Teoría de números

Profesores del curso:
Ronald Mass [1]
Ángel Ramírez [1]

[1]Universidad Nacional de Ingeniería, Lima, Perú

15 de agosto de 2020

Tabla de contenidos

Pequeño Teorema de Fermat

Teorema 1

Si p es un primo y $n \in \mathbb{N}$ relativamente primo con p, entonces:

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

Demostración:

Afirmamos que los números $n, 2n, 3n, \ldots, (p-1)n$ dejan todos ellos residuos distintos al dividirse entre p y, además, que ninguno de estos residuos es cero. En efecto, tomemos $0 < i < j < p-1$. Sabemos que cuando p es primo se cumple que $[n]$ tiene inverso en $\mathbb{Z}_p$. Sea $[m]$ su inverso. Luego, si $[in] = [jn]$ entonces multiplicando por $[m]$ a ambos lados resulta:

$$[i] = [i(ab)] = [j(ab)] = [j]$$

Pequeño Teorema de Fermat (cont.)

pero como i, j están entre 1 y p, esto implica que $i = j$. Además, ninguno es cero pues si $[ia] = [0]$ entonces al multiplicar por $[m]$ se tiene que:

$$[i] = [i(ab)] = [0b] = [0]$$

lo que es una contradicción.
Así, usando la afirmación en la siguiente cadena módulo p, se tiene:

$$\begin{aligned} (p-1)!a^{p-1} &= (a)(2a)(3a)\ldots((p-1)a) \\ &= 1 \cdot 2 \cdot \ldots \cdot (p-1) = (p-1)! \end{aligned}$$

El número $(p-1)!$ no es divisible entre p, pues es producto de puros números menores que p, de modo que $mcd(p,(p-1)!) = 1$, así que tiene inverso módulo p, de modo que podemos cancelarlo

Pequeño Teorema de Fermat (cont.)

de la congruencia anterior multiplicando en ambos lados por su inverso. Así, obtenemos la igualdad:

$$a^{p-1} \equiv 1 \, (mod \; p).$$

Ejemplo:

Demuestre que $13|(2^{50}+3^{50})$.

Demostración:

Por el pequeño teorema de Fermat:

$$\begin{aligned} 2^{12} &\equiv 1\,(mod\,13) \\ 3^{12} &\equiv 1\,(mod\,13) \end{aligned}$$

Como $50 = 4(12)+2$, entonces:

$$\begin{aligned} 2^{50} &= 2^{4(12)+2} = (2^{12})^4 \cdot 2^2 \equiv 1^4 \cdot 4 \equiv 4\,(mod\,13) \\ 3^{50} &= 3^{4(12)+2} = (3^{12})^4 \cdot 2^2 \equiv 1^4 \cdot 9 \equiv 9\,(mod\,13) \end{aligned}$$

luego: $2^{50}+3^{50} \equiv (4+9)\,(mod\,13) \equiv 0\,(mod\,13)$.

Tabla de contenidos

Proposición 1

Sea p un número primo. Los únicos elementos en $\mathbb{Z}_p$ que son inversos de sí mismos son $[1]$ y $[p-1]$.

Demostración: Claramente $[1]$ y $[p-1] = [-1]$ son inversos multiplicativos de sí mismos porque $1 \cdot 1 = (-1) \cdot (-1) = 1$. Ahora, si tenemos a tal que es inverso multiplicativo de sí mismo, tenemos que $[a^2] = [1]$ que por definición se tiene que $p|(a^2 - 1)$, pero $(a^2 - 1) = (a-1)(a+1)$. Cuando un primo divide a un producto, tiene que dividir a uno de los factores. Entonces p divide a $(a+1)$ o $(a-1)$ y obtenemos respectivamente que $[a] = [-1] = [p-1]$ o que $[a] = [1]$, que es lo que queríamos probar.

Teorema 2 (Teorema de Wilson)

Si p es un número primo, entonces $(p-1)! \equiv -1\,(mod\ p)$.

Demostración:

Si $p = 2$, el resultado es inmediato. Supongamos que $p \geq 3$. En $(p-1)!$ aparecen todos los números de 1 a $(p-1)$. Todos ellos son primos relativos con p, así que tienen inverso módulo p. Ese inverso también aparece en $(p-1)!$. Así podemos agrupar esos números en $(p-3)/2$ parejas de inversos multiplicativos, en donde por la proposición anterior sólo nos va a sobrar el 1 o -1. De esta forma:

$$(p-1)! \equiv (1)(-1)(1 \cdot 1 \cdot \ldots \cdot 1) \equiv -1\,(mod\ p),$$

en donde en la expresión intermedia tenemos un 1, un -1 y $(p-3)/2$ unos, uno por cada pareja de inversos que se multiplicaron, finalizando así la prueba.

Ejemplo:

Determine el residuo que se obtiene al dividir $15! + 16! + 17!$ entre 17.

Resolución:

Notemos que 17 divide a 17!, así que $17! \equiv 0\,(mod\,17)$. Por el teorema de Wilson, $16! \equiv -1\,(mod\,17)$. Podemos multiplicar esta igualdad por -1, resultando:

$$15! = 15!(-1)(-1) \equiv 15!(16)(-1) = 16!(-1) \equiv (-1)(-1) \equiv 1$$

por tanto:

$$15! + 16! + 17! \equiv 1 + (-1) + 0 \equiv 0\,(mod\,17).$$

Tabla de contenidos

Funciones aritméticas

Funciones aritméticas son aquellas funciones cuyo dominio es $\mathbb{N}$ y cuyo rango es un subconjunto de $\mathbb{C}$. Una función aritmética f es llamada **multiplicativa** si:

$$f(mn) = f(m)f(n) \quad \text{para todo} \quad m, n \in \mathbb{N} \quad \text{tal que} \quad mcd(m, n) = 1.$$

f es llamada **completamente multiplicativa** si:

$$f(mn) = f(m)f(n) \quad \text{para todo} \quad m, n \in \mathbb{N}$$

Función de Euler

Para cualquier $n \in \mathbb{N}$ la **función de Euler**, también llamada **Euler's Totien**, $\phi(n)$ es definida como la cantidad de $m \in \mathbb{N}$ tal que $m < n$ y $mcd(m, n) = 1$. Es decir:

$$\phi(n) = |\{m \in \mathbb{N} \,/\, m < n \wedge mcd(m, n) = 1\}|.$$

Ejemplo:
Si p es primo, entonces cualquier $j \in \mathbb{N}$ con $j < p$ es relativamente primo a p, entonces $\phi(p) = p - 1$.

Sistema de residuos reducidos

Si $n \in \mathbb{N}$, entonces cualquier conjunto de $\phi(n)$ enteros no congruentes módulo n y relativamente primos a n, es llamado un **sistema de residuos reducido** módulo n.

Ejemplo:
El conjunto $\{1, 3, 7, 9\}$ es un sistema de residuos reducidos módulo 10 porque $\phi(10) = 4$, y cada elemento del conjunto es relativamente primo a 10, y ellos no son congruentes módulo 10.

Teorema 3

La función es Euler es multiplicativa, es decir, dados $m, n \in \mathbb{N}$ relativamente primos, entonces:

$$\phi(mn) = \phi(m)\phi(n).$$

Además, si $n = \prod_{j=1}^{k} p_j^{a_j}$ *donde los* p_j *son primos distintos, entonces:*

$$\phi(n) = \prod_{j=1}^{k}(p_j^{a_j} - p_j^{a_j-1}) = \prod_{j=1}^{k}\phi(p_j^{a_j}).$$

Teorema de Euler

Si $n \in \mathbb{N}$ y $m \in \mathbb{Z}$ tal que $mcd(m, n) = 1$, entonces:

$$m^{\phi(n)} \equiv 1 \,(mod\ n)$$