Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC1253 - Matemáticas Discretas

Ayudantía 14 - Teoría de números

Héctor Núñez, Paula Grune, Manuel Irarrázaval

Resumen

Division y módulo

- **Relación divide a:** La relación divide a, denotada por $|$ sobre $\mathbb{Z}\backslash 0$, es tal que $a \mid b$ si y solo si $\exists k \in \mathbb{Z}$ tal que $b = k \cdot a$.
- **Relación módulo n:** La relación módulo n, denotada por $\equiv_n$ sobre $\mathbb{Z}$, es tal que $a \equiv_n b$ si y solo si $n \mid (b - a)$. Esta relación es de equivalencia.
- **Operacion módulo n:** La operación módulo n entrega el resto de la división por n, se denota por $a \bmod n$.
- **Teoremas:**

$$a \equiv_n b \Longleftrightarrow a \bmod n = b \bmod n$$

$$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$(a \cdot b) \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$$

Pequeño teorema de Fermat

- Si p es primo:

$$a^p \equiv_p a$$

- Si p es primo y no divide a a:

$$a^{p-1} \equiv_p 1$$

Máximo común divisor (GCD)

- **Máximo común divisor:** Dados a y b diremos que su máximo común divisor denotado como $\gcd(a, b)$ es el máximo natural n tal que $n \mid a$ y $n \mid b$.

- **Algoritmo de euclides:** Si $a > b$ entonces:

$$\gcd(a,b) = \gcd(r,b) \quad \text{con} \quad a \bmod b = r < b$$

Si seguimos recursivamente, llegamos a

$$\gcd(a,b) = \gcd(r,b) = \gcd(r, b \bmod r) = \cdots = \gcd(n,0) = n$$

- **Identidad de Bézout:** Esta identidad enuncia que si $a, b \in \mathbb{Z}$ son distintos de 0 y $\gcd(a,b) = d$, entonces existen $x, y \in \mathbb{Z}$ tales que:

$$a \cdot x + b \cdot y = d$$

Ejercicio 1: Aritmética Modular

Sean a, b, c y $m \in \mathbb{Z}$ tales que $m \geq 2$.

1. Demuestre que si $a \equiv b(\mod m)$, entonces $MCD(a, m) = MCD(b, m)$.
2. Demuestre que si $ac \equiv bc(\mod m)$, entonces $a \equiv b \left(\mod \frac{m}{MCD(c,m)}\right)$.

Ejercicio 2: Pequeño teorema de Fermat

1. Demuestre que $13 | (7^{121} + 6)$
2. Un googleplex es equivalente $10^{10^{100}}$. ¿Que dia de la semana va a ser en un googleplex dias? (Hoy dia es miércoles).

Ejercicio 3: Máximo común divisor y algoritmo euclidiano

Considere el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \end{cases}$$

Demuestre que el sistema tiene solución si y solo si $\mathrm{MCD}(m_1, m_2) \mid (a_1 - a_2)$.