Matemática discreta

«[…] El desarrollo tecnológico ha actuado en cada momento histórico como freno o impulsor de las expectativas científicas. En las últimas décadas, ese desarrollo ha influido enormemente en la expansión y profundización del estudio de problemas y teorías de antiguo origen, dando lugar a nuevas ciencias, enfoques y metodologías.

[…] Un ejemplo de ello lo proporciona la disciplina de computación, que se ha extendido y profundizado en diferentes direcciones y bajo diferentes nombres: ciencia de la computación, ingeniería en computación, informática, etc., cuya base común es, como siempre lo ha sido, el hecho de que se trata de una actividad matemática que ha tomado también forma y nombre como la rama llamada Matemática Discreta. Como su nombre lo indica, en matemática discreta se trabaja con conjuntos discretos, a diferencia de la matemática continua, que trabaja conjuntos continuos, como los números reales.

[…] El computador digital moderno es básicamente un sistema discreto y muchas de sus propiedades pueden ser entendidas y descritas modelándolas en un sistema matemático discreto.

[…] La matemática discreta debe su intenso desarrollo de los últimos años a la comunidad científica relacionada con las ciencias de la computación y en lo que se refiere a la educación, los estudios terciarios en dicha ciencia han incorporado cursos de matemática discreta con alta prioridad. Sin embargo, fuera del área de las ciencias de la computación, la matemática discreta es prácticamente inexistente y esta situación es la que creemos que debe corregirse, ya que consideramos que los estudios en matemática discreta son importantes para la formación de cualquier estudiante, aun de aquellos que no continúen estudios terciarios.

[…] hemos constatado a través de tests realizados a estudiantes del curso de Matemática Discreta del primer año de la carrera de Ingeniería en Computación, que los estudiantes desconocen los conjuntos y sus propiedades (todo se reduce al conjunto de los reales) y aplican incorrectamente los métodos de prueba más elementales por falta de una sólida base en lógica.

[…] este trabajo presenta una propuesta para comenzar a actualizar la enseñanza de matemática al nivel de enseñanza media. En pocas palabras, consiste en tomar de los programas actuales los temas de matemática discreta, como ser teoría de conjuntos, relaciones, funciones, combinatoria, inducción completa, divisibilidad, e introducirlos con un enfoque alternativo que rescate la naturaleza discreta de los mismos, al mismo tiempo permita dedicarles mayor tiempo y profundidad, relacionándolos entre ellos.

[…] queremos resaltar, una vez más, que aunque la actualización de la educación matemática en el sentido que proponemos redundará en un beneficio para todos los estudiantes, es innegable que la formación de los estudiantes que seguirán estudios terciarios en ciencias de la computación se verá enormemente favorecida».

Extraído de: Sylvia da Rosa, *La matemática discreta como formación básica*. Montevideo, Instituto de Computación, Facultad de Ingeniería.

5

DIVISIBILIDAD NUMÉRICA

En los números naturales

1 – INTRODUCCIÓN

En este capítulo se usarán solo los **números naturales** 0, 1, 2, 3, ... de modo que la resta de dos naturales diferentes no puede ser menor que uno (**si** $a \in \mathbb{N}$ $b \in \mathbb{N}$ $a - b \geq 1$ **con** $a > b$), que es la menor cantidad que hay entre un natural y otro.

2 – DEFINICIÓN DE DIVISIÓN ENTERA

Sean dos números naturales **a** (**dividendo**) y **b** (**divisor**) tales que $b \neq 0$ y $a \geq b$.
Dividir **a** *entre* **b** *consiste en encontrar dos números naturales* **q** (**cociente**) *y* **r** (**resto**) *que cumplan simultáneamente dos condiciones:*

$$a = bq + r \quad \text{y} \quad r < b$$

Nótese que **q** y **r** *existen* (véase punto 3) y son *únicos* (véase punto 4)

Esta división entera suele indicarse con el siguiente esquema utilizado al practicar la operación:

a	b
r	q

El punto encima de la letra b significa *múltiplo* de b.

Si el resto **r** es nulo **(r = 0)**, resulta que **a** es múltiplo de **b** $(a = \dot{b})$. También se dice que **a** es divisible entre **b**. Ello se expresa mediante el símbolo **b/a**.

Por lo tanto, **b/a** (**b** divide a **a**) si y solo si existe un natural **q** tal que $a = bq$.

a	b
0	q

$a = bq$ $\quad \begin{cases} a = \dot{b} \rightarrow (\textbf{a} \text{ es múltiplo de } \textbf{b}) \\ b/a \rightarrow (\textbf{b} \text{ divide a } \textbf{a}) \end{cases}$

A este caso particular de división entera se le llama *división exacta*.

NOTA

Se puede utilizar una notación de conjuntos para hacer referencia a los números que dividen exactamente a otros. A todos los números que dividen exactamente a **a**, se los denomina divisores de **a** y se anotan:

$d(a) \rightarrow$ conjunto de divisores de **a**

EJEMPLO:

$d(6) = \{1, 2, 3, 6\}$

Caso particular: $d(0) = \mathbb{N}^*$ $\quad \mathbb{N}^* = \mathbb{N} - \{0\}$

3 – EXISTENCIA DEL COCIENTE Y EL RESTO

Para determinar el cociente **q** y el resto **r** en una división entera, se forma la sucesión creciente de naturales de término general $(i\,b)$ con $i = 1, 2, 3, \ldots$ cuyos valores sean menores que **a**.

$$b < 2b < 3b < 4b < \ldots < (q-1)b < qb < a$$

Como el conjunto de estos naturales de la forma $(i\,b)$ es acotado, pues cualquier término de la sucesión es menor que **a**, entonces es finito y tiene un último término, al que se llamará $b\,q$.

La diferencia $r = a - bq$ debe ser menor que **b** $(r < b)$, pues si fuese $r > b$ existiría un término $(q+1)b < a$, lo que contradice la suposición de que **qb** es el último término de la sucesión.

Entonces se cumple que: $a = bq + r$ con $r < b$

DIV y MOD

En lenjuages informáticos es común el uso de las funciones DIV y MOD.

En la siguiente división entera, con $a \geq b$.

$$\begin{array}{r|l} a & b \\ \hline r & q \end{array}$$

q = a DIV b

r = a MOD b

La función DIV da el cociente de una división entera, y la función MOD da el resto de la división entera.

4 – UNICIDAD DE LA DIVISIÓN ENTERA

El cociente y el resto de una división entera son únicos.

Hipótesis: $a = bq + r$ con $r < b$; $a = bq' + r'$ con $r' < b$; $a \geq b$, $b \neq 0$ Tesis: $q = q'$ $r = r'$

La demostración se hace por el absurdo, suponiendo que existen dos cocientes **q** y **q'** y dos restos **r** y **r'**.

Primer paso: si **q > q'**

Por hipótesis, se cumple:

$$a = a \Rightarrow bq + r = bq' + r' \Rightarrow bq - bq' + r = r' \Rightarrow b(q - q') + r = r'$$

Dado que se supone **q > q'** resulta que la diferencia entre estos dos valores es mayor o igual a uno: $(q - q') \geq 1$

Multiplicando por **b** ambos miembros de esta desigualdad se obtiene que: $b(q - q') \geq b$. Si se suma **r** al primer miembro, resulta que: $b(q - q') + r > b$ (recuérdese que $b > 0$ por ser un natural no nulo).

Como por hipótesis $b(q - q') + r = r'$ se tendría que $r' > b$, lo que contradice la hipótesis de que $r' < b$. Por lo tanto, lo erróneo es suponer que **q** es mayor que **q'**.

Segundo paso: si **q < q'**

Por hipótesis, se cumple:

$$a = a \Rightarrow bq + r = bq' + r' \Rightarrow r = bq' - bq + r' \Rightarrow r = b(q' - q) + r'$$

Dado que se supone que $q < q'$ resulta que la diferencia entre estos dos valores es mayor o igual a uno: $(q' - q) \geq 1$

Si se multiplica por **b** ambos miembros de esta desigualdad, se obtiene que: $b(q' - q) \geq b$. Si se suma **r'** al primer miembro, resulta que: $b(q' - q) + r' > b$.

Como por hipótesis $b(q' - q) + r' = r$ se tendría que $r > b$, lo que contradice la hipótesis de que $r < b$. Por lo cual es erróneo suponer que **q** es menor que **q'**.

Si **q** no es ni mayor ni menor que **q'**, debe cumplirse que: $q = q'$ Y al cumplirse esta igualdad, se obtiene al hacer la siguiente resta que:

$$\begin{array}{r} a = bq + r \\ - \; a = bq + r' \\ \hline 0 = r - r' \end{array}$$

$r = r'$ → Esto prueba que el cociente y el resto de una división entera son únicos.