Material de Apoyo
14 de Septiembre de 2011

1. Notación Usual

$\mathbb{N}$	Los números naturales $\{1, 2, 3, \ldots\}$.
$\mathbb{Z}$	Los enteros $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$.
$\mathbb{Q}$	Los números racionales (fracciones).
$\mathbb{R}$	Los números reales.
$\mathbb{P}$	Los números primos $\{2, 3, 5, 7, 11, \ldots\}$.
$]a, b[$	El intervalo $\{x \in \mathbb{R} : a < x < b\}$.
$[a, b]$	El intervalo $\{x \in \mathbb{R} : a \leq x \leq b\}$.
$]a, b]$	El intervalo $\{x \in \mathbb{R} : a < x \leq b\}$.
$[a, b[$	El intervalo $\{x \in \mathbb{R} : a \leq x < b\}$.
$]a, +\infty[$	El intervalo $\{x \in \mathbb{R} : x > a\}$.
$[a, +\infty[$	El intervalo $\{x \in \mathbb{R} : x \geq a\}$.
$]-\infty, a[$	El intervalo $\{x \in \mathbb{R} : x < a\}$.
$]-\infty, a]$	El intervalo $\{x \in \mathbb{R} : x \leq a\}$.
$\lfloor x \rfloor$	El único entero que satisface $x - 1 < \lfloor x \rfloor \leq x$.
$\lceil x \rceil$	El único entero que satisface $x < \lceil x \rceil \leq x + 1$.
$\{x\}$	Parte fraccionaria de x.
$x \in X$	x pertenece a X.
$A \subset B$	A esta contenido en B.
$\forall$	Para todo.
$\exists$	Existe.
$\exists!$	Existe un único.
$\Rightarrow$	Implica.
$\Longleftrightarrow$	Si, y solo si.
$\therefore$	Por lo tanto.
$\blacksquare$	Lo cual queriamos demostrar.

2. Divisibilidad y Primos

2.1. Divisibilidad

Definición 1. *Un entero b es divisible por un entero a, no cero, si existe un entero x tal que $b = ax$ y se escribe $a \mid b$. En el caso en que no sea divisible por a se escribe $a \nmid b$.*
En ocasiones se usa la notación $a \,||\, b$, para indicar $a^k \mid b$, pero $a^{k+1} \nmid b$.

Teorema 1. *Dados $a, b, c \in \mathbb{Z}$ tenemos que:*

1. *$a \mid b$ implica $a \mid bc$ para cualquier entero c;*
2. *$a \mid b$ y $b \mid c$ implica $a \mid c$;*
3. *$a \mid b$ y $a \mid c$ implica $a \mid (bx + cy)$ para cualquiera enteros x y y;*
4. *$a \mid b$ y $b \mid a$ implica $a = \pm b$;*
5. *$a \mid b$, $a > 0, b > 0$, implica $a \leq b$.*

Teorema 2. *El algoritmo de la división. Dados dos enteros cualesquiera a y b, con $a \geq 0$, existen los enteros q y r tales que $b = qa + r$, $0 \leq r \leq a$. Si $a \mid b$, entonces r satisface las desigualdades más fuertes $0 < r < a$.*

Definición 2. *Si $k \mid a$ y $k \mid b$, entonces se dice que k es un divisor común o un factor común de a y b.*
Se dice que g es el máximo común divisor de a y b, si g es el mayor de los divisores comunes a a y b, y se denota por (a, b).

Teorema 3. *Si g es el máximo común divisor de b y c, entonces existen los enteros x_0 e y_0 tales que $g = (b, c) = bx_0 + cy_0$.*

Teorema 4 (El algoritmo euclideano)**.** *Dados los enteros b y $c > 0$, se hace una aplicación repetida del algoritmo de la división,*

$$\begin{array}{rcll} b & = & cq_1 + r_1 & 0 < r_1 < c, \\ c & = & r_1q_2 + r_2 & 0 < r_2 < r_1, \\ r_1 & = & r_2q_3 + r_3 & 0 < r_3 < r_2, \\ & \vdots & & \vdots \\ r_{j-2} & = & r_{j-1}q_j + r_j & 0 < r_j < r_{j-1}, \\ r_{j-1} & = & r_jq_{j+1} & \end{array}$$

$\Rightarrow (b, c) = r_j$, *los valores* x_0 *y* y_0 *en* $(b, c) = bx_0 + cy_0$ *pueden obtenerse eliminando* $r_1, r_2, \ldots, r_{j-1}$ *en el conjunto de ecuaciones.*

Definición 3. *Sean* $a, b \in \mathbb{Z}$*, el menor de los múltiplos de* a *y* b *recibe el nombre de mínimo común múltiplo y se denota por* $[a, b]$*.*