Aritmética

Vazquez Rocha Jorge Ivan

Escuela Superior de Física y Matemáticas
Instituto Politécnico Nacional

03/02/20

Aritmética

Divisibilidad

Dados dos números enteros a y b (con $a \neq 0$), se dice que a divide a b, y lo escribimos como $a \mid b$, si existe un $c \in Z$ tal que $b = ac$.

Máximo común divisor

Dados dos enteros a y b distintos de 0, decimos que el entero $d > 1$ es un máximo común divisor, o *mcd*, de a y b

si $d \mid a$, $d \mid b$ y para cualquier otro $c \in Z$ tal que $c \mid a$ y $c \mid b$, entonces $c \mid d$.

Algoritmo de la división

Dados $a, b \in Z$, *con* $b \neq 0$, existen dos únicos números enteros q, r tales que:

$$a = bq + r \qquad 0 \leq r < |b|$$

Algoritmo de Euclides

Para calcular el *mcd* de dos enteros a y b (ambos > 0, suponemos $a > b$) se definen q_i y r_i recursivamente mediante las ecuaciones:

$$\begin{aligned}
a &= bq_1 + r_1 & (0 < r_1 < b) \\
b &= r_1 q_2 + r_2 & (0 < r_2 < r_1) \\
r_1 &= r_2 q_3 + r_3 & (0 < r_3 < r_2) \\
&\vdots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} & (0 < r_{k-1} < r_{k-2}) \\
r_{k-2} &= r_{k-1} q_k + r_k & (r_k = 0)
\end{aligned}$$

Y de la proposición anterior, se sigue que:

$$mcd(a, b) = mcd(b, r_1) = mcd(r_1, r_2) = \cdots = mcd(r_{k-2}, r_{k-1}) = r_{k-1}$$

Teorema chico de Fermat

Si p es un número primo, entonces, para cada número natural a, con $a > 0$, $a^p = a(mod\ p)$