AMPLIACIÓN DE MATEMÁTICAS

REPASO DE MATEMÁTICAS DISCRETA. CONGRUENCIAS.

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.

Las propiedades de $(\mathbb{Z}, +, \times)$ como las de $(\mathbb{Z}_p, +, \times)$, se han estudiado en un curso de Matamática Discreta. En este cápitulo hacemos un breve repaso de cosas que necesitaremos. En el apéndice que sigue se desarrollan por motivos de completitud.

Teorema 1. *(**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 $0 \leq r < n$.*

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.*

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 2. *(**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*

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

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

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

El siguiente resultado es él que nos asegura que todo número entero puede descomponerse. En la prueba está implícito el como hacerlo, aunque de una forma poco eficiente.

Teorema 3. *(**Fundamental de la Aritmética.**) Todo número natural mayor que 1 puede expresarse de forma única como un producto de números primos (puede que algunos se repitan).*

Observación 2. *Un teorema similar también lo veremos para polinomios más adelante.*

Corolario 3. *Si n es un número natural mayor que 1 se puede escribir de forma única como potencias de primos. Es decir existe $p_1, p_2, ..., p_k$ números primos distintos y $r_1, r_2, ..., r_k$ enteros positivos de modo que*

$$n = p_1^{r_1} p_2^{r_2} .....p_k^{r_k}.$$

Corolario 4. *Si $a, b \in \mathbb{N}\backslash\{0\}$ de modo que $a = p_1^{r_1} p_2^{r_2} .....p_k^{r_k}$ y $b = p_1^{s_1} p_2^{s_2} .....p_k^{s_k}$, entonces*

- $m.c.d.(a,b) = p_1^{\text{mín}\{r_1,s_1\}} p_2^{\text{mín}\{r_2,s_2\}} .....p_k^{\text{mín}\{r_k,s_k\}}$.
- $m.c.m.(a,b) = p_1^{\text{máx}\{r_1,s_1\}} p_2^{\text{máx}\{r_2,s_2\}} .....p_k^{\text{máx}\{r_k,s_k\}}$.

Observación 3. *Lo anterior nos da un procedimiento para a hallar el máximo común divisor de dos números (¡el procedimiento del cole!), aunque no es muy eficiente. Es mejor usar el algoritmo de Euclides como veremos.*

Corolario 5. *Para cada $a, b \in \mathbb{N}\backslash\{0\}$ se tiene que*

$$ab = m.c.d.(a,b) m.c.m.(a,b)$$

Corolario 6. *Para cada $a, b \in \mathbb{N}\backslash\{0\}$ se tiene que*

$$m.c.m.(a,b) = \text{mín}\{c \in \mathbb{N}\backslash\{0\} \ : \ a|c \text{ y } b|c\}.$$

Ejemplo 0.1. *Si $a, b \in \mathbb{N}\backslash\{0\}$ hay que ver que $m.c.d.(a,b)|(na+mb)$ para todo $n, m \in \mathbb{Z}$.*

Sea $d = m.c.d.(a,b)$. d divide tanto a a como a b. Así $a = q_1 d$ y $b = q_2 d$, por lo tanto

$$na + mb = nq_1 d + mq_2 d = (nq_1 + mq_2)d.$$

Así $d|na + mb\square$

Ejemplo 0.2. $m.c.d.(n, n+1) = 1$.

Según la prueba del Lema de Bezout

$$m.c.d.(n, n+1) = \text{mín}\{x \in \mathbb{N}\backslash\{0\} \ : \ x = ua + vb \text{ donde } u, v \in \mathbb{Z}\}.$$

Para $u = -1$ y $v = 1$ se tiene que $1 = -n + (n+1)$, lo que dice que $1 = m.c.d.(a,b)$.

Ejemplo 0.3. *¿ m.c.d.$(n, n+2)$?*

Si $d = m.c.d.(n, n+2)$, entonces $d|n$ y $d|n+2$; por tanto $d|2$. Así d puede ser 1 o 2. Por ejemplo

$$m.c.d.(17, 19) = 1, \quad \text{sin embargo } m.c.d.(18, 20) = 2\square$$

Ejemplo 0.4. *¿ m.c.d.$(n, n+6)$?*

Si $d = m.c.d.(n, n+6)$, entonces $d|n$ y $d|n+6$; por tanto $d|6$. Así d puede ser $1, 2, 3$ o 6. Por ejemplo

$m.c.d.(5, 11) = 1$, $m.c.d.(2, 8) = 2, m.c.d.(3, 9) = 3$ y $m.c.d.(6, 12) = 6\square$

EL ALGORITMO DE EUCLIDES.

El **algoritmo de Euclides** es un método "rápido" de hallar el **máximo común divisor** de dos números (o de dos polinomios, como veremos más adelante). El algoritmo se basa en el siguiente hecho.

Lema 1. *Sean $a, b \in \mathbb{N}\backslash\{0\}$, de modo que $a = qb + r$, $0 < r < b$, entonces*

$$m.c.d.(a, b) = m.c.d.(b, r).$$

Teorema 4. ***(Algoritmo de Euclides.)*** *Dados dos números naturales $a, b \in \mathbb{N}\backslash\{0\}$ se define la sucesión decreciente de números naturales*

$$b = r_1 > r_2 > r_3 > ... > r_n > r_{n+1} = 0$$

dada por la relación

$$r_{i-1} = q_i r_i + r_{i+1} \text{ donde } r_0 = a \text{ (es decir } a = q_1 b + r_2).$$

Entonces $m.c.d.(a, b) = r_n$.

Ejemplo 0.5. *¿m.c.d.*(10,672, 4,147)*?*

Primero dividimos

$$\begin{array}{cc|c} 10672 & 4147 & 2 \\ 2387 & & \end{array} ; \quad \begin{array}{cc|c} 4147 & 2387 & 1 \\ 1769 & & \end{array} ; \quad \begin{array}{cc|c} 2387 & 1769 & 1 \\ 0609 & & \end{array} ; \quad \begin{array}{cc|c} 1769 & 609 & 2 \\ 551 & & \end{array} ;$$

$$\begin{array}{cc|c} 609 & 551 & 1 \\ 058 & & \end{array} ; \quad \begin{array}{cc|c} 551 & 58 & 9 \\ 29 & & \end{array} \quad \text{y} \quad \begin{array}{cc|c} 58 & 29 & 2 \\ 0 & & \end{array}$$

Escribimos la tabla

i	0	1	2	3	4	5	6	7	8	9
r_i	10672	4147	2378	1769	609	551	58	29	0	
q_i		2	1	1	2	1	9	2		
α_i	1	0								
β_i	0	1								

De momento las filas α_i y β_i no nos interesan. Lo que vemos es que el resto octavo se anula ($r_8 = 0$), luego el m.c.d. que buscamos es precisamente el resto anterior. Así en nuestro ejemplo, $m.c.d.(10672, 4147) = r_7 = 29$.

Otra forma del Algoritmo de Euclides

Teorema 5. *Sean $a, b \in \mathbb{N}\backslash\{0\}$, de modo que $a = qb + r$, $0 < r < b$. Generamos una tabla de cuatro entradas: r, q, α y β.*

i	*0*	*1*	*2*	*3*
r_i	a	b	r	
q_i		q		
α_i	*1*	*0*		
β_i	*0*	*1*		

donde se definen

$$\begin{array}{rcl} r_i & = & r_{i-2} - q_{i-1}r_{i-1} \\ \alpha_i & = & \alpha_{i-2} - q_{i-1}\alpha_{i-1} \quad \textit{para todo } i \geq 2, \\ \beta_i & = & \beta_{i-2} - q_{i-1}\beta_{i-1} \end{array}$$

siendo

$$r_0 = a, \;\; \alpha_0 = 1 \;\; y \;\; \beta_0 = 0$$

y

$$r_1 = b, \;\; \alpha_1 = 0 \;\; y \;\; \beta_1 = 1.$$

Entonces la sucesión

$$a = r_0 > b = r_1 > r_2 > .... > r_n > r_{n+1} = 0$$

que se obtiene es decreciente y además

$$m.c.d.(a, b) = r_n$$

y

$$m.c.d.(a, b) = \alpha_n a + \beta_n b.$$

Ejemplo 0.6. *¿$m.c.d.(10672, 4147)$? Y ¿$m.c.d.(10672, 4147) = \alpha$10,672+ β4,147?*

Lo primero es dividir, pero esa operación ya la hemos realizado arriba. Ahora completando la tabla

i	0	1	2	3	4	5	6	7	8	9
r_i	10672	4147	2378	1769	609	551	58	29	0	
q_i		2	1	1	2	1	9	2		
α_i	1	0	1	-1	2	-5	7	-68		
β_i	0	1	-2	3	-5	13	-18	175		

Deducimos que

$$\begin{aligned} m.c.d.(100672, 4147) = r_7 = 29 = \alpha_7 10{,}672 + \beta_7 4{,}147 \\ = -68 \times 10{,}672 + 175 \times 4{,}147. \end{aligned}$$

CONGRUENCIAS DE ENTEROS.

Definición 2. *Sea $m \in \mathbb{N}\backslash\{0\}$ se dice que $a, b \in \mathbb{Z}$ son **congruentes** módulo m si*

$$a = q_1 m + r \ \ y \ \ b = q_2 m + r \ \ \text{para algunos} \ \ q_1, q_2 \in \mathbb{Z}$$

y donde

$$0 \leq r < m.$$

*(**Notación:** escribimos $a \equiv b$ mód. m o también $aR_m b$).*

La relación definida entre dos enteros por la definición anterior tiene otra formulación equivalente.

Observación 4. *$a \equiv b$ mód. m si y solo si $m|a - b$.*

Proposición 2. *R_m es una relación de equivalencia sobre $\mathbb{Z}$.*

Dada la **relación** de equivalencia anterior nos fijamos en el **conjunto cociente** que produce sobre $\mathbb{Z}$.

Definición 3. *Sea $m \in \mathbb{N}\backslash\{0\}$.*

A: *Dado $a \in \mathbb{Z}$, con $a = qm + r$, notaremos por $[a]_m$ la clase de equivalencia de a respecto de la relación R_m (ser **congruente módulo** m).*

$$\begin{aligned} [a]_m = \{x \in \mathbb{Z} \ : \ x \equiv a \ \text{mód}\, m\} \\ = \{x \in \mathbb{Z} \ : \ x = km + r \ \ k \in \mathbb{Z}\}. \end{aligned}$$

B: *Notaremos por* $\mathbb{Z}_m = \mathbb{Z}/R_m$ *al* ***conjunto cociente*** *generado por la relación de equivalencia* R_m*, es decir*

$$\mathbb{Z}_m = \{[0]_m, [1]_m, ..., [m-1]_m\}.$$

OPERACIONES EN $\mathbb{Z}_m$.

Sobre los conjuntos cocientes $\mathbb{Z}_m$ se pueden definir una suma y un producto (llamados **suma en congruencias** y **producto en congruencias**).

Definición 4. **A:** *Se define la* ***suma en congruencias*** *sobre* $\mathbb{Z}_m$ *como la siguiente operación:*

$$\begin{array}{rccccc} + & : & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m & \\ & & ([a]_m, [b]_m) & \to & [a]_m + [b]_m & = & [a+b]_m. \end{array}$$

B: *Se define el* ***producto en congruencias*** *sobre* $\mathbb{Z}_m$ *como la siguiente operación:*

$$\begin{array}{rccccc} \times & : & \mathbb{Z}_m \times \mathbb{Z}_m & \to & \mathbb{Z}_m & \\ & & ([a]_m, [b]_m) & \to & [a]_m[b]_m & = & [ab]_m. \end{array}$$

Proposición 3. *Las operaciones de* ***suma*** *y* ***producto en congruencias*** *sobre* $\mathbb{Z}_m$ *están bien definidas.*

Demostración: Sean $a, a', b, b' \in \mathbb{Z}$ de modo que

$$a \equiv a' \text{ mód } m \text{ y } b \equiv b' \text{ mód } m.$$

Entonces

A: $[a]_m + [b]_m = [a']_m + [b']_m$, esto es así ya que

$$a + b = (q_1 m + r) + (q_2 m + s) = (q_1 + q_2)m + (r + s).$$

$$a' + b' = (q_1' m + r) + (q_2' m + s) = (q_1' + q_2')m + (r + s).$$

Luego $a + b \equiv r + s$ mód. m y $r + s \equiv a' + b'$ mód. m, luego por la propiedad transitiva se tiene que $a + b \equiv a' + b'$ mód. m. Es decir $[a + b]_m = [a' + b']_m$.

B: $[a]_m[b]_m = [a']_m[b']_m$, esto es así ya que

$$ab = (q_1 m + r)(q_2 m + s) = (q_1 q_2 + s q_1 + r q_2)m + (rs).$$

$$a'b' = (q_1' m + r)(q_2' m + s) = (q_1' q_2' + s q_1' + r q_2')m + (rs).$$

Luego $ab \equiv rs$ mód. m y $rs \equiv a'b'$ mód. m, luego por la propiedad transitiva se tiene que $ab \equiv a'b'$ mód. m. Es decir $[ab]_m = [a'b']_m \square$

Notación: una vez que fijamos la congruencia en la que estamos, en este ejemplo $\mathbb{Z}_4$, no escribimos $[a]_4$ ni $[a]$. Solamente a. Así, si en $\mathbb{Z}_4$ nos encontramos con el problema: $346 - 127$, lo resolveremos como $346 - 127 = 2 - 3 = 2 + 1 = 3$; donde implícitamente hemos hecho

$$\begin{array}{cc} 346 & |\underline{4} \\ 2 & 86 \end{array} \qquad\qquad \begin{array}{cc} 127 & |\underline{4} \\ 3 & 31. \end{array}$$

y además hemos "visto" en las tablas que $-3 = 1$.

Proposición 4. *Para $[n] \in \mathbb{Z}_m$, existe su inverso respecto de la multiplicación si y solo si $m.c.d.(n, m) = 1$.*

$$(\qquad \exists [n]^{-1} \Leftrightarrow \exists [k] \in \mathbb{Z}_m \text{ con } [n][k] = [1] \Leftrightarrow m.c.d.(n, m) = 1 \qquad).$$

Ejemplo 0.7. *¿Existe el inverso de 6 en $\mathbb{Z}_{17}$?*

En este caso, como 17 es un número primo, todo elemento no nulo de $\mathbb{Z}_{17}$ tiene inverso. Si $a \in \mathbb{N}\backslash\{0\}$, entonces $m.c.d.(a, 17) = 1$; en particular lo anterior es cierto para 6.

Ahora ¿cómo calculamos $[6]^{-1}$? Para ello necesitamos el lema de Bezout y el algoritmo de Euclides. Así dividiendo

$$\begin{array}{cc} 17 & |\underline{6} \\ 5 & 2 \end{array} ; \qquad \begin{array}{cc} 6 & |\underline{5} \\ 1 & 1 \end{array} ; \qquad \begin{array}{cc} 5 & |\underline{1} \\ 0 & 5 \end{array}$$

planteamos la tabla

i	0	1	2	3	4	5
r_i	17	6	5	1	0	
q_i		2	1	5		
α_i	1	0	1	-1		
β_i	0	1	-2	3		

, de la cuál se deduce que

$$1 = -17 + 3 \times 6 \Rightarrow [1]_{17} = [-17]_{17} + [3]_{17}[6]_{17} \Rightarrow [3] = [6]^{-1} \square$$

Observación 5. ***El método y las operaciones que aparecen en el ejemplo anterior son básicas, tanto en el contexto de números como en él de polinomios. Digamos que son un 50 % de los problemas que nos esperan en los próximos temas.***

Teorema 6. *Sea $m \in \mathbb{N}\backslash\{0\}$.*

A: *$(\mathbb{Z}_m, +, \times)$ es un anillo conmutativo.*

B: *$(\mathbb{Z}_m, +, \times)$ es un cuerpo si y solo si m es primo.*

Ejercicio 1. *Hay que resolver la* ***ecuación en congruencias***

$$5x \equiv 17 \qquad \textit{mód.} \qquad 19.$$

Como 19 es primo, existe $[5]^{-1} \in \mathbb{Z}_{19}$, y así $x \equiv [5]^{-1}17$ mód. 19. Haciendo la tabla de multiplicar de $\mathbb{Z}_{19}$ o buscando una identidad de Bezout $(1 = u19 + v5)$, vemos que $[4][5] = [1]$, y así

$$x \equiv 4 \times 17 = 68 \equiv 11 \qquad \text{mód.} \qquad 19.$$

Referencias

Departamento de Análisis Matemático, Facultad de Matemáticas, Universidad Complutense, 28040 Madrid, Spain
Email address: Cesar_Ruiz@mat.ucm.es