Numerical Bases and Euclid's Algorithm

Santiago Baca - A01656580

Numeric Bases

Theorem:

Given a number $b \in \mathbb{N}$ with $b \geq 2$ and $n \in \mathbb{N}$ with $n \neq 0$, there exist $l \in \mathbb{N}$ and $d_0, d_1, \ldots, uniqued_l \in \mathbb{N}$ such that:

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

$d_l \neq 0$ and for all $0 \leq i \leq l$ we have that $0 \leq di < b$

1. We will first show that such numbers exist. To do this, let's first do it for $b = 7$. Write all the steps to convert $(77)_{10}$ (seventy-seven base 10) to 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. Now write an algorithm to write any number in base 7.

   Input: A number n in base 10, where $n \in \mathbb{N}$, $n \neq 0$.

   Output: The base 7 representation of n, of the form $n = d_l \cdot 7^l + d_{l-1} \cdot 7^{l-1} + \ldots + d_1 \cdot 7^1 + d_0 \cdot 7^0$, where $0 \leq d_i < 7$.

   Step 1: Divide n by 7, and the remainder will be d_0.
   Step 2: Express n as $m_1 \cdot 7^1 + d_0 \cdot 7^0$ and observe m_1.
   Step 3: If $0 \leq m_1 < 7$, take m_1 as d_1 and finish the algorithm. Otherwise, divide m_1 by 7 and the remainder will be d_1.
   Step 4: Repeat from step 2 with $n = m_1$.

   This algorithm attempts to show that for any n and base $b = 7$, there exist $l \in \mathbb{N}$ and $d_0, d_1, \ldots, d_l \in \mathbb{N}$ unique that satisfy the given representation.

3. Finally, write a general algorithm to write a number in base b.

   Input: A number n, where $n \in \mathbb{N}$, $n \neq 0$.

   Output: The representation of n in base $b \geq 2$, of the form $n = d_l \cdot b^l + d_{l-1} \cdot b^{l-1} + \ldots + d_1 \cdot b^1 + d_0 \cdot b^0$, where $0 \leq d_i < b$.

   Step 1: Initialize $i = 0$ and coefficient list $d = [\,]$.
   Step 2: While $n \neq 0$, do the following steps:
   a) Calculate the remainder r and integer quotient c by dividing n by b.
   b) Add r to the list of coefficients d.
   c) Update $n = c$.
   d) Increase i by 1
   Step 3: The representation of n in base b is:
   $n = d_0 \cdot b^0 + d_1 \cdot b^1 + \ldots + d_{l-1} \cdot b^{l-1} + d_l \cdot b^l$

   This algorithm is valid for any n and $b \geq 2$. Step 2 is repeated until n becomes 0, accumulating the coefficients d_i representing the expansion of n in the base b. This also attempts to show that there are unique $l \in \mathbb{N}$ and $d_0, d_1, \ldots, d_l \in \mathbb{N}$ that satisfy the given representation.

4. Now we will prove uniqueness. Let's start with the uniqueness of l. Suppose it can be written with two different lengths. Use the fact that

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

   to show that both representations must have the same length.

   Suppose we can write a number n in two different representations in the base b with lengths l and m respectively, where $l \neq m$. So, we have:

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

   Since $l \neq m$, without loss of generality, let us assume that $l > m$. We subtract the first representation from the second:

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

   Which is equivalent to writing it such that:

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

   Since, it is clear to see that the difference in terms of the length of terms will be from the term $m+1$ to the l belonging to the expression n_1. This can be represented as follows:

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

   It is also important to note that the result of said summation will be at least the value of the last term of the summation for all values of b and m. And in turn, this last term will be at least the value of the first term of the sum. The above can be expressed like this:

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

   Now, let's remember our property of the number bases theorem, which states that $0 \leq d_i < b$. Let's define this expression for our coefficients on n_1 and n_2:

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

   These expressions can be joined in the following way:

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

   Based on the above, we will now estimate the result of the sum of the product of the base with power i by the differences of its coefficients d_i, in terms of its terms of equal length. This, using the given property, corresponding to the convergence of the finite geometric series.

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

   Recapitulating, we can gather and summarize the resulting expressions as follows:

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

   The above expression implies that if two representations of a number n in the base b have different lengths $l \neq m$, then the sum of the additional terms in the longer representation, starting at b^{m+1}, is greater than or equal to b^l. At the same time, b^l is greater than or equal to b^{m+1} and is strictly greater than the sum of the coefficient differences.

   This contradiction suggests that the initial assumption of having two different lengths cannot be valid. Therefore, we conclude that the two representations must have the same length $l = m$ so that n can be correctly represented in the basis b. This proves the uniqueness of length l.

   In summary, the equation highlights that if the lengths differ, then we would be considering different representations of different numbers.

5. Now we must make an inductive argument. Suppose we have $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$ with $0 \leq d_i^* < b$ and $0 \leq di < b$. First argue that $d_0 - d_0^*$ is divisible by b and that $d_0 = d_0^*$.

   Starting from the given equation $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$. We will exclude the first term of both sums and we will go through the index of these:

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

   Let's remember the definition of divisibility:

   - **Definition:** We say that $x|y$, where $x, y \in \mathbb{Z}$ if there exists $m \in \mathbb{Z}$ such that $y = m \cdot x$

   So, it is clear to see that $b|d_0$ and $b|d_0^*$. Simplifying the first equation, we have:

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

   Since we are interested in demonstrating the divisibility by b of the left side of the equation, we will exclude the first term of b^i from the sum and we will adjust the indices properly to keep its convergence intact.

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

   Since $\sum_{i=1}^{l} (d_i^* - d_i) \cdot b^{i-1} \in \mathbb{Z}$, let us note that we have the form $y = m \cdot x$. Therefore:

$$b|d_0 - d_0^*$$

   The above is only possible if $d_0 - d_0^*$ is a multiple of b. And since, $-b < d_0 - d_0^* < b$ this implies that the only multiple of b that satisfies it is 0. According to property 4 of divisibility seen in class.

   Therefore:

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

6. Knowing that $d_0 = d_0^*$, argue that $d_1 - d_1^*$ is divisible by b and therefore $d_1 - d_1^* = 0$. (Hint: Show that $d_1 \cdot b - d_1^* \cdot b$ is divisible by b^2).

   In a similar way to the previous exercise, we will use $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$. We will exclude the first and second terms of both sums and we will go through the index of these:

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

   Cancel d_0 and d_0^* due to the property $d_0 = d_0^*$ tested above; and we simplify the equation

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

   Just as in the previous exercise, we will exclude the first term of b^i from the sum and we will adjust the indices properly to keep its convergence intact.

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

   Since $\sum_{i=2}^{l} (d_i^* - d_i) \cdot b^{i-2} \in \mathbb{Z}$, notice that we have the form $y = m \cdot x$. Therefore:

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

   And, simplifying this expression, we will notice that we will arrive at an equation similar to the one in the previous exercise:

$$b|d_1 - d_1^*$$

   The above is only possible if $d_1 - d_1^*$ is a multiple of b. And since, $-b < d_1 - d_1^* < b$ this implies that the only multiple of b that satisfies it is 0. According to property 4 of divisibility seen in class.

   Therefore:

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

   Note that, inductively, we can prove that this occurs for any d_i and d_i^* since the powers can always be canceled for any base b given that $i \in \mathbb{N}$. In this way, we declare that:

$$d_i = d_i^*$$

7. Finally, assume that $d_i = d_i^*$, argue that $d_{i+1} - d_{i+1}^* = 0$. With this, the test is complete.

   Similar to the previous exercises, we will exclude all previous elements up to index $i + 1$ and use $n = \sum_{i=0}^{l} d_i \cdot b^i = \sum_{i=0}^{l} d_i^* \cdot b^i$. Also going through the index of these, starting from the change of variable $j = i + 2$:

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

   Cancel $\sum_{i=0}^{i} d_i \cdot b^i$ and $\sum_{i=0}^{i} d_i^* \cdot b^i$ due to the property $d_i = d_i^*$ previously tested; and we simplify the equation

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

   Just as in the previous exercises, we will exclude the first term of b^j from the sum and we will adjust the indices properly to keep its convergence intact.

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

   Since $\sum_{j=i+2}^{l} (d_j^* - d_j) \cdot b^{j-i-2} \in \mathbb{Z}$, notice that we have the form $y = m \cdot x$. Therefore:

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

   And, simplifying said expression, we will again arrive at an equation similar to those already known:

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

   The above is only possible if $d_{i+1} - d_{i+1}^*$ is a multiple of b. And since, $-b < d_{i+1} - d_{i+1}^* < b$ this implies that the only multiple of b that satisfies it is 0. According to property 4 of divisibility seen in class.

   Therefore:

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

Algoritmo de Euclides

In [ ]:
```
# Function that implements the extended Euclid algorithm to find the GCD and the linear combination
def euclides(a, b):
    if b == 0:
        # When b is 0, the GCD has been reached, and the GCD, and the coefficients x and y are returned
        return a, 1, 0
    else:
        # Recursive call with arguments (b, a % b)
        mcd, x, y = euclides(b, a % b)
        # The GCD and the updated x and y coefficients are returned
        return mcd, y, x - (a // b) * y

def main():
    # Enter the two numbers to find their GCD and the linear combination
    num1 = int(input("Enter the first number: "))
    num2 = int(input("Enter the second number: "))

    # Call the euclid function to obtain the GCD and the coeffcients
    mcd, coeficiente_num1, coeficiente_num2 = euclides(num1, num2)

    # Print the result
    print(f"\nThe Greatest Common Divisor (GCD) of {num1} and {num2} is: {mcd}")
    print(f"The coefficients of the linear combination are: ({coeficiente_num1}, {coeficiente_num2})")
    print(f"Therefore, the GCF can be expressed as: {coeficiente_num1}*{num1} + {coeficiente_num2}*{num2} = {mcd}")

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

```
The Greatest Common Divisor (GCD) of 145 and 327 is: 1
The coefficients of the linear combination are: (106, -47)
Therefore, the GCF can be expressed as: 106*145 + -47*327 = 1
```