1. Teoría de Números

1.1. División

Considerando a $\mathbb{Z}$ como el conjunto de los números enteros, para $a, b \in \mathbb{Z}$ y $a \neq 0$, se dice que a divide a b si es que:

$$a|b \leftrightarrow \exists q \in \mathbb{Z} \; . \; a \cdot q = b$$

En el caso que esto no se cumpla, entonces a no divide b, expresado como $a \nmid b$

1.1.1. Propiedades de la división

- Si $a|b$ y $a|c$, entonces $a|(b+c)$
- Si $a|b$, entonces $a|(b \cdot c)$ para todo $c \in \mathbb{Z}$
- Si $a|b$ y $b|c$, entonces $a|c$

Corolario: Si $a|b$ y $b|c$, entonces $a|(b \cdot m + n \cdot c)$, para todo $m, n \in \mathbb{Z}$

1.2. Módulo

Con $a, b \in \mathbb{Z}$, $a > 0$ y $a|b$, entonces existe un único par $q, r \in \mathbb{Z}$ tal que $a \cdot q + r = b$. Esta corresponde a la definición de la división con resto. Mediante esta, se define el operador módulo (mod) y el operador división (div).

$$\begin{aligned} b \text{ div } a &= q \\ b \bmod a &= r \end{aligned}$$

1.3. Congruencia modular

Con $m \in \mathbb{Z}$ y $m > 0$, diremos que para todo $a, b \in \mathbb{Z}$, a es congruente con b mod m si:

$$a \equiv b (\bmod m) \quad \text{si, y solo si} \quad m|(a-b)$$

1.3.1. Propiedades de la congruencia modular

Para todo $a, b, m \in \mathbb{Z}$, donde $m > 0$, se cumple que:

- $a \equiv b (\bmod m)$
- $a = b + m \cdot s$, para algún $s \in \mathbb{Z}$
- $(a \bmod m) = (b \bmod m)$

1.3.2. Suma y multiplicación de la congruencia modular

Para todo $m > 0$, si $a \equiv b (\bmod m)$ y $c \equiv d (\bmod m)$ entonces:

$$\begin{aligned} a + c &\equiv b + d (\bmod m) \\ a \cdot c &\equiv b \cdot d (\bmod m) \end{aligned}$$

Adicionalmente...

$$\begin{aligned} (a+b) \bmod m &= ((a \bmod m) + (b \bmod m)) \bmod m \\ (a \cdot b) \bmod m &= ((a \bmod m) \cdot (b \bmod m)) \bmod m \end{aligned}$$

1.3.3. Aritmética módulo m - Aritmética modular

Con $m > 0$, se define $\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}$. Entonces, para todo $a, b \in \mathbb{Z}_m$, se definen las operaciones $+_m$ y $\cdot_m$

$$\begin{aligned} a +_m b &= (a + b) \bmod m \\ a \cdot_m b &= (a \cdot b) \bmod m \end{aligned}$$

La aritmética modular cumple con las siguientes propiedades:

Clausura:	$a +_m b \in \mathbb{Z}_m \quad ; \quad a \cdot_m b \in \mathbb{Z}_m$
Conmutatividad	$a +_m b = b +_m a \quad ; \quad a \cdot_m b = b \cdot_m a$
Asociatividad	$a +_m (b +_m c) = (a +_m b) +_m c \quad ; \quad a \cdot_m (b \cdot_m c) = (a \cdot_m b) \cdot_m c$
Identidad:	$a +_m 0 = a \quad ; \quad a \cdot_m 1 = a$
Inverso aditivo:	$a \neq 0,\ \exists a' \in \mathbb{Z}_m \ .\ a +_m a' = 0$
Distributividad:	$a \cdot_m (b +_m c) = (a \cdot_m b) + (a \cdot_m c)$