Ciencias de la Computación I

Tópicos de Teoría de Números III

Eduardo Contrera Schneider

Universidad de la Frontera

19 de octubre de 2016

Empecemos por los siguientes lemas:

Lema 1

Sea $a, b \in \mathbb{Z}^+$ y p un número primo. Si $p|ab$, entonces $p|a$ o $p|b$.

Lema 2

Sea $a \in \mathbb{Z}^+$ para todo $1 \leq i \leq n$. Si p es primo y $p|a_1 a_2 \cdots a_n$, entonces $p|a_i$ para algún $1 \leq i \leq n$.

Con este último resultado podemos demostrar que el número $\sqrt{p}$ con p primo es irracional.

Teorema Fundamental de la Aritmética

Con los resultados precedentes podemos justificar el siguiente resultado que probablemente es de los más importantes en la teoría de números.

Teorema

Todo entero $n > 1$ puede escribirse de manera única como un producto de potencias de números primos, a excepción del orden de estos.

Lema

Si $n \in \mathbb{Z}^+$ y n es compuesto, entonces existe un número primo p tal que $p|n$ y $p \leq n$.

Aritmética Modular

Congruencia

Si a y b son enteros y m es un entero positivo, entonces se dice que a será *congruente* con b módulo m si $a - b$ es un múltiplo de m, es decir, $m|(a - b)$. Esto se denota como $a \equiv b(mod \quad m)$, donde m recibe el nombre de módulo de la congruencia y b recibe el nombre de residuo (o resto) de $a(mod \quad m)$

No es difícil ver que la congruencia es una relación de equivalencia que particiona el conjunto de enteros en subconjuntos disjuntos dos a dos formados por sus correspondientes restos.

Propiedades

1. Si $a \equiv b(mod \quad m)$, entonces a y b tienen el mismo resto al ser divididos por m.
2. Si $a \equiv b(mod \quad m)$ y $c \in \mathbb{Z}$, entonces
   1. $a \pm c \equiv b(mod \quad m)$
   2. $ac \equiv bc(mod \quad m)$
3. Si $ac \equiv (bc)(mod \quad m)$, entonces $a \equiv b(mod \quad m)$, entonces $a \equiv b(mod(\frac{m}{mcd(c,m)}))$
4. Si $a, b, c, d \in \mathbb{Z}$ y m es un entero positivo tal que $a \equiv b(mod \quad m)$ y $c \equiv d(mod \quad m)$, entonces:
   1. $a \pm c \equiv (b \pm d)(mod \quad m)$
   2. $ac \equiv (bd)(mod \quad m)$
   3. $a^n \equiv b^n(mod \quad m)$, donde n es un entero positivo.

Clases de Equivalencia

El conjunto de todos los enteros b que son congruentes con a módulo m recibe el nombre de congruencia módulo m de clase a y se denota por $\bar{a}$ o $[a]$ o $[a]_m$. Conjuntistamente tenemos,

$$\bar{a} = \{b \in \mathbb{Z} | b \equiv a (mod \quad m)\}$$

Se habla también de este conjunto como la **clase** de a.

Ejemplos

En los enteros módulo 5 tenemos,

- $\bar{0} = \{b \in \mathbb{Z} | b = 5k, \quad k \in \mathbb{Z}\}$
- $\bar{1} = \{b \in \mathbb{Z} | b = 5k + 1, \quad k \in \mathbb{Z}\}$
- $\bar{2} = \{b \in \mathbb{Z} | b = 5k + 2, \quad k \in \mathbb{Z}\}$
- $\bar{3} = \{b \in \mathbb{Z} | b = 5k + 3, \quad k \in \mathbb{Z}\}$
- $\bar{4} = \{b \in \mathbb{Z} | b = 5k + 4, \quad k \in \mathbb{Z}\}$

Propiedades Clases

- $[a] + [b] = [a + b]$
- $[a][b] = [ab]$

Una congruencia de la forma $ax \equiv b(mod\ \ m)$, donde m es un entero positivo, a, b y x (la incógnita) son enteros, se llama congruencia lineal. No es difícil ver que resolver una congruencia lineal es resolver una ecuación diofántica equivalente. Cualquier valor de x que es solución de la congruencia $ax \equiv 1(mod\ \ m)$ se denomina inverso de a módulo m.

Teorema Chino del Resto

Cuando $m_1, m_2, ..., m_k$ son enteros positivos y primos relativos de dos en dos, el sistema de congruencia $x \equiv a_1 (mod \quad m_1), x \equiv a_2 (mod \quad m_2), ..., x \equiv a_k (mod \quad m_k)$, donde $a_1, a_2, ..., a_k$ son enteros dados, tiene una solución única módulo m, donde $m = m_1 m_2 ... m_k$. La solución a este sistema está dada por

$$x = a_1 M_1 x_1 + a_2 M_2 x_2 + ... + a_k M_k x_k$$

donde $M_i = \frac{m}{m_i}$ con $i = 1, 2, ..., k$.

Ejemplo

Determine un número que al ser dividido por 3 da resto 2, al ser dividido por 5 da resto 2 y al ser dividido por 7 da resto 3.