

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).

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

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 $b \text{ mod } m$ si:

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

1.3.1. Propiedades de la congruencia modular

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

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

1.3.2. Suma y multiplicación de la congruencia modular

Para todo $m > 0$, si $a \equiv b(\text{ mod } m)$ y $c \equiv d(\text{ mod } m)$ entonces:

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

Adicionalmente...

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

1.3.3. Aritmética módulo m - Aritmética modular

Con $m > 0$, se define $\mathbb{Z}_m = \{0, 1, 2, \dots, m-1\}$. 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:

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

1.4. Representación de los números

Sea $b > 1$. Si $n \in \mathbb{N} - \{0\}$, entonces n se puede escribir de forma única como:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + a_{k-3}b^{k-3} + \dots + a_2b^2 + a_1b^1 + a_0 = \sum_{i=0}^{k-1} a_i b^i$$

con

- $k \geq 1$
- Para todo $i < k$, $a_i < b$
- $a_{k-1} \neq 0$

Para poder simplificar un poco las cosas, vamos a establecer que todo número en representación de n en base b corresponde a la secuencia

$$(n)_b = a_{k-1} \dots a_2 a_1 a_0$$

Como pequeño dato curioso, si esto le parece familiar al lector, es porque esto representa la forma en que nosotros escribimos los números normalmente, en donde la base $b = 10$.

1.4.1. Encontrando la representación de n en base b

Ahora que entendemos que podemos representar números usando distintas bases, ¿cómo podemos encontrar la representación de cualquier número en cualquier base?

Si se tiene un número $n \in \mathbb{N} - \{0\}$ y $b > 0$, sabiendo que su representación debe ser de la forma $(n)_b = a_{k-1} \dots a_2 a_1 a_0$ y que por la división con resto, sabemos que $n = q \cdot b + r$, entonces tenemos que

$$\begin{aligned} r &= a_0 \\ (q)_b &= a_{k-1} \dots a_1 \end{aligned}$$

1.4.2. Suma de números en base b

La forma de llegar al algoritmo para la suma de números en base b corresponde al siguiente, considerando que n y m son números en base b .

$$\begin{aligned} n + m &= (n_{k-1} + m_{k-1}) \cdot b^{k-1} + \dots + (n_2 + m_2) \cdot b^2 + (n_1 + m_1) \cdot b + (n_0 + m_0) & / (n_0 + m_0) = c_0 \cdot b + s_0 \\ n + m &= (n_{k-1} + m_{k-1}) \cdot b^{k-1} + \dots + (n_2 + m_2) \cdot b^2 + (n_1 + m_1 + c_0) \cdot b + s_0 & / (n_1 + m_1 + c_0) = c_1 \cdot b + s_1 \\ n + m &= (n_{k-1} + m_{k-1}) \cdot b^{k-1} + \dots + (n_2 + m_2 + c_1) \cdot b^2 + s_1 \cdot b + s_0 & / (n_2 + m_2 + c_1) = c_2 \cdot b + s_2 \\ & & / \dots \end{aligned}$$

Si se continua aplicando hasta terminar con toda la ecuación, se obtiene que

$$n + m = c_{k-1} \cdot b^k + s_{k-1} \cdot b^{k-1} + \dots + s_1 \cdot b + s_0$$

Estas son muchas letras y posiblemente confunde demasiado, por lo que es mejor trabajar con un ejemplo de como se usa este algoritmo. Supongamos que queremos realizar la suma $(11)_2 + (14)_2$, donde $(11)_2 = 1011$ y $(14)_2 = 1110$.

Se comienza con el primer dígito (1011; 1110):	$1 + 0$	$=$	$0 \cdot 2 + 1$	Resultado: 1
Se continua con el segundo dígito (1011; 1110):	$1 + 1 + 0$	$=$	$1 \cdot 2 + 0$	Resultado: 01
Se continua con el tercer dígito (1011; 1110):	$0 + 1 + 1$	$=$	$1 \cdot 2 + 0$	Resultado: 001
Se continua con el cuarto dígito (1011; 1110):	$1 + 1 + 1$	$=$	$1 \cdot 2 + 1$	Resultado: 1001
Siguiente dígito de la base (5° dígito acumulado):	$0 + 0 + 1$	$=$	$0 \cdot 2 + 1$	Resultado: 11001

Entonces, $(11)_2 + (14)_2 = 11001$.

Este algoritmo es exactamente lo que se usa para realizar sumas de forma manual en base 10.

1.4.3. Multiplicación de números en base b

Considerando que n y m son números en base b , la multiplicación $m \cdot n$

$$n \cdot m = n(m_{k-1}b^{k-1} + \dots + m_2b^2 + m_1b + m_0) = n \cdot (m_{k-1}b^{k-1}) + \dots + n \cdot (m_2b^2) + n \cdot (m_1b) + n \cdot (m_0)$$

Considerando esto, se define p_i como

$$(p_i)_b = n \cdot (m_i \cdot b) = \begin{cases} 0 & \text{si } m_i = 0 \\ n_{k-1} \dots n_1 n_0 0 \dots 0 & \text{si } m_i = 1. \text{ La cantidad de ceros es } i \end{cases}$$