AMPLIACIÓN DE MATEMÁTICAS

DIVISIBILIDAD DE NÚMEROS ENTEROS.

En el conjunto de los números enteros

$$\mathbb{Z} = \{....., -n, ..., -2, -1, 0, 1, 2, 3, ..., n, n+1, ...\}$$

tenemos definidos una suma y un producto para los cuáles

- para todo $m \in \mathbb{Z}$ existe $-m \in \mathbb{Z}$ de modo que $m + (-m) = 0$.
- para todo $m \in \mathbb{Z}$ **no existe** $\frac{1}{m} \in \mathbb{Z}$ de modo que $m \times (\frac{1}{m}) = 1$.

La carencia de un inverso respecto de la multiplicación en los enteros $\mathbb{Z}$ nos puede llevar por varios caminos. Uno, el "inventar" los números racionales $\mathbb{Q}$. Otro, encontrar los cuerpos finitos $\mathbb{Z}_p$, que es el que vamos a seguir aquí y en el cuál encontraremos interesantes aplicaciones.

Propiedades básicas de los números Naturales.

Antes de estudiar la divisibilidad en $\mathbb{Z}$, recordemos que es lo que sabemos de divisibilidad en el conjunto de los números naturales

$$\mathbb{N} = \{0, 1, 2, 3, ..., n, n+1, ...\}.$$

El resultado siguiente es muy sencillo, pero es la base sobre la que se demuestran resultados más ambiciosos y fundamentales como el teorema del resto o el Lema de Bezout.

Teorema 1. *(**Principio de buena ordenación.**) Si A es un subconjunto no vacio de $\mathbb{N}$, es decir $A \subset \mathbb{N}$ y $A \neq \emptyset$, entonces existe el mínimo de A (existe $\min A \in A$ de modo que $\min A \leq a$ para todo $a \in A$).*

Demostración: Si $A \neq \emptyset$, existe un $a \in A$. Ahora buscamos el mínimo de A entre los números $0, 1, 2.., a$. Es decir, tomamos el 0, si el $0 \in A$, entonces $0 = \min A$. Si no, si $0 \notin A$, vemos si $1 \in A$ (en este caso $1 = \min A$),si no pasamos al 2 ...etc□

Teorema 2. *(**Principio de Inducción.**) Si $S \subset \mathbb{N}$, de modo que $1 \in S$ y se cumple que para todo $n \in \mathbb{N}$ se tiene que también $n+1 \in S$, entonces se tiene que $\mathbb{N}\backslash\{0\} \subset S$.*

Este Teorema se ve en profundidad en un primer curso. Lo usaremos entre otras cosas para probar el Teorema Fundamental de la Aritmética así como el Algoritmo de Euclides.

Teorema 3. *(**del resto de** $\mathbb{N}$.) Si $n, m \in \mathbb{N}$ con $n \neq 0$, entonces existen $q, r \in \mathbb{N}$ de modo que $m = qn + r$ y $0 \leq r < n$.*

Demostración: Sea

$$A = \{x \in \mathbb{N} : xn \geq m\}.$$

A es no vacío, ya que como $n \neq 0$, así $n \geq 1$ y por tanto $(m+1) \times n = m + n > m$. Por el Principio de buena Ordenación, existe $\alpha = \min A$. Ahora puede ocurrir dos cosas.

- Si $\alpha = 0$, entonces $0n \geq m$, lo que implica que $m = 0$ y es suficiente con tomar $q = 0$ y $r = 0 < n$. Este es el caso trivial.
- Si $\alpha \neq 0$, tomamos $q = \alpha - 1 \in \mathbb{N}$. Como ahora $q \notin A$ se tiene que

  $$qn < m \leq (q+1)n = nq + n.$$

  Si $m = n(q+1)$ tomamos $r = 0$ y se verifica el enunciado. Si no, tomamos $r = m - qn$; es claro que $m = qn + r$ y por otro lado

  $$qn < m = nq + r < (q+1)n = nq + n \Rightarrow 0 < r < n \square$$

Observación 1. *Del mismo modo si $n, m \in \mathbb{Z}$ con $n \neq 0$, entonces existen $q \in \mathbb{Z}$ y $0 \leq r < |n|$ de modo que $m = qn + r$.*

Divisibilidad de enteros

Definición 1. **A:** *$b \in \mathbb{N}\backslash\{0\}$ se dice **divisor** de $a \in \mathbb{N}$ si existe $q \in \mathbb{N}$ de modo que $a = qb$ (**notación:** escribiremos $b|a$; también se dice que b **divide** a a).*

B: *$p \in \mathbb{N}\backslash\{0, 1\}$ se dice **primo** o **número primo** si no es divisible por ningún número distinto del 1 o el mismo (es decir si $b|p$ implica que $b = 1$ o bien $b = p$).*

C: *Si $a, b \in \mathbb{N}\backslash\{0\}$, se llama **máximo común divisor** de a y b al mayor de los divisores comunes de a y b (**Notación:***

m.c.d.(a,b) *o también simplemente* (a,b)*). Es decir* $d \in \mathbb{N}$ *es el m.c.d.*(a,b) *si*

$$d|a, \qquad d|b \qquad \text{y además si} \qquad c|a, \quad y \quad c|b \Rightarrow c \leq d.$$

D: *Si* $a, b \in \mathbb{N}$*, se llama* ***mínimo común múltiplo*** *de* a *y* b *al menor* ***múltiplo*** *común de* a *y* b *(****Notación:*** *m.c.m.*(a,b) *o también simplemente* $[a,b]$*). Es decir* $m \in \mathbb{N}$ *es el m.c.m.*(a,b) *si*

$$a|m, \qquad b|m \qquad \text{y además si} \qquad a|c, \quad y \quad b|c \Rightarrow m \leq c.$$

Las siguientes propiedades son conocidas.

Proposición 1. **A:** *Para todo* $n \in \mathbb{N}\backslash\{0,1\}$ *existe* p *primo tal que* $p|n$.

B: *El conjunto de los números primos tiene cardinal infinito (es decir* ***no*** *hay una cantidad finita de números primos).*

C: *Dados* $a, b \in \mathbb{N}\backslash\{0\}$ *existe su máximo común divisor.*

Demostracción: **A:** Consideramos el conjunto

$$A = \{b \in \mathbb{N} \ : \ b > 1 \text{ y } b|n\}.$$

A es no vacío ya que $n|n$. Sea $p = \min A$, que sabemos que existe por el principio de buena ordenación. Ahora $p \geq 2$ ya que $0, 1 \notin A$. Por otro lado como $p \in A$ se tiene que $p|n$. Veamos que p es primo. Si existe $r > 1$ de modo que $r|p$ (y por tanto $p = rq$ para algún q), entonces como $a = kp$ se tiene que $a = qkr$. Concluimos que $r|a$, que $r \leq p$ y como p es el mínimo de A ocurre que $r = p$. Lo que prueba que p es primo.

B: Razonemos por reducción al absurdo. Supogamos que hay una cantidad $N \in \mathbb{N}$ de números primos. Estos serán $p_1, p_2, ...p_N$.Definimos el número

$$p = p_1 \times p_2 \times .... \times p_N + 1.$$

Veamos que p es un primo mayor que los anteriores y concluiremos que no puede ser N la cantidad de primos.

Por definición de p este es mayor que 1. Por el apartado **A** existe un primo que lo divide, el cuál será uno de nuestra lista de primos; pongamos p_j. Así existe un $q \neq 0$ de modo que

$$p = p_1 \times p_2 \times .... \times p_N + 1 = qp_j$$

lo que es equivalente a

$$(p_1 \times p_2 \times .. \times p_{j-1} \times p_{j+1} \times .. \times p_N - q)p_j + 1 = 0;$$

lo cuál no puede ocurrir ya que

$$p_1 \times p_2 \times .. \times p_{j-1} \times p_{j+1} \times .. \times p_N \geq q.$$

Luego $p_j \nmid p$ (p_j no divide a p) para todo $j = 1, 2, ..., N$. Luego por definición de primo, p lo es.

C: Si $c|a$ y $c|b$ tiene que ocurrir que $c \leq a$ y que $c \leq b$. Luego $1 \leq c \leq \text{mín}\{a, b\}$. Ahora definimos

$$d = \text{máx}\{c \ : \ c|a \text{ y } c|b\}.$$

Como $1 \in \{c \ : \ c|a \text{ y } c|b\}$, este conjunto es no vacío y está acotado superiormente. Luego tiene que existir el máximo que hemos llamado d. Luego claramente por definición de d este es el m.c.d.$(a, b)\square$

Otra forma de probar lo anterior es con el **Lema de Bezout**. Este sencillo resultado es una de la claves teóricas para descomponer números (y polinomios como veremos más adelante). La otra herramienta práctica para hacerlo es el **algoritmo de Euclides** que veremos después (y más adelante para anillos de polinomios).

Teorema 4. *(**Lema de Bezout.**) Para todo par de números naturales $a, b \in \mathbb{N}\backslash\{0\}$ existe otro par de números enteros $u, v \in \mathbb{Z}$ de modo que*

$$m.c.d.(a, b) = ua + vb$$

Demostración: Definimos el conjunto de números naturales

$$U = \{x \in \mathbb{N}\backslash\{0\} \ : \ x = ua + vb \ \text{ donde } \ u, v \in \mathbb{Z}\}$$

Como $a = 1a + 0b$ y $b = 0a + 1b$, se tiene que $a, b \in U$. Así $U \neq \emptyset$. Por el principio de buena ordenación existe el mínimo de U. Sea $d = \text{mín}\, U$. Como $d \in U$ existirán cierto $u, v \in \mathbb{Z}$ de modo que

$$d = ua + vb.$$

Veamos en primer lugar que $d|x$ para todo $x \in U$. Si no fuese así, existiría $x \in U$ con $x = qd + r$ y $0 < r < d$. Como $x \in U$ podemos escribir $x = na + mb$ y así

$$\begin{aligned} r = x - qd &= (na + mb) - q(ua + vb) \\ &= (n - qu)a + (m - qv)b \end{aligned}$$

lo que nos dice que $r \in U$ y $r < d$; esto contradice la definición de d. LLegamos pués a contradicción. Así d es divisor común de todos los elementos del conjunto U. En particular $d|a$ y $d|b$.

Si tenemos otro número c que verifica que $c|a$ y $c|b$ y por tanto $a = q_1 c$ y $b = q_2 c$, entonces

$$d = ua + vb = uq_1 c + vq_2 c = (uq_1 + vq_2)c$$

de lo que se sigue que $c|d$ y por tanto $c \leq d$. De la definición de máximo común divisor deducimos que d lo es de a y $b\square$

Corolario 1. *Si p es un número primo y $p|ab$, entonces o bien $p|a$ o bien $p|b$.*

Demostración: Supongamos que $p \nmid a$, como además p es primo se tiene que $1 = m.c.d.(p, a)$. Por el Lema de Bezout se tiene que $1 = up + va$ para cierto $u, v \in \mathbb{Z}$ y así $b = upb + vab$. Ahora como $p|ab$, se sigue que $p|b\square$

Corolario 2. *Si $c|a$ y $c|b$, entonces $c|m.c.d.(a, b)$.*

Demostración: Por un lado $a = q_1 c$ y $b = q_2 c$. Por el Lema de Bezout existen $u, v \in \mathbb{Z}$ de modo que $m.c.d.(a, b) = ua + vb$, luego podemos escribir

$$m.c.d.(a, b) = uq_1 c + vq_2 c = (uq_1 + vq_2)c.$$

Así vemos que $c|m.c.d.(a, b)$ (Observación, como $c > 0$ y $m.c.d.(a, b) \geq 1$, entonces necesariamente $uq_1 + vq_2 > 0)\square$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain

Email address: Cesar_Ruiz@mat.ucm.es