El anillo $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$

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 $n \mid b - a$.

Proposición

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

Algunos ejemplos:

$$3 \equiv 8 \pmod{5}$$

$$6 \equiv -1 \pmod{7}$$

$$12 \equiv 0 \pmod{3}$$

La congruencia es una relación de equivalencia

Proposición

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

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

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

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

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

Clases de congruencia módulo n

Notación:

Para cada $n \in \mathbb{N}$, $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ es el conjunto de clases módulo n.

En general, habrá n clases de equivalencia módulo n, una por cada posible resto de la división entera por n.

$$\mathbb{Z}_n = \{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\}$$

Compatiblidad de las congruencias con las operaciones

Proposición

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

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

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

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

Operaciones con clases módulo n

El hecho de ser compatible la relación de congruencia con las operaciones de suma, resta y producto hace posible definir las correspondientes operaciones entre las clases de restos módulo n (es decir en $\mathbb{Z}_n$)

Definición

Sean $A, B \in \mathbb{Z}_n$ dos clases de restos módulo n. Para definir la suma $A + B$ procedemos del siguiente modo, elegimos un elemento cualquiera $a \in A$ y otro elemento $b \in B$. Entonces definimos la clase $A + B$ como la clase en $\mathbb{Z}_n$ que contiene al elemento $a + b$. Del mismo modo para definir la resta $A - B$ o el producto $A \cdot B$ procedemos del mismo modo, eligiendo un elemento $a \in A$ y otro $b \in B$, y definiendo $A - B$ (respectivamente $A \cdot B$) como la clase en $\mathbb{Z}_n$ que contiene al elemento $a - b$ (respectivamente $a \cdot b$).

En virtud de la proposición 3, estas operaciones entre las clases módulo n resultan bien definidas ya que el resultado sólo depende de las clases A y B, y no de los elementos que $a \in A, b \in B$ que hayamos elegido.

Ejemplo

Consideremos dos clases módulo 5 por ejemplo,

$$A = \overline{3} = \{\ldots, -7, -2, 3, 8, 13, 18, \ldots\}$$

$$B = \overline{4} = \{\ldots, -6, -1, 4, 9, 14, 19, \ldots\}$$

Para efectuar la suma $A + B$ podemos elegir cualquier número en la clase A, por ejemplo $a = 13$ y cualquier número en la clase B por ejemplo $b = -6$, efectuamos la suma $a + b = 7$ y nos fijamos en qué clase módulo 5 cae el resultado (mirando cuál es el resto en la división entera de 7 por 5). En este caso $7 \in C$, siendo

$$C = \overline{2} = \{\ldots, -8, -3, 2, 7, 12, 17, \ldots\}$$

por lo que, de acuerdo a la definición tenemos que, $A + B = C$, o también podemos expresarlo del siguiente modo:

$$\overline{13} + \overline{-6} = \overline{7}$$

Ejemplo (continuación)

¿Qué pasaría si hubieramos elegido otros **representantes** de las clases A y B por ejemplo $a = 3$ y $b = 9$?. En este caso, $a + b = 12$, pero notemos que 12 pertenece a la misma clase C que obtuvimos antes, y en consecuencia volvemos a obtner que $A + B = C$. Esto se debe a que justamente como

$$13 \equiv 3 \pmod{5}$$

y

$$-6 \equiv 9 \pmod{5}$$

podemos concluir que:

$$13 + (-6) \equiv 3 + 9 \pmod{5}$$

Otra manera de escribir la definición de las operaciones en $\mathbb{Z}_n$

En general, la definición de las operaciones en Z_n significa que:

$$\overline{a+b} = \overline{a} + \overline{b}$$

$$\overline{a-b} = \overline{a} - \overline{b}$$

$$\overline{a \times b} = \overline{a} \times \overline{b}$$

Con estas operaciones, el conjunto $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ de las clases módulo n tiene estructura de anillo. Lo que quiere decir que en él podemos sumar, restar y multiplicar con las reglas usuales.

Tablas de la suma y el producto en $\mathbb{Z}_5$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

El caso del módulo 2

El ejemplo más sencillo de aritmética modular con el que en realidad estamos familiarizados desde la escuela primaria, es $\mathbb{Z}_2$.
De hecho, existen dos clases módulo 2, la de los números pares

$$P = \overline{0} = \{\ldots, -6, -4, -2, 0, 2, 4, 6, \ldots\}$$

y la de los números impares:

$$I = \overline{1} = \{\ldots - 5, -3, -1, 1, 2, 3, 5, \ldots\}$$

Las tablas de la suma y el producto en $\mathbb{Z}_2$ son:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Definición de anillo

Un anillo es un conjunto A donde están definidas dos operaciones

$$+ : A \times A \to A$$

$$\cdot : A \times A \to A$$

de modo que se verifiquen las siguientes propieades (axiomas de la estructura de anillo):

1. Propiedad Asociativa de la suma:

$$(a + b) + c = a + (b + c) \; \forall \; a, b, c \in A$$

2. Propiedad Conmutativa de la suma

$$a + b = b + a \; \forall \; a, b \in A$$

Definición de anillo (2)

1. Existencia de neutro para la suma Existe un elemento $0 \in A$, tal que:
$$a + 0 = 0 + a = a \; \forall \; a \in A$$
2. Existencia de inversos aditivos Para todo $a \in A$, existe un elemento $-a \in A$, tal que:
$$a + (-a) = (-a) + a = 0$$
Notamos que en cualquier anillo se puede definir la operación de resta $a - b$ especificando que:
$$a - b = a + (-b)$$
3. Propiedad asociativa del producto
$$(a \cdot b) \cdot c = a \cdot (b \cdot c) \; \forall \; a, b, c \in A$$
4. Existencia de elemento neutro para el producto Existe un elemento $1 \in A$ tal que
$$a \cdot 1 = 1 \cdot a = a$$

Definición de anillo (3)

1. Propiedad Distributiva

$$a \cdot (b + c) = a \cdot b + a \cdot c \;\forall\; a, b, c \in A$$

$$(a + b) \cdot c = a \cdot c + b \cdot c \;\forall\; a, b, c \in A$$

Si además se verifica que:

$$a \cdot b = b \cdot a \;\forall a, b \in A$$

diremos que A es un anillo conmutativo.
Son ejemplos de anillos conmutativos: $\mathbb{Z}$ (los enteros), $\mathbb{Q}$ (los números racionales), $\mathbb{R}$ los números reales, $\mathbb{C}$ (los números complejos) y $\mathbb{Z}_n$ (las clases de enteros módulo n).

Existen ejemplos de anillos que no son comutativos, como las matrices de $n \times n$ con coeficientes reales, pero no trabajaremos con ellos en este curso.

Comparando $\mathbb{Z}_5$ y $\mathbb{Z}_6$

Comparemos el caso $\mathbb{Z}_5$ (módulo primo) que vimos antes

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

con el caso de $\mathbb{Z}_6$ (módulo compuesto)

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{5}$	$\overline{5}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{0}$	$\overline{2}$	$\overline{4}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{0}$	$\overline{3}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{4}$	$\overline{2}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

El caso de un módulo primo

En la tabla del producto de $\mathbb{Z}_p$ con p primo, el elemento neutro $\overline{1}$ aparece una (única) vez en cada cada fila y columna salvo las que corresponden al $\overline{0}$ (elemento absorbente).

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$x \in \mathbb{Z}_5^*$	x^{-1}
$\overline{1}$	$\overline{1}$
$\overline{2}$	$\overline{3}$
$\overline{3}$	$\overline{2}$
$\overline{4}$	$\overline{4}$

Eso significa que cada elemento no nulo $\overline{a}$ de $\mathbb{Z}_p$ tiene un inverso multiplicativo $\overline{a}^{-1} = \overline{b}$ donde b es un entero tal que

$$a \cdot b \equiv 1 \pmod{p}$$

Decimos que $\mathbb{Z}_p$ es un cuerpo cuando p es primo (un cuerpo es un anillo conmutativo en el que podemos dividir por cualquier elemento no nulo).

El caso de un módulo compuesto (1)

Cuando n es compuesto, notamos

$$\mathbb{Z}_n^* = \{\overline{a} \in \mathbb{Z}_n : a \text{ es coprimo con } n\}$$

Notemos que esta definición es correcta porque si $a \equiv b \pmod{n}$, a será coprimo con n si y sólo si b lo es.

Como ya vimos, los elementos de $\mathbb{Z}_n^*$ son exactamente los que tienen un inverso multiplicativo en $\mathbb{Z}_n$, $\overline{a}^{-1} = \overline{b}$ donde b es un entero tal que

$$\overline{a} \cdot \overline{b} = \overline{1} \text{ en } \mathbb{Z}_n$$

o sea

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

Como ya vimos, b se encuentra mediante el algoritmo de Euclides extendido: se encuentran $s, t \in \mathbb{Z}$ tales que

$$s \cdot a + t \cdot n = 1 \Rightarrow s \cdot a \equiv 1 \pmod{n}$$

Luego podemos tomar $b = s$.

El caso de un módulo compuesto (2)

Veámoslo en el ejemplo de Z_{10}. Aquí

$$\mathbb{Z}_{10}^* = \{\overline{1}, \overline{3}, \overline{7}, \overline{9}\}$$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$	$\overline{8}$	$\overline{9}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{8}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{9}$	$\overline{2}$	$\overline{5}$	$\overline{8}$	$\overline{1}$	$\overline{4}$	$\overline{7}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$	$\overline{0}$	$\overline{4}$	$\overline{8}$	$\overline{2}$	$\overline{6}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{0}$	$\overline{5}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$	$\overline{0}$	$\overline{6}$	$\overline{2}$	$\overline{8}$	$\overline{4}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{8}$	$\overline{5}$	$\overline{2}$	$\overline{9}$	$\overline{6}$	$\overline{3}$
$\overline{8}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{8}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{9}$	$\overline{0}$	$\overline{9}$	$\overline{8}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$x \in \mathbb{Z}_{10}^*$	x^{-1}
$\overline{1}$	$\overline{1}$
$\overline{3}$	$\overline{7}$
$\overline{7}$	$\overline{3}$
$\overline{9}$	$\overline{9}$

La estructura de Z_n^*

Notamos que:

- $\overline{1} \in \mathbb{Z}_n^*$.
- si $\overline{a} \in \mathbb{Z}_n^*$ y $\overline{b} \in \mathbb{Z}_n^*$, $\overline{a} \cdot \overline{b} \in \mathbb{Z}_n^*$.
- si $\overline{a} \in \mathbb{Z}_n^*$, $\overline{a}^{-1} \in \mathbb{Z}_n^*$.

Se dice que $\mathbb{Z}_n^*$ tiene estructura de grupo con respecto a la operación de producto.

Por ejemplo, la tabla del producto en $\mathbb{Z}_{10}^*$ es

$\cdot$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{7}$	$\overline{9}$
$\overline{3}$	$\overline{3}$	$\overline{9}$	$\overline{1}$	$\overline{7}$
$\overline{7}$	$\overline{7}$	$\overline{1}$	$\overline{9}$	$\overline{3}$
$\overline{9}$	$\overline{9}$	$\overline{7}$	$\overline{3}$	$\overline{1}$

El orden de un entero módulo n

Definición

Sea $\overline{a} \in \mathbb{Z}_n^*$. Definimos el órden (multiplicativo) de $\overline{a}$ en $\mathbb{Z}_n^*$ (o el orden de $a \in \mathbb{Z}$ módulo n, siendo a coprimo con n), como el menor expoente $d \in \mathbb{N}$ tal que

$$\overline{a}^d = 1 \text{ en } \mathbb{Z}_n$$

o lo que es lo mismo:

$$a^d \equiv 1 \pmod{n}$$

Un ejemplo

Calculando una tabla de potencias módulo n

```
def tabla_potencias(a,n):
      for k  in range(0,n)
            print(a,"^",k,"=",(a**k)%n)
```

Consideramos $a = 3$, $n = 11$ ¿Cómo calculamos su orden módulo 11?

Tabla de las potencias de 3 módulo 11

$$3^0 \equiv 1, 3^1 \equiv 3, 3^2 \equiv 9, 3^3 \equiv 5, 3^4 \equiv 4$$
$$3^5 \equiv 1, 3^6 \equiv 3, 3^7 \equiv 9, 3^8 \equiv 5, 3^4 \equiv 1, 3^{10} \equiv 1, \dots$$

´

El orden es 5. Las potencias se repiten con período 5.

Existencia del orden

Si a es coprimo con n, el orden de a módulo n siempre existe y es menor que n. Para demostrarlo consideremos la sucesión de potencias de a

$$a, a^2, \ldots, a^n, a^{n+1}$$

Como son $n+1$, módulo n habrá dos de ellas que caen en la misma clase: existirán i, j con $1 \leq i < j \leq n+1$

$$a^i \equiv a^j \pmod{n} \Rightarrow a^i \cdot 1 \equiv a^i \cdot a^{j-i} \pmod{n}$$

y como a es coprimo con n, a^i también lo será y podemos cancelarlo

$$a^{j-i} \equiv 1 \pmod{n}.$$

Luego existe d con $1 \leq d \leq n$ tal que

$$a^d \equiv 1 \pmod{n}$$

y por el principio del mínimo entero, existe un k mínimo.

El orden de un entero módulo n

Teorema

Sea $\overline{a} \in \mathbb{Z}_n^*$. Entonces la sucesión de las potencias

$$\overline{a}^0 = \overline{1}, \overline{a}, \overline{a}^2, \overline{a}^3, \ldots, \overline{a}^k, \ldots,$$

(en $\mathbb{Z}_n^*$) es períodica, con período d, siendo d el orden de a módulo n. Es decir que se verifica que:

$$a^i \equiv a^j \pmod{n}$$

sí y sólo si

$$i \equiv j \pmod{d}$$

En particular, se tiene que

$$a^i \equiv 1 \pmod{d}$$

si y sólo si $d | i$.

Demostración

Podemos suponer claramente que $i \geq j$. Si $i \equiv j \pmod{d}$, entonces: $i - j = kd$ para algún $k \in \mathbb{N}_0$. Luego:

$$a^i = a^{i-j} a^j = (a^d)^k a^j \equiv a^j \pmod{n}$$

Recíprocamente si,

$$a^i \equiv a^j \pmod{n}$$

tendremos que:

$$a^{i-j} a^j \equiv a^j \pmod{n}$$

y como a^j es coprimo con n, por hipótesis, podremos cancelarlo, en esta congruencia: obteniendo que:

$$a^{i-j} \equiv 1 \pmod{n}$$

Demostración (2)

Efectuemos la división entera de $i - j$ por d, de modo que:

$$i - j = qd + r \text{ con } 0 \leq r < d$$

Si fuera $r \neq 0$, tendremos que:

$$a^{i-j} = (a^q)^d \cdot a^r \equiv a^r \pmod{n}$$

y consecuentemente:

$$a^r \equiv 1 \pmod{d}$$

Pero $1 \leq r < d$, contradiciendo la definición de d. Consecuentemente, debe ser $r = 0$, es decir que $d | i - j$, o sea que:

$$i \equiv j \pmod{d}$$

El caso de un módulo primo

Cuando p es primo y p no divide a a, sabemos por el teorema de Fermat que

$$a^{p-1} \equiv 1 \pmod{p}$$

en consecuencia, el orden de a módulo p debe ser un divisor de $p-1$.

En el ejemplo anterior, $a=3$, $p=11$ vimos que el orden es 5 que es un divisor de $p-1=10$.

¿Qué pasa si a no es coprimo con n?

Lo anterior falla cuando a no es coprimo con n.
Podría ocurrir que a^n nunca sea congruente a 1 módulo n. Por ejemplo eligiendo $a = 2$ y $n = 10$ obtuve:

Calculando una tabla de potencias módulo n

```
2 ^ 0 = 1
2 ^ 1 = 2
2 ^ 2 = 4
2 ^ 3 = 8
2 ^ 4 = 6
2 ^ 5 = 2
2 ^ 6 = 4
2 ^ 7 = 8
2 ^ 8 = 6
2 ^ 9 = 2
```