Representación en Bases

Alan Reyes-Figueroa

Teoría de Números (Aula 10) 02.agosto.2024

Bases

La notación usual para números naturales es llamada la notación **base 10**, con dígitos $0, 1, 2, \ldots, 9$. Esto significa por ejemplo, que

$$196883 = 1 \cdot 10^5 + 9 \cdot 10^4 + 6 \cdot 10^3 + 8 \cdot 10^2 + 8 \cdot 10^1 + 3 \cdot 10^0.$$

El siguiente resultado muestra cómo escribir cualquier natural en cualquier base $d > 1$.

Teorema (Representación en Bases)

Sean $n \in \mathbb{N}$, y $d > 1$. Existe una única secuencia (los dígitos de n en la base d) $a_0, a_1, \ldots, a_k, \ldots$ con las siguientes propiedades

1. *para todo $k \in \mathbb{N}$, $0 \leq a_k < d$,*
2. *existe $m \in \mathbb{N}$ tal que $a_k = 0$, para todo $k \geq m$,*
3. *$n = \sum_{k \geq 0} a_k d^k$.*

<u>Prueba</u>: Usando el Algoritmo de la División, escribimos $n = n_0 = n_1 d + a_0$, $0 \leq a_0 < d$, $n_1 = n_2 d + a_1$, $0 \leq a_1 < d$; y en general, $n_k = n_{k+1} d + a_k$, con $0 \leq a_k < d$, y vale (1).

Bases

Afirmamos primero que $n_k = 0$, para algún $k \in \mathbb{N}$. De hecho, si $n_0 < d^m$, entonces $n_1 = \lfloor \frac{n_1}{d} \rfloor < d^{m-1}$, y, más generalmente, por inducción se muestra que $n_k < d^{m-k}$. En particular, para $k \geq m$, tenemos $n_k < 1 \;\Rightarrow\; n_k = 0$.
Se sigue de ahí que $a_k = 0$, para todo $k \geq m$, lo que muestra (2).

Para mostrar (3), procedemos por inducción sobre $m+1$ el número de dígitos a_j no nulos. Para $m = 0$, $n = a_0 < d \;\Rightarrow\; n = a_0 = a_0 \cdot d^0$, y se cumple la representación. Supongamos válida la propiedad para todo número entero con a lo sumo m dígitos en su representación base d. Entonces, si $n = (a_m \cdots a_1 a_0)_d$, tenemos que $n = dn_1 + a_0$. En particular $n_1 = (a_m \cdots a_1)_d$. Por la hipótesis inductiva aplicada a n_1

$$n = dn_1 + a_0 = d\Big(\sum_{j=0}^{m-1} a_{j+1} d^j\Big) + a_0 = \sum_{j=0}^{m-1} a_{j+1} d^{j+1} + a_0 = \sum_{j=1}^{m} a_j d^j + a_0 = \sum_{j=0}^{m} a_j d^j.$$

Para la unicidad, suponga que n admite dos representaciones en base d: $\sum_{k\geq 0} a_k d^k = n = \sum_{k\geq 0} b_k d^k$. Si las secuencias $\{a_k\}$ y $\{b_k\}$ son distintas, existe un menor índice j tal que $a_j \neq b_j$. Tomamos

Bases

$$a_j + \sum_{k>j} a_k d^{k-j} = b_j + \sum_{k>j} b_k d^{k-j} \quad \Rightarrow \quad a_j - b_j = \sum_{k>j} (b_k - a_k) d^{k-j},$$

lo que muestra que $d \mid a_j - b_j$. Pero $0 \leq a_k, b_k < d \;\Rightarrow\; 0 \leq |a_j - b_j| < d$, implica que $a_j - b_j = 0$, y portanto $a_j - b_j$ no puede ser un múltiplo de d, un absurdo. Esto muestra que la representación en base d es única. $\square$

Notación: Ignorando los ceros iniciales, escribimos $n = (a_m a_{m-1} \cdots a_1 a_0)_d = \sum_{k=0}^{m} a_k d^k$, y llamamos a ésta la **representación en base** d **de** n.

Ejemplo: La representación binaria de $n = 105$ es

$$105 = 1\dot{2}^6 + 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 0\dot{2} + 1 = 2^6 + 2^5 + 2^3 + 1,$$

o, en forma compacta, $105 = (1101001)_2$.

Ejemplo: Por otro lado, la representación $(1001111)_2$ corresponde a

$$n = 1 \cdot 2^6 + 0 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 1 \cdot 2^2 + 1 \cdot 2 + 1 = 2^6 + 2^3 + 2^2 + 1 = 79.$$

Potenciación Modular

Aplicación: Cálculo de potencias grandes módulo n.

Con frecuencia deseamos calcular el valor de una potencia $a^k \pmod{n}$, cuando k es grande. ¿Existe una forma eficiente de obtener este cálculo?

Uno de esos procedimientos, es llamado el **algoritmo exponencial binario**, y se basa en elevar al cuadrado de forma sucesiva, módulo n.
Más específicamente, el exponente k se escribe en forma binaria, como

$$k = (b_m b_{m-1} \cdots b_2 b_1 b_0)_2 = \sum_{i=0}^{m} b_i\, 2^i, \qquad \text{con } b_i = 0 \text{ ó } b_i = 1.$$

Luego

$$a^k = a^{\sum_{i=0}^{m} b_i\, 2^i} = \prod_{i=0}^{m} a^{b_i\, 2^i} = \prod_{b_i=1} a^{2^i} \pmod{n}.$$

y los valores $a^{2^i} \pmod{n}$ se calculan para las potencias de 2, que corresponden a los 1's en la representación binaria de k, y se multiplican.

Potenciación Modular

Ejemplo: Calcular $5^{110} \pmod{131}$.

Primero, expresamos el exponente 110 en base 2 como

$$110 = 64 + 32 + 8 + 4 + 2 = 2^6 + 2^5 + 2^3 + 2^2 + 2^1 = (1101110)_2.$$

Obtenemos ahora las potencias de $5^{2^j} \pmod{131}$, correspondientes a los 1's en la representación anterior:

$$\begin{aligned}
5^2 &\equiv 25 \pmod{131},\\
5^4 &\equiv 25^2 \equiv 625 \equiv 101 \pmod{131},\\
5^8 &\equiv 101^2 \equiv 10201 \equiv 114 \pmod{131},\\
5^{16} &\equiv 114^2 \equiv 12996 \equiv 27 \pmod{131},\\
5^{32} &\equiv 27^2 \equiv 729 \equiv 74 \pmod{131},\\
5^{64} &\equiv 74^2 \equiv 5476 \equiv 105 \pmod{131}.
\end{aligned}$$

Potenciación Modular

Multiplicamos ahora los resultados parciales, correspondientes a los 1's en la expansión binaria del exponente

$$5^{110} = 5^{64} \cdot 5^{32} \cdot 5^{8} \cdot 5^{4} \cdot 5^{2} \equiv 105 \cdot 74 \cdot 114 \cdot 101 \cdot 25 \equiv 60 \pmod{131}.$$

Como una variación del procedimiento anterior, se podrían calcular módulo 131, las potencias $5^2, 5^3, 5^6, 5^{12}, 5^{24}, 5^{48}, 5^{96}$ para llegar al resultado

$$5^{110} = 5^{96} \cdot 5^{12} \cdot 5^{2} \equiv 41 \cdot 117 \cdot 25 \equiv 60 \pmod{131},$$

lo que requeriría menos multiplicaciones.

Potenciación Modular

Teorema

Sea $P(x) = \sum_{k=0}^{m} c_k x^k$ *una función polinomial de x, con coeficientes enteros* $c_k \in \mathbb{Z}$*. Si* $a \equiv b \pmod{n}$*, entonces* $P(a) \equiv P(b) \pmod{n}$*.*

Prueba: Como $a \equiv b \pmod{n}$, de las propiedades de congruencias, tenemos que $a^k \equiv b^k \pmod{n}$, para todo $k = 0, 1, 2, \ldots, m$. Luego, $c_k a^k \equiv c_k b^k \pmod{m}$, para todo $k = 0, 1, 2, \ldots, n$. Sumando todas estas congruencias, se obtiene

$$P(a) = \sum_{k=0}^{m} c_k a^k \equiv \sum_{k=0}^{m} c_k b^k = P(b) \pmod{n}.$$

Corolario

Si a es una solución de $P(x) \equiv 0 \pmod{n}$ *y* $a \equiv b \pmod{n}$*, entonces b también es una solución.*

Prueba: Del teorema, $a \equiv \pmod{n}$ implica que $P(a) \equiv P(b) \pmod{n}$. Por tanto, si a es una solución de $P(x) \equiv 0 \pmod{n}$, entonces $P(b) \equiv P(a) \equiv 0 \pmod{n}$, y b una solución.