Ayudantía 08

Teoría de números

Ayudante: Diego Rodríguez Cid – darodriguez6@uc.cl

Repaso de conceptos

Enteros y Divisibilidad

Un entero d divide a otro entero a (denotado $d \mid a$) si existe un entero k tal que

$$a = d \cdot k.$$

El máximo común divisor de a y b se escribe $\gcd(a, b)$.

Congruencias

Dados enteros a, b y un módulo $m \geq 1$, decimos que

$$a \equiv b \pmod{m}$$

si m divide a $a - b$. Las congruencias son compatibles con la suma, resta y multiplicación:

$$\text{si } a \equiv b \pmod{m},\ c \equiv d \pmod{m}, \implies a \pm c \equiv b \pm d \pmod{m},\ ac \equiv bd \pmod{m}.$$

Aritmética modular

- **Clases de restos.** El conjunto de clases módulo m se escribe

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

- **Operaciones.** Dados $[a]_m$, $[b]_m \in \mathbb{Z}_m$, definimos

$$[a]_m + [b]_m = [a+b]_m, \quad [a]_m \cdot [b]_m = [a \cdot b]_m.$$

Algoritmo extendido de Euclides

Sean 2 enteros a y b. El algoritmo de Euclides nos permite encontrar MCD(a,b) mediante la siguiente recursión:

$$r_0 = a$$

$$r_1 = b$$

$$r_{i+1} = r_{i-1} \bmod r_i$$

Si $r_k = 0$, entonces $\text{MCD}(a, b) = r_{k-1}$.

Para el algoritmo extendido, se agregan las secuencias s_i y t_i tal que se cumpla:

$$r_i = s_i \cdot a + t_i \cdot b$$

En este caso, si $r_k = 0$, entonces $\text{MCD}(a, b) = r_{k-1} = s_{k-1} \cdot a + t_{i-1} \cdot b$ y el algoritmo retorna $\text{MCD}(a, b)$, s_{i-1} y t_{i-1}. Así, el algoritmo parte de la siguiente manera

$$\begin{aligned} r_0 &= 1 \cdot a + 0 \cdot b, \\ r_1 &= 0 \cdot a + 1 \cdot b, \\ r_{i+1} &= \left(s_{i-1} - \lfloor \tfrac{r_{i-1}}{r_i} \rfloor \cdot s_i\right) a + \left(t_{i-1} - \lfloor \tfrac{r_{i-1}}{r_i} \rfloor \cdot t_i\right) b. \end{aligned}$$

Problema 1. Aritmética modular

Demuestre la propiedad

$$\text{si } a \equiv b \pmod{m},\ c \equiv d \pmod{m},\ \Longrightarrow\ ac \equiv bd \pmod{m}.$$

Problema 2. Euclides extendido

Demuestre que el algoritmo extendido de Euclides funciona en tiempo polinomial en el largo de la entrada

Problema 3

Demuestre que $[a]_n \in \mathbb{Z}/n\mathbb{Z}$ tiene inverso si y solo si MCD(a,n) = 1