Teoría de números

Daniel Campos Salas

(Material en construcción)

Contents

1 Divisibilidad

Decimos que un entero a es **divisible** por un entero $b \neq 0$ si existe un entero c tal que $a = bc$. Podemos decir también que b **divide** a a, b es un **divisor** de a o a es un **múltiplo** de b, y denotamos esta relación mediante $b|a$. Decimos que un número p es **primo** si sus únicos divisores son $\{1, p\}$.

Comentario. *Es importante observar que la notación* ***no es simétrica****: las afirmaciones $a|b$ y $b|a$ son diferentes.*

Ejemplo 1. *Todo entero divide a 0 porque $0 = m \cdot 0$ para todo $m \in \mathbb{Z}$.*

Ejemplo 2. *Cualquier entero es divisible por 1 porque $m = 1 \cdot m$ para todo $m \in \mathbb{Z}$.*

Recogemos ahora algunas propiedades básicas de la división.

Proposición 1.1. *Sea a un entero que divide a b y c. Entonces se tiene lo siguiente:*

1. *a divide a $b \pm c$,*
2. *a divide a bd para cualquier entero d,*
3. *si $b \neq 0$, entonces $|a| \leq |b|$.*

Prueba. Por la definición sabemos que existen enteros m y n tales que $b = am$ y $c = an$. Por lo tanto, $b \pm c = am \pm an = a(m \pm n)$. Como $m \pm n$ es un entero, entonces concluimos que a divide a $b \pm c$.

Tenemos además que $bd = (am)d = a(md)$, y como md es un entero entonces a divide a bd.

Finalmente, si $b \neq 0$, entonces $m \neq 0$. Esto implica que $|m| \geq 1$. Por lo tanto, $|b| = |a||m| \geq |a|$, como queríamos probar. □

Corolario 1.2. *Si a es un entero que divide a b y c, entonces a divide a las combinaciones lineales $bm + cn$, para cualesquiera m, n enteros.*

2 Máximo divisor común

Nos gustaría establecer un converso al segundo enunciado de Proposición 1.1. Es decir, buscamos condiciones para poder decir que si a divide a bc entonces a divide a b.

No-ejemplo. *Claramente el resultado anterior no puede ser válido siempre. Por ejemplo, tenemos que* 4 *divide a* $2 \cdot 6 = 12$*, pero* 4 *no divide a* 2 *ni a* 6.

Lo que parece fallar en el ejemplo anterior es que 4 comparte divisores tanto con 2 como con 6. Esto nos lleva a la siguiente definición. Dados dos enteros a y b el conjunto de sus divisores comunes es no vacío (pues 1 pertenece a ambos) y acotado (los divisores comunes deben ser menores que a y b por Proposición 1.1), por lo que tiene un elemento máximo; llamamos a este elemento el **máximo divisor común**. Denotamos a este número por (a, b).

Ejemplo 3. *Si* $a|b$*, entonces* $(a, b) = a$.

Ejemplo 4. *Los divisores de* 18 *y* 30 *son* $\{1, 2, 3, 6, 9, 18\}$ *y* $\{1, 2, 3, 5, 6, 10, 15, 30\}$*. Por lo tanto sus divisores comunes son* $\{1, 2, 3, 6\}$ *y el máximo divisor común es* 6.

Aunque el máximo divisor común de dos números se puede calcular de la forma anterior, esto requiere de alguna forma la capacidad de factorizar el número, el cual es un problema complejo (pensando en factorizar números grandes). El siguiente algoritmo permite llevar a cabo este proceso de manera más rápida.

2.1 Algoritmo euclidiano y teorema de Bézout

Si a es divisible por b, entonces existe un único entero q, al que llamamos **cociente**, tal que $a = bq$. Cuando a no es divisible por b la afirmación anterior se puede "restaurar" diciendo que existe un entero r tal que $a - r$ es divisible por b, es decir, $a - r = bq$ para algún q. Sin embargo existen infinitas formas de arreglar esto; para cualquier entero k, el número $a + bk$ lo satisface. El siguiente teorema nos dice que hay una forma "canónica" de hacerlo.

Teorema 2.1 (Euclides)**.** *Sean* a *y* b *enteros, con* $b \neq 0$*. Entonces existen enteros únicos* q *y* r *tales que* $a = bq + r$*, con* $0 \leq r < |b|$.

Al entero r del enunciado anterior lo llamamos el **residuo** de dividir a por b. La importancia de este teorema es que se garantiza que el residuo es (estrictamente!) menor que el "divisor". Esto parece inocente, pero es realmente muy poderoso, ya que permite reducir un problema a otro **más pequeño**.

Vamos a usar la idea anterior en el siguiente algoritmo. Sean a y b enteros positivos y supongamos sin pérdida de generalidad que $a > b$. Vamos a definir una sucesión $\{c_n\}$ de la siguiente manera: $c_0 = a$, $c_1 = b$, y para $n \geq 1$ definimos c_{n+1} como el residuo al dividir c_{n-1} por c_n. El proceso se detiene cuando $c_{n+1} = 0$. Sabemos en efecto que el proceso se acaba ya que $c_{n+1} < c_n$ por Teorema 2.1.

Ejemplo 5. *Llevemos a cabo la construcción con* $a = 48$ *y* $b = 10$*. Vamos a encerrar los términos de la sucesión:*

$$\boxed{48} = 4 \cdot \boxed{10} + \boxed{8}$$

$$\boxed{10} = 1 \cdot \boxed{8} + \boxed{2}$$

$$\boxed{8} = 4 \cdot \boxed{2} + \boxed{0}$$

Vamos a estar interesados en el último término no nulo de la sucesión, que en este caso es 2.

Ejercicio. *Lleve a cabo el algoritmo para* 18 *y* 30*. Compare su resultado con el Ejemplo 4.*

Ejercicio. *Lleve a cabo el algoritmo para su pareja de números enteros favoritos.*

Con el resultado del ejemplo y de este ejercicio nos atrevemos a conjeturar el siguiente resultado.

Teorema 2.2 (Algoritmo euclidiano)**.** *El último término no nulo de la sucesión definida anteriormente es el máximo divisor común de los primeros dos términos.*

Prueba. Sea d el máximo divisor común y sea c_N el último término de la sucesión; queremos probar que $c_N = d$. Empezamos por notar lo siguiente: c_{n+1} es una combinación lineal de c_{n-1} y c_n. Como consecuencia de esto se sigue que todos los términos de la sucesión son combinaciones lineales de $c_0 = a$ y $c_1 = b$. Por Corolario 1.2 tenemos que d divide a todos los términos de la sucesión, y en particular divide a c_N. La última parte de Proposición 1.1 implica que $d \leq c_N$.

Otra observación necesaria es que el último término no nulo no solo divide al anterior, sino a todos los demás. En efecto, si c_N es este término, entonces c_N divide a c_{N-1} porque $c_{N+1} = 0$. Además, la relación $c_{N-2} = q \cdot c_{N-1} + c_N$, muestra que c_N divide a c_{N-2}, y continuando de esta manera se demuestra la segunda observación. Esto implica que c_N divide a a y b, y por lo tanto $c_N \leq d$.

Las dos observaciones anteriores implican $c_N = d$, como queríamos probar. □

Ejercicio. *La idea de la prueba del teorema se puede resumir en el siguiente resultado: para cualesquiera a, b, c enteros se tiene que $(a, b) = (a, b - ac)$. Demuestre esto usando las definiciones.*

Ejercicio. *Sea $\{F_n\}$ la sucesión de Fibonacci, definida por $F_1 = F_2 = 1$ y $F_{n+2} = F_n + F_{n+1}$ para $n \geq 1$. Demuestre que $(F_n, F_{n+1}) = 1$ para todo $n \geq 1$.*

La observación en la prueba anterior de que todos los términos de la sucesión son combinaciones lineales de los primeros dos términos nos lleva al siguiente teorema.

Teorema 2.3 (Bézout)**.** *Sean a y b enteros positivos. Entonces, existen enteros m y n tales que $am + bn = (a, b)$.*

Comentario. *Es claro que el máximo divisor común (a, b) divide a cualquier combinación lineal $am + bn$; el teorema lo que afirma es que es posible realizar (a, b) como una combinación lineal.*

Ejemplo 6. *Retomamos Ejemplo 5. Vamos a escribir los términos de la sucesión como combinaciones lineales de 48 y 10. Del cálculo en Ejemplo 5 tenemos que*

$$\boxed{8} = 1 \cdot \boxed{48} - 4 \cdot \boxed{10}$$
$$\boxed{2} = 1 \cdot \boxed{10} - 1 \cdot \boxed{8} = \boxed{10} - (\boxed{48} - 4 \cdot \boxed{10}) = 5 \cdot \boxed{10} - 1 \cdot \boxed{48}.$$

Ejercicio. *Tome sus dos números consecutivos favoritos de la sucesión de Fibonacci. Por un ejercicio sabemos que estos términos son coprimos. Lleve a cabo el algoritmo para expresar 1 como una combinación lineal de estos términos. ¿Qué observa de los coeficientes de la combinación lineal?*

Estos resultados anteriores nos llevan a demostrar el converso que estábamos buscando al principio de la sección. Decimos que a y b son **coprimos** si $(a, b) = 1$.

Ejemplo 7. *Sea p un número primo que no divide a un entero a. Como los únicos divisores de p son $\{1, p\}$ y p no divide a a, entonces el máximo (y único) divisor común de a y p es 1, es decir, a y p son coprimos.*

Teorema 2.4. *Si a divide a bc y a y b son coprimos, entonces c es divisible por a.*

Prueba. Por definición sabemos que $bc = am$ para algún entero m. Además, por la hipótesis y Teorema 2.3 tenemos que existen enteros n, p tales que $an + bp = 1$. Podemos multiplicar esta ecuación por c, y usar que $bc = am$, para obtener que

$$c = 1 \cdot c = (an + bp)c = acn + bcp = acn + amp = a(cn + mp),$$

de donde concluimos que a divide a c. □

Corolario 2.5 (Euclides)**.** *Si p es un número primo que divide a ab, entonces alguno de a o b es divisible por p.*

Prueba. Supongamos que p no divide a a, de manera que a y p son coprimos por Ejemplo 7. Por Teorema 2.4 tenemos que p divide a b como queríamos. □

3 Congruencias

Ejercicio.

Muchas veces es necesario poder dispensar de Dado un entero $m \neq 0$, decimos que a y b son **congruentes** módulo m, si m divide a $a - b$, o bien a y b dejan el mismo residuo al dividirse por m.

4 Residuos cuadráticos I

Recordamos los números que se escriben como suma de dos cuadrados forman un conjunto cerrado bajo multiplicación y que solo los primos $4k + 1$ se puede escribir como suma de dos cuadrados. Esto quiere decir, que exactamente los números que son productos de primos $4k+1$ y de cuadrados perfectos son los que se pueden escribir como suma de dos cuadrados. Nos referimos a este como el problema "global".

Podemos considerar también una versión "local". Dado un entero positivo N, decimos que a es un **residuo cuadrático** en $\mathbb{Z}/N\mathbb{Z}$ (es decir, módulo N), si existe un entero b tal que $a \equiv b^2 \pmod{N}$. El problema local es el siguiente:

Dado un entero positivo N, ¿cuáles residuos en $\mathbb{Z}/N\mathbb{Z}$ se pueden escribir como suma de dos residuos cuadráticos?

Ejemplo 8. *Para $N = 8$, los residuos cuadráticos son $\{0, 1, 4\}$:*

a	0	±1	±2	±3	4
a^2	0	1	4	1	0

Por lo tanto, los residuos que obtenemos como sumas son $\{0, 1, 2, -3, 4\}$:

	0	1	4
0	0	1	4
1	$*$	2	-3
4	$*$	$*$	0

Ejemplo 9. *Para $N = 7$, los residuos cuadráticos son $\{0, 1, 2, -3\}$:*

a	0	±1	±2	±3
a^2	0	1	-3	2

Por lo tanto, obtenemos todos los residuos como sumas:

	0	1	2	-3
0	0	1	2	-3
1	$*$	2	3	-2
2	$*$	$*$	-3	-1
-3	$*$	$*$	$*$	1

Ejercicio. *Escoja otros enteros positivos N y realice las sumas correspondientes.*

Una primera impresión con el problema es que parece ser más accesible de resolver en el caso en que N es primo, por lo que vamos a concentrarnos de momento en esto. Una primera observación, sugerida por el ejemplo $N = 7$ es la siguiente.

Proposición 4.1. *Sea p un número primo. Si a, b son residuos en $\mathbb{Z}/p\mathbb{Z}$ y $a^2 \equiv b^2$, entonces $a \equiv \pm b$. En particular, si p es un primo impar entonces hay exactamente $(p + 1)/2$ residuos cuadráticos.*

Prueba. Si $a^2 \equiv b^2$, entonces p divide a $a^2 - b^2 = (a-b)(a+b)$. Como p es un número primo, entonces p divide a alguno de los dos factores, de donde se concluye que $a \equiv \pm b$. Finalmente si p es impar, excepto por el 0, todos los demás residuos podemos agruparlos en pares $\{a, -a\}$, $a \not\equiv -a$, que dejan el mismo residuo cuadrático; es decir, hay $1 + (p-1)/2 = (p+1)/2$ residuos cuadráticos. □

Si denotamos por $Q \subseteq \mathbb{Z}/p\mathbb{Z}$ el conjunto de residuos cuadráticos módulo p y a $2Q := Q + Q$ el conjunto de todas las posibles sumas de dos elementos de Q, entonces hay $|Q|$ que se obtienen al sumar los elementos consigo mismo y $\binom{|Q|}{2}$ sumas posibles de dos elementos distintos; claramente pueden haber repeticiones entre los elementos que contamos. Dado que $|Q| = (p+1)/2$, obtenemos que

$$|Q| + \binom{|Q|}{2} = \frac{p+1}{2} + \binom{(p+1)/2}{2} = \frac{p+1}{2} + \frac{(p+1)(p+3)}{8} > \frac{p}{2} + \frac{p}{2} = p.$$

Los ejemplos anteriores y este cálculo motivan el siguiente resultado.

Teorema 4.2. *Si p es un número primo, entonces todos los residuos en $\mathbb{Z}/p\mathbb{Z}$ se pueden expresar como suma de dos residuos cuadráticos.*

Proof. Para $p = 2$ esto es obvio, por lo que suponemos que p es un primo impar. Sean Q y $2Q$ como antes. Como $0 \in Q$, entonces $Q \subseteq 2Q$. Por lo tanto, lo que resta demostrar es que $\mathbb{Z}/p\mathbb{Z} \setminus Q \subseteq 2Q$, es decir, que los números que no son residuos cuadráticos pertenecen a $2Q$. Sin embargo, es suficiente demostrar que un solo residuo no cuadrático pertenece a $2Q$; si tal fuera el caso, entonces el producto de este residuo por los $(p-1)/2$ residuos cuadráticos no nulos nos da el resto de los residuos no cuadráticos (recordemos que el producto de un residuo no cuadrático con un residuo cuadrático no nulo es un residuo no cuadrático) como suma de dos residuos cuadráticos. En efecto,

$$a \equiv b^2 + c^2 \Longrightarrow ad^2 \equiv (bd)^2 + (cd)^2.$$

Supongamos que este no es el caso, es decir, $2Q = Q$. Sea $q \in Q$, $q \not\equiv 0$. La suposición implica que el conjunto $q + Q = \{q + r : r \in Q\} \subseteq 2Q$ debe ser igual a Q, pues tiene $|Q|$ elementos distintos. En particular, la suma de los elementos de Q y la de $q + Q$ debe ser la misma, pero esto implica que $|Q|q \equiv 0$, lo cual no es posible porque $|Q| = (p+1)/2 < p$ y $q \not\equiv 0$. □

Problema 1 (Variación OIMU 2018)**.** *Sea $p > 5$ un número primo. Considere los conjuntos $A = \{m^2 : m \in \mathbb{Z}/p\mathbb{Z}\}$ y $B = \{n^4 : n \in \mathbb{Z}/p\mathbb{Z}\}$. Demuestre que todo residuo en $\mathbb{Z}/p\mathbb{Z}$ se puede escribir como una suma de un elemento de A y uno de B.*

5 Raíces primitivas

6 Propiedades

Ejercicio. *Si m divide a n, entonces $a^m - b^m$ divide a $a^n - b^n$.*

Ejercicio. *Si m divide a n, entonces*

$$\left(a^m - b^m, \frac{a^n - b^n}{a^m - b^m}\right) = \left(a^m - b^m, \frac{n}{m}\right).$$

Ejercicio. $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.

Problema 2 (R. Barton, Prueba de Selección IMO 2003, EE.UU.)**.** *Halle todas las ternas de primos (p, q, r) tales que*

$$p|q^r + 1, \quad q|r^p + 1, \quad r|p^q + 1.$$

7 ¿Qué sigue después?

References