

- [Primer Trabajo de Control Parcial](#)
 - [Ejercicios](#)
 - [Problema 1](#)
 - [Problema 2](#)
 - [Problema 3](#)
 - [Soluciones](#)
 - [Solución 2](#)
 - [Función](#)
 - [Demostración \(Somoza\)](#)
 - [Demostración \(Temas escogidos de Teoría de Números\)](#)
 - [Demostración \(Youtube\)](#)

Primer Trabajo de Control Parcial

Ejercicios

Problema 1

Demuestre o refute:

1. El número $2^{2^n} - 1$ tiene al menos n divisores primos distintos.
2. La suma de los elementos de un sistema residual reducido modulo n es divisible entre n para todo n mayor o igual que 2.
3. Demuestra que si p es primo y $p \equiv 5 \pmod{8}$ y $p \mid (a^4 + b^4) \implies p \mid a$ y $p \mid b$.

Problema 2

Demuestre que la funcion $\varphi(n)$ es multiplicativa por una via distinta a la vista en clase.

Problema 3

Demostrar que para cualquier a, b, c enteros, si $\text{mcd}(a, b) = 1 \implies$ existen infinitos n enteros tal que $\text{mcd}(a + bn, c) = 1$

Soluciones

Solución 2

Función $\varphi(n)$

Para demostrar este teorema haremos uso de los siguientes lemas:

Lema 1:

Sean $a, b, m \in \mathbb{N} \Rightarrow$ se cumple que $\text{mcd}(ab, m) = 1 \Leftrightarrow \text{mcd}(a, m) = 1$ y $\text{mcd}(b, m) = 1$

La demostración en el sentido \Leftarrow es obvia. En el otro caso, supongamos que no se cumple, sin pérdida de generalidad sea $\text{mcd}(a, m) = d > 1 \Rightarrow \exists p$ primo tal que $p \mid m$ y $p \mid a \Rightarrow p \mid ab \Rightarrow p \mid \text{mcd}(ab, m)$ contradicción porque $\text{mcd}(ab, m) = 1$

Lema 2:

Sean $a, b \in \mathbb{Z}_+^*$ coprimos, entonces se cumple que $\text{mcd}(ax, b) = 1 \Leftrightarrow \text{mcd}(x, b) = 1$

(\Rightarrow) Supongamos que $\text{mcd}(ax, b) = 1$ y $\text{mcd}(x, b) = d > 1 \Rightarrow \exists p$ primo tal que $p \mid b$ y $p \mid x \Rightarrow p \mid ax \Rightarrow p \mid \text{mcd}(ax, b)$ contradicción porque $\text{mcd}(ax, b) = 1$. Por tanto $d = 1$

(\Leftarrow) Supongamos que $\text{mcd}(x, b) = 1$ y $\text{mcd}(ax, b) = d > 1 \Rightarrow \exists p$ primo tal que $p \mid b$ y $p \mid ax$, pero como $\text{mcd}(a, b) = 1 \Rightarrow p \nmid a$ porque p no puede dividir a a . Luego $p \mid x$ contradicción, por lo que $d = 1$

Lema 3:

Sean $k, l \in \mathbb{Z}_+^*$ coprimos. Si x y y recorren respectivamente sistemas completos de restos módulos k y l , entonces $xl + yk$ recorre un sistema completo de restos módulo kl

No es difícil ver que existen exactamente kl números de la forma $xl + yk$. Supongamos que $xl + yk$ no recorre el sistema completos de restos módulo kl , entonces:

$$x_1l + y_1k \equiv x_2l + y_2k \pmod{kl}$$

Por propiedades de congruencia se cumple que:

$$\begin{aligned} x_1l + y_1k &\equiv x_2l + y_2k \pmod{k} \\ x_1l &\equiv x_2l \pmod{k} \end{aligned}$$

Como $\text{mcd}(k, l) = 1$ entonces:

$$x_1 \equiv x_2 \pmod{k}$$

Contradicción porque x recorre un SRC módulo k . Análogamente se hace el análisis con l

Lema 4:

Sean $a, n \in \mathbb{N}$. Se cumple que $\text{mcd}(a, n) = 1 \Leftrightarrow \text{mcd}(x, n) = 1$ siendo $a \equiv x \pmod{n}$

Nótese que ambas expresiones son análogas, ya que $a \equiv x \pmod{n}$ es equivalente a $x \equiv a \pmod{n}$ por lo que basta demostrar en un solo sentido de la doble implicación.

Supongamos que dado $\text{mcd}(a, n) = 1$ se cumple que $\text{mcd}(x, n) = d > 1 \Rightarrow \exists p$ primo tal que $p \mid x$ y $p \mid n$ pero como $a \equiv x \pmod{n}$ se cumple que $n \mid (a - x) \Rightarrow p \mid (a - x)$ y como $p \mid x \Rightarrow p \mid a \Rightarrow p \mid \text{mcd}(a, n) = 1$ contradicción porque $\text{mcd}(a, n) = 1$

Demostración (Somoza)

Agrupemos los números desde 1 hasta mn de la siguiente forma:

$$\begin{array}{ccccc} 1 & m+1 & 2m+1 & \cdots & (n-1)m+1 \\ 2 & m+2 & 2m+2 & \cdots & (n-1)m+2 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ m & 2m & 3m & \cdots & nm \end{array}$$

Según el **Lema 1** para saber cuántos números hay coprimos con mn basta calcular cuántos números son coprimos con m y coprimos con n simultáneamente.

Nótese que en una fila, si un elemento deja resto k módulo m entonces todos los elementos de esa fila dejan resto k módulo n

Por cada columna tenemos un SRC módulo m , en el cual hay $\varphi(m)$ números primos relativos con m , ya que su resto módulo m es primo relativo con m

Analicemos ahora las filas, nótese que si tenemos un SRC módulo n , al multiplicarlo por m , como son coprimos seguiremos teniendo un SRC, y al sumarle una constante k igual el resultado será un SRC, luego, si en la matriz buscamos en la fila k observamos que es exactamente lo que tenemos, por lo cual, en cada fila de la matriz hay un SRC módulo n , en el cual hay $\varphi(n)$ números primos relativos con n

Por último, como tenemos en cada columna $\varphi(m)$ coprimos con m y en cada fila $\varphi(n)$ primos relativos con n , la cantidad total de números coprimos con m y n a la vez son $\varphi(m)\varphi(n)$

Demostración (Temas escogidos de Teoría de Números)

Sean a y b enteros positivos coprimos. Supongamos que x y y recorren sistemas completos de restos módulos a y b respectivamente. Por el **Lema 3** $xb + ya$ recorre un sistema completo de restos módulo ab , luego aplicando el **Lema 1** y **Lema 2** se cumple que:

$$(xb + ya, ab) = 1 \Leftrightarrow (xb + ya, a) = 1, (xb + ya, b) = 1 \Leftrightarrow (xb, a) = 1, (ya, b) = 1 \Leftrightarrow (x, a) = 1, (y, b) = 1$$

Esto significa que $xb + ya$ es primo relativo con ab si y solo si x es coprimo con a y y es primo relativo con b , entonces $\varphi(ab) = \varphi(a)\varphi(b)$

Demostración (Youtube)

Queremos probar que la función $\varphi(n)$ es multiplicativa, o sea, $\varphi(mn) = \varphi(m)\varphi(n)$.

Sean $M = \{m_1, m_2, \dots, m_p\}$ y $N = \{n_1, n_2, \dots, n_q\}$ los sistemas de restos reducidos de m y n respectivamente. Si hallamos una función f biyectiva entre el producto cartesiano de ambos conjuntos y los números que son primos relativos con mn menores que mn habríamos demostrado que la cardinalidad tanto del producto cartesiano ($\varphi(m)\varphi(n)$) como la de $\varphi(mn)$ son iguales.

Apoyándonos en el **Lema 1** y **Lema 4** basta encontrar todos restos primos relativos con m y con n y los números que cumplen con esos restos simultáneamente, por lo que serán coprimos con mn , por tanto, nuestra función f será sobreyectiva. Utilizando el *Teorema Chino del Resto* dados m_i, n_j restos de m, n respectivamente, como $\text{mcd}(m, n) = 1 \Rightarrow$ el sistema de congruencia:

$$\begin{aligned}x &\equiv m_i \pmod{m} \\x &\equiv n_j \pmod{n}\end{aligned}$$

Tiene solución y es única, por tanto, garantizamos que la función f es total (abarca todos los elementos del producto cartesiano de ambos conjuntos) y es inyectiva (porque la solución proporcionada por el *Teorema Chino del Resto* es única). Por tanto, podemos concluir que la función f es biyectiva, lo que implica que el producto cartesiano tiene tantos elementos como coprimos menores que $mn \Rightarrow \varphi(mn) = \varphi(m)\varphi(n)$