Bases Numéricas y Algoritmo de Euclides

Santiago Baca - A01656580

Bases Numéricas

Teorema:

Dado un número $b \in \mathbb{N}$ con $b \geq 2$ y $n \in \mathbb{N}$ con $n \neq 0$, existen $l \in \mathbb{N}$ y $d_0, d_1, \ldots, d_l \in \mathbb{N}$ únicos tales que

$$n = d_0 \cdot b^0 + d_1 \cdot b^1 + \ldots + d_{l-1} \cdot b^{l-1} + d_l \cdot b^l$$

$d_l \neq 0$ y para todo $0 \leq i \leq l$ tenemos que $0 \leq di < b$

1. Primero mostraremos que tales números existen. Para ello, primero hagámoslo para $b = 7$. Escribe todos los pasos para pasar $(77)_{10}$ (setenta y siete base 10) a base 7.

$$(77)_{10} = (11 \cdot 7 + 0) \cdot 7^0$$

$$(77)_{10} = 11 \cdot 7^1 + 0 \cdot 7^0$$

$$(77)_{10} = (1 \cdot 7 + 4) \cdot 7^1 + 0 \cdot 7^0$$

$$(77)_{10} = 1 \cdot 7^2 + 4 \cdot 7^1 + 0 \cdot 7^0$$

$$(77)_{10} = (140)_7$$

2. Ahora escribe un algoritmo para escribir cualquier número en base 7.

   Entrada: Un número n en base 10, siendo $n \in \mathbb{N}$, $n \neq 0$.

   Salida: La representación de n en base 7, de la forma $n = d_l \cdot 7^l + d_{l-1} \cdot 7^{l-1} + \ldots + d_1 \cdot 7^1 + d_0 \cdot 7^0$, donde $0 \leq d_i < 7$.

   Paso 1: Dividir n entre 7, y el residuo será d_0.
   Paso 2: Expresar n como $m_1 \cdot 7^1 + d_0 \cdot 7^0$ y observar m_1.
   Paso 3: Si $0 \leq m_1 < 7$, tomar m_1 como d_1 y finalizar el algoritmo. En caso contrario, dividir m_1 entre 7 y el residuo será d_1.
   Paso 4: Repetir a partir del paso *2* con $n = m_1$.

   Este algoritmo intenta demostrar que para cualquier n y base $b = 7$, existen $l \in \mathbb{N}$ y $d_0, d_1, \ldots, d_l \in \mathbb{N}$ únicos que cumplen con la representación dada.

3. Finalmente, escribe un algoritmo general para escribir un número en base b.

   Entrada: Un número n, siendo $n \in \mathbb{N}$, $n \neq 0$.

   Salida: La representación de n en base $b \geq 2$, de la forma $n = d_l \cdot b^l + d_{l-1} \cdot b^{l-1} + \ldots + d_1 \cdot b^1 + d_0 \cdot b^0$, donde $0 \leq d_i < b$.

   Paso 1: Inicializar $i = 0$ y lista de coeficientes $d = [\,]$.
   Paso 2: Mientras $n \neq 0$, hacer los siguientes pasos:
   a) Calcular el residuo r y cociente entero c al dividir n entre b.
   b) Agregar r a la lista de coeficientes d.
   c) Actualizar $n = c$.
   d) Incrementar i en 1
   Paso 3: La representación de n en base b es:
   $n = d_0 \cdot b^0 + d_1 \cdot b^1 + \ldots + d_{i-1} \cdot b^{i-1} + d_i \cdot b^i$

   Este algoritmo es válido para cualquier n y $b \geq 2$. El paso 2 se repite hasta que n se convierte en 0, acumulando los coeficientes d_i que representan la expansión de n en la base b. Este también intenta demostrar que existen $l \in \mathbb{N}$ y $d_0, d_1, \ldots, d_l \in \mathbb{N}$ únicos que cumplen con la representación dada.

4. Ahora demostraremos la unicidad. Empecemos con la unicidad de l. Supongamos que se puede escribir con dos longitudes distintas. Utiliza el hecho de que

$$\sum_{i=0}^{m-1} (b-1) \cdot b^i = b^m - 1$$

   para mostrar que ambas representaciones deben tener la misma longitud.

   Supongamos que podemos escribir un número n en dos representaciones diferentes en la base b con longitudes l y m respectivamente, donde $l \neq m$. Entonces, tenemos:

$$n_1 = d_0 \cdot b^0 + d_1 \cdot b^1 + \ldots + d_{l-1} \cdot b^{l-1} + d_l \cdot b^l$$

$$n_2 = d_0^* \cdot b^0 + d_1^* \cdot b^1 + \ldots + d_{m-1}^* \cdot b^{m-1} + d_m^* \cdot b^m$$

   Dado que $l \neq m$, sin pérdida de generalidad, asumamos que $l > m$. Restamos la primera representación de la segunda:

$$n_1 - n_2 = d_0 \cdot b^0 + d_1 \cdot b^1 + \ldots + d_{l-1} \cdot b^{l-1} + d_l \cdot b^l - (d_0^* \cdot b^0 + d_1^* \cdot b^1 + \ldots + d_{m-1}^* \cdot b^{m-1} + d_m^* \cdot b^m)$$

   Lo cual es equivalente a escribirlo tal que:

$$n_1 - n_2 = \sum_{i=0}^{m} (d_i - d_i^*) \cdot b^i + \sum_{i=m+1}^{l} d_i \cdot b^i$$

   Ya que, es claro de ver que la diferencia en cuanto a la longitud de términos, será a partir del término $m+1$ hasta el l pertenecientes a la expresión n_1. Esto se puede representar de la siguiente manera:

$$\sum_{i=m+1}^{l} b^i \cdot d_i = d_{m+1} \cdot b^{m+1} + d_{m+2} \cdot b^{m+2} + \ldots + d_{l-1} \cdot b^{l-1} + d_l \cdot b^l$$

   También es importante notar que el resultado de dicha sumatoria será por lo menos el valor del último término de la sumatoria para todo valor de b y m. Y que a su vez, este último término será a lo menos el valor del primer término de la sumatoria. Lo anterior puede expresarse así:

$$\sum_{i=m+1}^{l} b^i \cdot d_i \geq b^l \geq b^{m+1}$$

   Ahora, recordemos nuestra propiedad del teorema de bases numéricas, que enuncia que $0 \leq d_i < b$. Definamos esta expresión para nuestros coeficientes en n_1 y n_2:

$$0 \leq d_i \leq b - 1$$

$$-b + 1 \leq -d_i^* \leq 0$$

   Estas expresiones se pueden unir de la siguiente forma:

$$-b + 1 \leq d_i - d_i^* \leq b - 1$$

   Apoyándonos en lo anterior, a continuación estimaremos el resultado de la sumatoria del producto de la base con potencia i por las diferencias de sus coeficientes d_i, en cuanto a sus términos de igual longitud. Esto, empleando la propiedad dada, correspondiente a la convergencia de la serie geométrica finita.

$$\sum_{i=0}^{m} (d_i - d_i^*) \cdot b^i \leq \sum_{i=0}^{m} (b-1) \cdot b^i = b^{m+1} - 1 < b^{m+1}$$

   Recapitulando, podemos reunir y resumir las expresiones resultantes de la siguiente forma:

$$\sum_{i=m+1}^{l} b^i \cdot d_i \geq b^l \geq b^{m+1} > b^{m+1} - 1 \geq \sum_{i=0}^{m} (d_i - d_i^*) \cdot b^i$$

   La expresión anterior implica que si dos representaciones de un número n en la base b tienen longitudes diferentes $l \neq m$, entonces la suma de los términos adicionales en la representación más larga, a partir de b^{m+1}, es mayor o igual a b^l. Al mismo tiempo, b^l es mayor o igual a b^{m+1} y es estrictamente mayor que la suma de las diferencias de coeficientes.

   Esta contradicción sugiere que la suposición inicial de tener dos longitudes diferentes no puede ser válida. Por lo tanto, concluimos que las dos representaciones deben tener la misma longitud $l = m$ para que n pueda ser correctamente representado en la base b. Esto demuestra la unicidad de la longitud l.

   En resumen, la ecuación destaca que si las longitudes difieren, entonces estaríamos considerando representaciones distintas de números distintos.

5. Ahora debemos hacer un argumento inductivo. Supongamos que tenemos $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$ con $0 \leq d_i^* < b$ y $0 \leq di < b$. Primero argumenta que $d_0 - d_0^*$ es divisible entre b y que $d_0 = d_0^*$.

   Partiendo desde la ecuación dada $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$. Excluiremos el primer término de ambas sumatorias y recorreremos el índice de estas:

$$d_0 \cdot b^0 + \sum_{i=1}^{l} d_i \cdot b^i = d_0^* \cdot b^0 + \sum_{i=1}^{l} d_i^* \cdot b^i$$

   Recordemos la definición de divisibilidad:

   - **Definición:** Decimos que $x|y$, donde $x, y \in \mathbb{Z}$ si existe $m \in \mathbb{Z}$ tal que $y = m \cdot x$

   Por lo que, es claro de ver que $b|d_0$ y $b|d_0^*$. Simplificando la primera ecuación, tenemos:

$$d_0 - d_0^* = \sum_{i=1}^{l} (d_i^* - d_i) \cdot b^i$$

   Puesto que nos interesa demostrar la divisibilidad por b del lado izquierdo de la ecuación, excluiremos el primer término de b^i de la sumatoria y ajustaremos los índices propiamente para mantener intacta la convergencia de ésta.

$$d_0 - d_0^* = b \cdot \sum_{i=1}^{l} (d_i^* - d_i) \cdot b^{i-1}$$

   Dado que $\sum_{i=1}^{l} (d_i^* - d_i) \cdot b^{i-1} \in \mathbb{Z}$, observemos que tenemos la forma $y = m \cdot x$. Por lo tanto:

$$b|d_0 - d_0^*$$

   Lo anterior es únicamente posible si $d_0 - d_0^*$ es un múltiplo de b. Y dado que, $-b < d_0 - d_0^* < b$ esto implica que el único múltiplo de b que lo cumple es el 0. De acuerdo con la propiedad 4 de divisibilidad vista en clase.

   Por lo tanto:

$$d_0 - d_0^* = 0 \leftrightarrow d_0 = d_0^*$$

6. Sabiendo que $d_0 = d_0^*$, argumenta que $d_1 - d_1^*$ es divisible entre b y, por tanto, $d_1 - d_1^* = 0$. (Pista: Muestra que $d_1 \cdot b - d_1^* \cdot b$ es divisible entre b^2).

   De forma similar al ejercicio anterior, emplearemos $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$. Excluiremos el primer y segundo término de ambas sumatorias y recorreremos el índice de estas:

$$d_0 \cdot b^0 + d_1 \cdot b^1 + \sum_{i=2}^{l} d_i \cdot b^i = d_0^* \cdot b^0 + d_1^* \cdot b^1 + \sum_{i=2}^{l} d_i^* \cdot b^i$$

   Cancelamos d_0 y d_0^* debido a la propiedad $d_0 = d_0^*$ probada anteriormente; y simplificamos la ecuación

$$(d_1 - d_1^*) \cdot b^1 = \sum_{i=2}^{l} (d_i^* - d_i) \cdot b^i$$

   Así como en el ejercicio anterior, excluiremos el prímer término de b^i de la sumatoria y ajustaremos los índices propiamente para mantener intacta la convergencia de ésta

$$(d_1 - d_1^*) \cdot b^1 = b^2 \sum_{i=2}^{l} (d_i^* - d_i) \cdot b^{i-2}$$

   Dado que $\sum_{i=2}^{l} (d_i^* - d_i) \cdot b^{i-2} \in \mathbb{Z}$, observemos que tenemos la forma $y = m \cdot x$. Por lo tanto:

$$b^2|(d_1 - d_1^*)b$$

   Y, simplificando dicha expresión, notaremos que llegaremos a una ecuación similar a la del ejercicio anterior:

$$b|d_1 - d_1^*$$

   Lo anterior es únicamente posible si $d_1 - d_1^*$ es un múltiplo de b. Y dado que, $-b < d_1 - d_1^* < b$ esto implica que el único múltiplo de b que lo cumple es el 0. De acuerdo con la propiedad 4 de divisibilidad vista en clase.

   Por lo tanto:

$$d_1 - d_1^* = 0 \leftrightarrow d_1 = d_1^*$$

   Notemos que, de manera inductiva, podemos probar que esto ocurre para cualquier d_i y d_i^* ya que siempre se podrán cancelar las potencias para cualquier base b dado que $i \in \mathbb{N}$. De esta forma, declaramos que:

$$d_i = d_i^*$$

7. Finalmente, asume que $d_i = d_i^*$. Argumenta que $d_{i+1} - d_{i+1}^* = 0$. Con esto, la prueba está completa.

   Similar a los ejercicios previos, excluiremos todos los elementos previos hasta el índice $i+1$ y emplearemos $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$. Recorriendo igualmente el índice de estas, a partir del cambio de variable $j = i + 2$:

$$\sum_{i=0}^{i} d_i \cdot b^i + d_{i+1} \cdot b^{i+1} + \sum_{j=i+2}^{l} d_j \cdot b^j = \sum_{i=0}^{i} d_i^* \cdot b^i + d_{i+1}^* \cdot b^{i+1} + \sum_{j=i+2}^{l} d_j^* \cdot b^j$$

   Cancelamos $\sum_{i=0}^{i} d_i \cdot b^i$ y $\sum_{i=0}^{i} d_i^* \cdot b^i$ debido a la propiedad $d_i = d_i^*$ probada anteriormente; y simplificamos la ecuación

$$(d_{i+1} - d_{i+1}^*) \cdot b^{i+1} = \sum_{j=i+2}^{l} (d_j^* - d_j) \cdot b^j$$

   Así como en los ejercicios anteriores, excluiremos el prímer término de b^j de la sumatoria y ajustaremos los índices propiamente para mantener intacta la convergencia de ésta

$$(d_{i+1} - d_{i+1}^*) \cdot b^{i+1} = b^{i+2} \sum_{j=i+2}^{l} (d_j^* - d_j) \cdot b^{j-i-2}$$

   Dado que $\sum_{j=i+2}^{l} (d_j^* - d_j) \cdot b^{j-i-2} \in \mathbb{Z}$, observemos que tenemos la forma $y = m \cdot x$. Por lo tanto:

$$b^{i+2}|(d_{i+1} - d_{i+1}^*)b^{i+1}$$

   Y, simplificando dicha expresión, nuevamente llegaremos a una ecuación similar a las ya conocidas:

$$b|d_{i+1} - d_{i+1}^*$$

   Lo anterior es únicamente posible si $d_{i+1} - d_{i+1}^*$ es un múltiplo de b. Y dado que, $-b < d_{i+1} - d_{i+1}^* < b$ esto implica que el único múltiplo de b que lo cumple es el 0. De acuerdo con la propiedad 4 de divisibilidad vista en clase.

   Por lo tanto:

$$d_{i+1} - d_{i+1}^* = 0 \leftrightarrow d_{i+1} = d_{i+1}^*$$

Algoritmo de Euclides

In [ ]:

```python
# Función que implementa el algoritmo de Euclides extendido para encontrar el MCD y la combinación lineal
def euclides(a, b):
    if b == 0:
        # Cuando b es 0, se ha alcanzado el MCD, y se devuelve el MCD, y los coeficientes x e y
        return a, 1, 0
    else:
        # Llamada recursiva con los argumentos (b, a % b)
        mcd, x, y = euclides(b, a % b)
        # Se devuelve el MCD y los coeficientes x e y actualizados
        return mcd, y, x - (a // b) * y

def main():
    # Ingresar los dos números para encontrar su MCD y la combinación lineal
    num1 = int(input("Ingresa el primer número: "))
    num2 = int(input("Ingresa el segundo número: "))

    # Llamada a la función euclides para obtener el MCD y los coeficientes
    mcd, coeficiente_num1, coeficiente_num2 = euclides(num1, num2)

    # Imprimir el resultado
    print(f"\nEl Máximo Común Divisor (MCD) de {num1} y {num2} es: {mcd}")
    print(f"Los coeficientes de la combinación lineal son: ({coeficiente_num1}, {coeficiente_num2})")
    print(f"Por lo tanto, el MCD se puede expresar como: {coeficiente_num1}*{num1} + {coeficiente_num2}*{num2} = {mcd}")

if __name__ == "__main__":
    main()
```

```
El Máximo Común Divisor (MCD) de 145 y 327 es: 1
Los coeficientes de la combinación lineal son: (106, -47)
Por lo tanto, el MCD se puede expresar como: 106*145 + -47*327 = 1
```