Enteros

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Primer cuatrimestre de 2020

Parte I

Repaso de congruencias

Definición de congruencias

Definición

Sean $a, b \in \mathbb{Z}$ y sea $n \in \mathbb{N}$. Decimos que a y b son congruentes módulo n y lo escribimos

$$a \equiv b \ (mod\ n)$$

cuando $n|b-a$.

Propisición

Otra definición equivalente Sean $a, b \in \mathbb{Z}$ y sea $n \in \mathbb{N}$. Entonces, $a \equiv b$ (mód n) si y sólo si a y b proporcionan el mismo resto cuando los dividimos por n.

Algunos ejemplos:

$$3 \equiv 8 \quad (\text{mód } 5)$$

$$6 \equiv -1 \quad (\text{mód } 7)$$

$$12 \equiv 0 \quad (\text{mód } 3)$$

La congruencia es una relación de equivalencia

Propisición

La relación de congruencia tiene las siguientes propiedades:

- **Reflexividad**: $a \equiv a \pmod{n}$.
- **Simetría**: *Si* $a \equiv b \pmod{n}$, *entonces* $b \equiv a (mod\ n)$.
- **Transitividad**: *Si* $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$, *entonces* $a \equiv c \pmod{n}$

Clases de congruencia módulo n

Recordamos que una relación de equivalencia determina una partición de su dominio en clases de equivalencia [teorema 1.2.6 del apunte].
Así, pues la relación de congruencia parte a los enteros en clases de congruencia módulo n. Por ejemplo, hay cuatro clases de congruencia módulo 4 que son

$$\overline{0} = \{\ldots, -16, -8, -4, 0, 4, 8, 12, 16, \ldots.\}$$

$$\overline{1} = \{\ldots, -15, -7, -3, 1, 5, 9, 13, 17, \ldots.\}$$

$$\overline{2} = \{\ldots, -14, -6, -2, 2, 6, 10, 14, 18, \ldots.\}$$

$$\overline{3} = \{\ldots, -13, -5, -1, 3, 7, 11, 15, 19, \ldots.\}$$

En general, habrá n clases de equivalencia módulo n, una por cada posible resto $\{0, 1, 2, \ldots, n-1\}$ de la división entera por n.

Compatiblidad de las congruencias con las operaciones

Propisición

Si $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces se verifican:*

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}$$

$$ac \equiv bd \pmod{n}$$

Ejemplo: de

$$2 \equiv 12 \pmod{10} \wedge 5 \equiv 15 \pmod{10}$$

podemos deducir

$$2 + 5 \equiv 12 + 15 \pmod{10} \text{ o sea } 7 \equiv 27 \pmod{10}$$

$$2 - 5 \equiv 12 - 15 \pmod{n} \text{ o sea } -3 \equiv -3 \pmod{10}$$

$$2 \cdot 5 \equiv 12 \cdot 15 \pmod{n} \text{ o sea } 10 \equiv 180 \pmod{10}$$

El caso del módulo 2

Cuando $n = 2$, tenemos dos clases de congruencia módulo 2. La clase de los números pares y la de los impares

$$\overline{0} = \{\ldots, -10, -8, -6 - 4, -2, 0, 2, 4, 6, 8, ...\}$$

$$\overline{1} = \{\ldots, -9, -7, -5, -3, -2, -1, 1, 3, 5, 7, 9, 11, 13, ...\}$$

La proposición anterior generaliza reglas que ya conocemos como

$$0 + 0 \equiv 0 \pmod 2 \Rightarrow par + par = par$$

$$0 + 1 \equiv 1 \pmod 2 \Rightarrow par + impar = impar$$

$$1 + 1 \equiv 0 \pmod 2 \Rightarrow impar + impar = par$$

¡No se puede dividir congruencias!

En general no es posible cancelar factores no nulos en las congruencias. Por ejemplo:

$$2 \times 1 \equiv 2 \times 4 \pmod{6}$$

Sin embargo,

$$1 \not\equiv 4 \pmod{6}$$

En consecuencia, en general no se puede dividir congruencias.

Otra propiedades útiles

Corolario

Si $a \equiv b \pmod{n}$, *entonces para todo* $k \in \mathbb{N}_0$ $a^k \equiv b^k \pmod{n}$

Observación

Si $a \equiv b \pmod{n}$ *y* $m|n$ *entonces también tenemos que* $a \equiv b \pmod{m}$.

Tablas de Restos

Una ecuación de congruencias como

$$x^2 \equiv -1 \pmod 5$$

puede entonces resolverse considerando un número finito de casos:

$x \pmod 5$	$x^2 \pmod 5$
0	0
1	1
2	$4 \equiv -1$
$3 \equiv -2$	$9 \equiv 4 \equiv -1$
$4 \equiv -1$	$16 \equiv 1$

Podemos pensar a la función $x \mapsto x^2$ como actuando en las clases módulo 5.

Vemos que $x^2 \equiv -1 \pmod 5 \Leftrightarrow x \equiv 2 \pmod 5 \vee x \equiv 3 \pmod 5$. -1 es un resto cuadrático módulo 5 (es el cuadrado de alguien módulo 5)

Tablas de Restos (2)

Para comparar, consideramos una ecuación de congruencias similar pero módulo 7.

$$x^2 \equiv -1 \pmod 7$$

$x \pmod 7$	$x^2 \bmod 7$
0	0
1	1
2	4
3	$9 \equiv 2$

$x \pmod 7$	$x^2 \bmod 7$
$4 \equiv -3$	2
$5 \equiv -2$	4
$6 \equiv -1$	1

Como $-1 \equiv 6 \pmod 7$ vemos que esta congruencia no tiene solución. -1 es un no resto cuadrático módulo 7.

Parte II

Repaso de la clase anterior

El MCD como combinación lineal

Una consecuencia muy importante del algoritmo de Euclides es el siguiente teorema:

Teorema (4.4.5 en el apunte de la profesora Kirck)

El máximo común divisor entre dos enteros a y b se puede escribir como una combinación lineal de ellos: es decir, existen enteros $s = s(a, b)$ y $t = t(a, b)$ tales que

$$s \cdot a + t \cdot b = (a : b)$$

Parte III

Números Primos

Números primos

Definición

Un número $p \in \mathbb{Z}$ se dice primo si es distinto de $0, \pm 1$ y sus únicos divisores son ± 1 y $\pm p$. Un número $n \in \mathbb{Z}$ distinto de $0, \pm 1$ que no es primo se dice compuesto.

Los primeros números primos (menores que 100) son

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43$$

$$47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97$$

Existencia de la factorización en primos

La importancia de los números primos radica en que en algún sentido son los "átomos" o "bloques" con los que se forman los demás números:

Teorema

Todo entero $n > 1$, o bien es primo o se puede descomponer como producto de números primos (positivos).

Más adelante probaremos que esta descomposición es única salvo el orden de los factores (teorema fundamental de la aritmética).

Corolario

Todo número entero $n > 1$ que no sea primo, es divisible por un primo (menor o igual que su raíz cuadrada).

Demostración de la existencia de la factorización

Hacemos inducción completa en n.

- Para $n = 1$ no afirmamos nada (luego el teorema es trivialmente cierto en este caso).
- Consideremos pues un número $n > 1$, y supongamos que el teorema es cierto para los números menores que n. Si n es primo, tampoco afirmamos nada. Supongamos pues que n es compuesto. En este caso, por definición, es posible escribir a n como producto de dos números naturales $n_1, n_2 \in \mathbb{N}$ menores que n

$$n = n_1 n_2$$

Demostración de la existencia de la factorización (2)

Hacemos inducción completa en n.
Pero por hipótesis de inducción entonces, n_1 y n_2 se descomponen como producto de primos:

$$n_1 = p_1 p_2 \dots p_k$$

$$n_2 = q_1 q_2 \dots q_s$$

donde $p_1, p_2, \dots p_k$ y $q_1, q_2, \dots q_s$ son primos. Entonces n también se puede descomponer como producto de primos:

$$n = p_1 p_2 \dots p_k q_1 q_2 \dots q_s$$

En virtud del principio de inducción completa, concluimos que el teorema es verdadero para cualquier $n \in \mathbb{N}$.

Existen infinitos primos

Teorema (Euclides)

Existen infinitos números primos.

Supongamos que conocemos sólo una cantidad finita de números primos:

$$p_1 = 2, p_2 = 3, p_3 = 5, \ldots, p_N$$

vamos a ver un procedimiento para encontrar un primo que no está en la lista. (Esto demostrará que no puede haber finitos primos, pero además proporcionará un algoritmo para encontrar tantos primos como queramos.) El argumento de Euclides, consiste entonces en formar el número

$$q = p_1 p_2 \ldots p_N + 1$$

Conforme al corolario del teorema anterior, o bien q es primo, o bien es divisible por algún primo $q' < q$. Pero q no es divisible por ninguno de los primos p_1, p_2, ...p_N (ya que $q \equiv 1 \pmod{p_i}$ para todo i). En cualquiera de los dos casos, hemos encontrado un primo que no no está en nuestra lista inicial.

Parte IV

Números Coprimos

Números coprimos

Definición

Decimos que dos números $a, b \in \mathbb{Z}$ son coprimos (o primos entre sí) si los únicos divisores comunes de a y b son ± 1. Esto es claramente equivalente a decir que su máximo común divisor $mcd(a, b)$ es 1. Lo notamos $a \perp b$.

Corolario

Dos enteros $a, b \in \mathbb{Z}$ son coprimos si y sólo si existen $s, t \in \mathbb{Z}$ tales que $sa + tb = 1$.

Demostración.

Por el teorema de la clase pasada, si el máximo común divisor es 1, se escribe como una combinación lineal de a y b. Recíprocamente, si existen s y t tales que $1 = sa + tb$ entonces si d es un divisor común de a y b, tenemos que $d|sa$, $d|sb$ y en consecuencia: $d|sa + sb = 1$, luego $d = \pm 1$. Concluimos que a y b son coprimos. □

Divisibilidad con coprimos

Corolario

Si $a|bc$ y a es coprimo con b, entonces a divide a c.

Demostración.

Como a es coprimo con b, por lo anterior 1 se escribe como una combinación lineal de a y b, es decir existen $s, t \in \mathbb{Z}$ tales que:

$$sa + tb = 1$$

Entonces, multiplicando por c tenemos que:

$$sac + tbc = c$$

Como $a|sac$, y $a|tbc$, concluimos que $a|c$. □

La propiedad fundamental de los números primos

Observación

Si p es primo y p no divide a $a \in \mathbb{Z}$, entonces a y p son coprimos.

Teorema (de Euclides, 4.6.3 en el apunte)

Sea p un primo y sean $a, b \in \mathbb{Z}$. Entonces

$$p|a \cdot b \Rightarrow p|a \vee p|b.$$

Por inducción esto se generaliza a un producto de más números

Teorema

Sea p un primo y sean $a_1, a_2, \ldots a_n \in \mathbb{Z}$. Entonces

$$p|\prod_{k=1}^{n} a_k \Rightarrow p|a_k \text{ para algún } k$$

Divisibilidad con coprimos (2)

Corolario

Si $c|a$, $d|a$ y c es coprimo con d, entonces $cd|a$.

Demostración.

$$c \perp d \Rightarrow 1 = sc + td \Rightarrow a = s(ca) + t(da)$$

pero

$$d|a \Rightarrow cd|ca \wedge c|a \Rightarrow cd|da$$

luego

$$cd|s(ca) + t(da) = a$$

Inversos Módulo n

Propisición

Sean $a \in \mathbb{Z}$ y $n \in \mathbb{N}$. Si a es coprimo con n entonces existe $\tilde{a}$ (inverso de a módulo n) tal que

$$a \cdot \tilde{a} \equiv 1 \pmod{n}$$

Demostración.

Como a es coprimo con n existen s, t tales que

$$s \cdot a + t \cdot n = 1$$

Si miramos esta ecuación módulo n,

$$s \cdot a \equiv 1 \pmod{n}$$

luego $\tilde{a} = s$ cumple lo pedido. □

Un ejercicio de la práctica

Ejercicio 7, v)

$$7|a^2+b^2 \Leftrightarrow 7|a \wedge 7|b$$

$$a^2+b^2 \equiv 0 \pmod 7 \Leftrightarrow a \equiv 0 \pmod 7 \wedge b \equiv 0 \pmod 7$$

La implicación $\Leftarrow$ es fácil. Veamos la implicación $\Rightarrow$. Si 7 no dividiera a a, sería coprimo con 7 (por ser 7 primo) entonces existiría un inverso $\tilde{a}$ de a módulo 7. Pero entonces multiplicando por $\tilde{a}^2$

$$a^2+b^2 \equiv 0 \pmod 7 \Rightarrow \tilde{a}^2\left(a^2+b^2\right) \equiv 0 \pmod 7$$

luego

$$(a\cdot\tilde{a})^2+(b\cdot\tilde{a})^2 \equiv 0 \pmod 7$$

luego

$$(b\cdot\tilde{a})^2 \equiv -1 \pmod 7$$

absurdo porque -1 era un no resto cuadrático módulo 7. Luego $7|a$.

¿Qué pasaría módulo 5?

De nuevo,

Lo que vale módulo 5

$$a \equiv 0 \pmod 5 \wedge b \equiv 0 \pmod 5 \Rightarrow a^2 + b^2 \equiv 0 \pmod 5$$

Pero la vuelta no vale. Si repetimos el razonamiento, si 5 no divide a a

$$(b \cdot \tilde{a})^2 \equiv -1 \pmod 5$$

donde $\tilde{a}$ es el inverso de a módulo 5. Pero no obtenemos un absurdo pues -1 es un resto cuadrático módulo 5.

De hecho

$$a \equiv 1, b \equiv 2$$

es una solución de

$$a^2 + b^2 \equiv 0 \pmod 5$$

donde a y b no son congruentes a cero módulo 5.

Coprimalizar

Propisición

Sean $a, b \in \mathbb{Z}$ no nulos, y sea $d = (a : b)$. Entonces $a' = a : d$ y $b' = b : d$ son coprimos.

Demostración.

Sabemos que existen s, t tales que

$$sa + tb = d$$

Notamos que d divide a a y a b por definición. Entonces podemos dividir la ecuación por d y obtener

$$sa' + tb' = 1$$

y como observamos antes esto implica que a' y b' son coprimos. □

El Teorema fundamental de la aritmética

Teorema (4.6.5 en el apunte)

Sea $a \in \mathbb{Z}$, $a \neq 0, \pm 1$. Entonces a se escribe en forma única como producto de primos (positivos), (o se factoriza en forma única como producto de primos (positivos),) es decir:

1. $\forall \in \mathbb{Z}, a \neq 0, \pm 1$, *existe* $r \in \mathbb{N}$ *y existen primos positivos* $p_1, \ldots p_r$ *distintos y* $m_1, \ldots m_r \in N$ *tales que*

$$a = \pm p_1^{m_1} \cdot p_2^{m_2} \ldots p_r^{m_r}$$

2. *Esta escritura es única salvo permutación de los primos.*