podemos separar la $\phi(n)$ en k productos pares, donde k es el número de factores primos impares, ahora de como son productos pares podemso factorizar un dos de cada uno por lo tanto, al momento de calcular la $\phi(n)$ podremos factorizar k veces el número 2, por lo tanto $2^k|\phi(n)$

8. Ejercicio 8

Calcula $\phi(35)$

Solución:

$$\begin{aligned}\phi(35) = \phi(7*5) &= 35\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\\ &= 35\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)\\ &= 35\left(\frac{24}{35}\right)\\ &= 24\end{aligned}$$

Calcula $\phi(105)$

Solución:

$$\begin{aligned}\phi(105) = \phi(5*3*7) &= 105\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\\ &= 105\left(\frac{2}{3}\right)\left(\frac{4}{5}\right)\left(\frac{6}{7}\right)\\ &= 105\left(\frac{48}{105}\right)\\ &= 48\end{aligned}$$

Calcula $\phi(333)$

Solución:

$$\begin{aligned}\phi(333) = \phi(3^2\cdot 37) &= 333\left(1-\frac{1}{3}\right)\left(1-\frac{1}{37}\right)\\ &= 333\left(\frac{2}{3}\right)\left(\frac{36}{37}\right)\\ &= (3)(2)(36) = 216\end{aligned}$$

Calcula $\phi(2401)$

Solución:

$$\begin{aligned}\phi(2401) = \phi(7^4) &= 2401\left(1-\frac{1}{7}\right)\\ &= 2401\left(\frac{6}{7}\right)\\ &= 7^3(6) = 2058\end{aligned}$$

9. Ejercicio 9

Esta tarea no se debería leer en orden cronologico porque voy a usar un teorema de demuestro en el siguiente ejercicio, es fácil, veamos que ya sabemos que:

Si $(a, n) = 1$ y $(a - 1, n) = 1$ es decir si tanto a como su antecesor es primo relativo con m tenemos que: $1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}$

Y ahora toma a $a = 9$ y $n = 35$, por lo tanto $\phi(35) - 1 = 23$, por lo tanto: $1 + 9 + 9^2 + \cdots + a^{23} \equiv 0 \pmod{35}$.

Ahora si lo que quieres es comprobarlo simplemente hacemos la geometrica:

$$\begin{aligned}\sum_{k=0}^{23} 9^k &= \frac{9^{23} - 1}{8} \\ &= \frac{7976644307687250986336}{8} \\ &= 35\left(\frac{2279041230767785996096}{8}\right) \\ &= 35(18232329846142287968768)\end{aligned}$$

10. Ejercicio 10

Si $(a, n) = 1$ y $(a - 1, n) = 1$ es decir si tanto a como su antecesor es primo relativo con m tenemos que:

$1 + a + a^2 + \cdots + a^{\phi(n)-1} \equiv 0 \pmod{n}$

Demostración:

Esta demostración pide a gritos una serie geométrica, hagamosla y veamos que:

$$1 + a + a^2 + \cdots + a^{\phi(n)-1} = \sum_{k=0}^{\phi(n)-1} a^k = \frac{a^{\phi(n)} - 1}{a - 1}$$

Ahora, sabemos que como $(a, n) = 1$ entonces $a^{\phi(n)} \equiv 1 \pmod{n}$ es decir $n | a^{\phi(n)} - 1$ es decir $a^{\phi(n)} - 1 = qn$ entonces en vez de decir $\frac{a^{\phi(n)}-1}{a-1}$ podriamos decir $\frac{nq}{a-1}$

Ahora recuerda que $\frac{nq}{a-1}$ es un entero, pero aun más que como $(a - 1, n) = 1$ $a - 1$ no elimina tienen ningún factor en común con n, por lo tanto podemos sacar comodamente a n y decir que $1 + a + a^2 + \cdots + a^{\phi(n)-1} = \frac{a^{\phi(n)}-1}{a-1} = n\frac{q}{a-1}$ es decir $1 + a + a^2 + \cdots + a^{\phi(n)-1}$ es un multiplo de n, por lo tanto es congruente con cero módulo n

11. Ejercicio 11

Para cualquier entero n, tal que $(n, 10) = 1$ tenemos que n divide a algún N que consiste de solamente unos en su representación decimal:

Demostración:

Esta se ve difícil pero veras que solo es una aplicación del teorema: Si $(a, n) = 1$ y $(a-1, n) = 1$ es decir si tanto a como su antecesor es primo relativo con m tenemos que: $1+a+a^2+\cdots+a^{\phi(n)-1} \equiv 0 \pmod{n}$

Si $(n, 10) = 1$ y $(n, 9) = 1$. Y con esto podemos aplicar ya el Teorema, pues podemos ver a N como $10^0 + 10^1 + 10^{\phi(n)-1}$.

Gracias a ese Teorema vemos que esa N que son puros unos contendrá a $\phi(n) - 1$ unos, quiza no sea la menor N pero es una válida siempre.

Pero... que pasa si $(9, n) \neq 1$.

Entonces piensa que si $(n, 10) = 1$ si y solo si $(9n, 10)$ pues $9n = (n)(3)(3)$ y la única forma en que esto afectaría el valor del gcd es que 10 compartierá algun factor con nueve, pero como no, podemos afirmar esto.

Entonces $10^{\phi(9n) \equiv 1 \pmod{()9n}}$ por el Teorema de Fermat-Euler si $(10, 9n) = 1$ lo que implica que $(10, n)$.

Ahora, ya que sabemos que $10^{\phi(9n) \equiv 1 \pmod{()9n}}$ podemos escribirlo como que: $10^{\phi(9n)} - 1 = 9nq$ que podemos poner como:

$$\begin{aligned} nq &= \frac{10^{\phi(9n)} - 1}{9} \\ &= \frac{10^{\phi(9n)} - 1}{10 - 1} \\ &= \sum_{k=0}^{\phi(9n)-1} 10^k \end{aligned}$$

Por lo tanto siempre lo podemos escribir como una suma geometríca, es decir una N que esta hecha de puros unos.

Por lo tanto y como resumen:

- Si es que $(n, 10) = 1$ y $n \neq 3k$ entonces un número creado por $\phi(n) - 1$ unos siempre será un múltiplo de n.
- Si es que $(n, 10) = 1$ y $n = 3k$ entonces un número creado por $\phi(9n) - 1$ unos siempre será un múltiplo de n.

Demostración Versión 2:

Para alguna n arbitaria crea el conjunto $Unos = 1, 11, 111, 1111, \cdots \sum_{k=0}^{N} 10^k$. Ahora, nota que $Unos$ tiene $N+1$ elementos, desde 0 hasta N.

Ahora ve los residuos que obtiene al dividir cada elementos de $Unos$ entre n. Si te das cuenta al dividir entre n solo tendrás n residuos posibles, pero como tienes $N+1$ elementos 2 elementos diferentes tendrán un mismo residuo, por lo tanto su resta será divisible entre n (llamemos a la resta N').

Entonces para cualquier n tenemos que es posible encontrar una N' que esta hecha de la resta de dos números que contienen puros unos en su representación decimal, por lo tanto N' tendrá la forma de $N' = 1 \cdots 0 \cdots$, es decir N' esta formada de q unos consecutivos y de k ceros consecutivos.

Finalmente si $(10, n) = 1$ y sabemos que $n|N'$ tenemos que $n|(N)(10^k)$ con N siendo un número de puros unos, por lo tanto tenemos que $n|N$ pues n no puede dividir a 10^k pues es primo relativo con 10.