Teoría de enteros
Matemática Estructural y Lógica

Miguel De Ávila

3 de noviembre de 2017

Axiomas de Peano

Los números naturales pueden definirse con ayuda de los axiomas de Peano. Los axiomas se expresan en términos del 0 y la función sucesor $S : \mathbb{N} \to \mathbb{N}$.

1. $0 \in \mathbb{N}$
2. $(\forall n : \mathbb{N} | : S(n) \in \mathbb{N})$
3. $(\forall n : \mathbb{N} | : S(n) \neq 0)$
4. $(\forall n, m : \mathbb{N} | S(n) = S(m) : n = m)$
5. $(\forall A : \mathbb{P}(\mathbb{N}) | 0 \in A \wedge (\forall n : A | : S(n) \in A) : A = \mathbb{N})$.

Una vez definidos los números naturales es posible definir los números enteros y las operaciones de suma y multiplicación.

Principio del buen orden

El axioma 5 de los axiomas de Peano es equivalente al principio del buen orden, que establece lo siguiente:

Teorema

Sea $A \subseteq \mathbb{N}$ un conjunto de números naturales tal que $A \neq \emptyset$. Entonces A tiene un elemento mínimo. Es decir: existe un a tal que:

1. $a \in A$.
2. $(\forall b : A| : a \leq b)$.

La relación $|$

Recordemos la definición de la relación divide: $| : \mathbb{Z} \leftrightarrow \mathbb{Z}$ donde

$$a|b \equiv (\exists c : \mathbb{Z} | : b = ac)$$

En caso de que $a|b$ se dice que a divide a b o que b es múltiplo de a.

Teoremas de $|$

Los siguientes son algunos teoremas importantes sobre $|$. a, b y c son enteros cualesquiera.

1. $a|b \Rightarrow a|bc$.
2. $a|b \wedge b|c \Rightarrow a|c$.
3. $a|b \wedge a|c \Rightarrow a|(mb + nc)$.
4. $c \neq 0 \Rightarrow (ca|cb \equiv a|b)$.
5. $a|b \wedge b|a \Rightarrow |a| = |b|$.
6. $(a|b) \wedge (a > 0) \wedge (b > 0) \Rightarrow a \leq b$.

Números primos

Un número natural p se dice primo si $p > 1$ y los únicos divisores de p son 1 y p. O sea:

$$primo(p) \equiv p > 1 \wedge (\forall d : \mathbb{N} | d > 0 \wedge d | p : d = 1 \vee d = p)$$

Más adelante veremos que existen infinitos números primos.

Algoritmo de la división

El algoritmo de la división afirma que dados dos enteros: un dividendo y un divisor, si el divisor es distinto de 0 entonces podemos encontrar un cociente y un residuo:

Teorema

Sean $n, d \in \mathbb{Z}$ *con* $d > 0$. *Entonces existen* q, r *tal que* $0 \leq r < d$ *y* $n = qd + r$. *Más aún,* q *y* r *son únicos.*

Como el teorema garantiza que q y r son únicos podemos definir dos funciones importantes.

$\div$ y *mod*

Definimos las funciones $\div$ y *mod* así:

$$n \div d = q \text{ donde } q \text{ y } r \text{ son tal que } n = qd + r.$$
$$n \bmod d = r \text{ donde } q \text{ y } r \text{ son tal que } n = qd + r.$$

Entonces $n \div d$ es el cociente de la división entera de n entre d, mientras que $n \bmod d$ es el residuo de la misma.
Por ejemplo, $-17 \div 6 = -3$, $-17 \bmod 6 = 1$.

mcd y mcm

Definimos las funciones mcd, mcm.

$$mcd, mcm : \mathbb{Z} \leftrightarrow \mathbb{Z}$$

$$mcd(b, c) = (\max d : \mathbb{N} | (d|b \wedge d|c) : d) \text{ si } b \neq 0 \vee c \neq 0$$
$$mcd(0, 0) = 0.$$

$$mcm(b, c) = (\min d : \mathbb{N} | (b|d \wedge c|d) : d) \text{ si } b \neq 0 \vee c \neq 0$$
$$mcm(0, 0) = 0.$$

Propiedades del mcd

Algunas propiedades importantes del *mcd*:

1. $mcd(b, c) = mcd(c, b)$.
2. Si $b \neq 0$ o $c \neq 0$ entonces
   $mcd(b, c) = (\min x, y | bx + cy > 0 : bx + cy)$.
3. $mcd(b, mcd(c, d)) = mcd(mcd(b, c), d)$
4. $d|c \wedge d|b \Rightarrow d|mcd(b, c)$.
5. $mcd(b, b) = |b|$.
6. $mcd(b, 1) = 1$.
7. $mcd(b, c) = mcd(b, b + c) = mcd(b, b - c)$.
8. $d > 0 \Rightarrow d \cdot \text{mcd}(b, c) = mcd(db, dc)$.
9. $d|bc \wedge mcd(d, c) = 1 \Rightarrow d|b$.

Algoritmo de Euclides

Utilizando el hecho de que $mcd(b, c) = mcd(c, b \bmod c)$. Se propone el siguiente algoritmo para calcular el *mcd* de b y c:

$$
\begin{aligned}
&x = b;\\
&y = c;\\
&while(y! = 0)\{\\
&\quad x_1 = x;\\
&\quad x = y;\\
&\quad y = x_1 \bmod x;\\
&\}
\end{aligned}
$$

Al final, $x = mcd(b, c)$. Por ejemplo, calculemos $mcd(963, 657)$. Es posible extender este algoritmo para hallar los *coeficientes de Bézout* de b y c, o sea x e y tales que $mcd(b, c) = bx + cy$.

Más sobre primos

El siguiente teorema nos será útil:

Teorema

Si p es primo y $p|ab$ entonces $p|a$ o $p|b$.

Demostración.

Si $p|a$ entonces se tiene el resultado. Si $p \not| a$, entonces $mcd(a, p) = 1$. Por el resultado 9 de las propiedades del mcd, entonces $p|b$. De cualquier modo, $p|a \vee p|b$. □

Teorema fundamental de la aritmética

Teorema

Sea n un número natural, $n > 1$. Entonces n es un producto de primos:

$$n = p_1 \dots p_n$$

Además, $p_1, \dots, p_n$ son únicos salvo orden.

Usos del teorema fundamental

Teorema

Existen infinitos primos

Demostración.

Suponga por contradicción que no. Entonces $p_1, \ldots, p_k$ *es una lista con todos los primos que existen. Considere* $n = p_1 \ldots p_k + 1$. *Por el teorema fundamental de la aritmética,* n *es un producto de primos, pero ninguno de los* p_i *divide a* n, *porque de lo contrario dividirían a* 1, *lo cual es imposible. Entonces* n *debe ser primo, pero entonces encontramos un nuevo primo que no estaba en la lista, lo cual nos da la contradicción deseada.* □

Teorema

$\text{mcd}(b, c) \cdot \text{mcm}(b, c) = bc$

Congruencias

Definición

Sea m un entero con $m \neq 0$. Definimos la siguiente relación: $=_m$: $\mathbb{Z} \leftrightarrow \mathbb{Z}$ dada por

$$a =_m b \equiv m|(b-a)$$

Se lee: a congruente módulo m a b. También es usual escribir $a \equiv_m b$.

Es fácil ver que $=_m$ es una relación de equivalencia.

Propiedades de congruencias

Teorema

1. $a =_m b \equiv res(a, m) = res(b, m)$.
2. $=_m$ *es una relación de equivalencia.*
3. $a =_m b \Rightarrow a + c =_m b + c$.
4. $a =_m b \Rightarrow ac =_m bc$
5. $a =_m b \wedge c =_m d \Rightarrow (a + c) =_m (b + d)$.
6. $a =_m b \wedge c =_m d \Rightarrow ac =_m bd$.

Clase de equivalencia de $=_m$

Como $=_m$ es una relación de equivalencia, podemos calcular la clase de equivalencia de un entero a. El numeral 1 del teorema nos dice que

$$[a] = \{x| : x \bmod m = a \bmod m\} = [a \bmod m]$$

Entonces podemos identificar cada clase de equivalencia con el residuo que dejan sus elementos al ser divididos por m, o sea $a \bmod m$.

Más propiedades del módulo

Teorema

1. $(ax =_m ay \wedge mcd(a, m) = 1 \Rightarrow x =_m y)$.
2. $x =_m y \wedge d|m \Rightarrow x =_d y$.

Teorema de Fermat

El teorema de Fermat nos da una propiedad interesante para congruencias con exponentes primos:

Teorema

Sea p un primo que no divide a a. Entonces $a^{p-1} =_p 1$.

Función ϕ de Euler

Definición

Se dice que m y n son *primos relativos* (y se escribe $m \perp n$) si $mcd(m, n) = 1$.

Definición

Definimos la función ϕ de Euler así:

$$\phi(n) = (+k|0 < k \leq n \wedge k \perp n : 1)$$

Esta función cumple las siguientes dos propiedades:

1. Si p es primo, $\phi(p) = p - 1$.
2. Si $p \perp q$ entonces $\phi(pq) = \phi(p) \cdot \phi(q)$.

Teorema de Euler

Teorema

Sean a, m enteros tal que $a \perp m$. Entonces

$$a^{\phi(m)} =_m 1$$