Aritmética II

Leandro Marín

leandro@um.es

Septiembre 2010

UNIVERSIDAD DE MURCIA

Índice

La definición de $\mathbb{Z}_n$

Definition

Sea $n > 1$ un número entero. Dos números a y b diremos que son congruentes módulo n si $a - b$ es un múltiplo de n. A esta relación la denotaremos $a \equiv b(n)$.

La relación de congruencia módulo n cumple las siguientes propiedades:

- $a \equiv a(n)$ para todo a de $\mathbb{Z}$.

La definición de $\mathbb{Z}_n$

Definition

Sea $n > 1$ un número entero. Dos números a y b diremos que son congruentes módulo n si $a - b$ es un múltiplo de n. A esta relación la denotaremos $a \equiv b(n)$.

La relación de congruencia módulo n cumple las siguientes propiedades:

- $a \equiv a(n)$ para todo a de $\mathbb{Z}$.
- Si $a \equiv b(n)$ entonces $b \equiv a(n)$.

UNIVERSIDAD DE MURCIA

La definición de $\mathbb{Z}_n$

Definition

Sea $n > 1$ un número entero. Dos números a y b diremos que son congruentes módulo n si $a - b$ es un múltiplo de n. A esta relación la denotaremos $a \equiv b(n)$.

La relación de congruencia módulo n cumple las siguientes propiedades:

- $a \equiv a(n)$ para todo a de $\mathbb{Z}$.
- Si $a \equiv b(n)$ entonces $b \equiv a(n)$.
- Si $a \equiv b(n)$ y $b \equiv c(n)$ entonces $a \equiv c(n)$.

UNIVERSIDAD DE MURCIA

Theorem

Todo número a es congruente módulo n con el resto de dividir a entre n, por lo tanto todo número es congruente módulo n con alguno de los siguientes números $\{0, 1, 2, \cdots, n-1\}$.

Demostración.

Como $a = n \cdot q + r$ entonces $a - r = nq$ es un múltiplo de n. Además por el teorema de la división $r \in \{0, 1, \cdots, n-1\}$. $\square$

Al elemento del conjunto $\{0, 1, 2, \cdots, n-1\}$ con el cual es congruente, lo llamaremos su clase, así hablaremos de la clase del 0, la del 1, etc.

Propiedades Aritméticas de las Congruencias

La relación de congruencia módulo n tiene las siguentes propiedades aritméticas:

- Si $a \equiv b(n)$ y $c \equiv d(n)$ entonces $a + c \equiv b + d(n)$.

Propiedades Aritméticas de las Congruencias

La relación de congruencia módulo n tiene las siguentes propiedades aritméticas:

- Si $a \equiv b(n)$ y $c \equiv d(n)$ entonces $a + c \equiv b + d(n)$.
- Si $a \equiv b(n)$ y $c \equiv d(n)$ entonces $a \cdot c \equiv b \cdot d(n)$.

Propiedades Aritméticas de las Congruencias

La relación de congruencia módulo n tiene las siguentes propiedades aritméticas:

- Si $a \equiv b(n)$ y $c \equiv d(n)$ entonces $a + c \equiv b + d(n)$.
- Si $a \equiv b(n)$ y $c \equiv d(n)$ entonces $a \cdot c \equiv b \cdot d(n)$.
- En particular, como $c \equiv c(n)$ entonces si $a \equiv b(n)$ entonces $ac \equiv bc(n)$ y $a + c \equiv b + c(n)$ por lo que podemos sumar y multiplicar los dos miembros de una relación de congruencia por cualquier número.

Definición de $\mathbb{Z}_n$

Denotaremos por $\mathbb{Z}_n$ al conjunto de clases $\{0, 1, 2, \cdots, n-1\}$ con las operaciones de suma y producto tales que si al realizar la operación, el resultado queda fuera del conjunto $\{0, 1, 2, \cdots, n-1\}$, pondremos como resultado el elemento de este conjunto que sea congruente módulo n con él.

Ejemplo: $\mathbb{Z}_5$

Podemos considerar $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ con las operaciones:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Definiciones

- Dado un elemento $a \in \mathbb{Z}_n$ diremos que a es una unidad si existe $b \in \mathbb{Z}_n$ tal que $a \cdot b \equiv 1(n)$. Al subconjunto de las unidades de $\mathbb{Z}_n$ lo denotaremos $\mathbb{Z}_n^\star$.

Definiciones

- Dado un elemento $a \in \mathbb{Z}_n$ diremos que a es una unidad si existe $b \in \mathbb{Z}_n$ tal que $a \cdot b \equiv 1(n)$. Al subconjunto de las unidades de $\mathbb{Z}_n$ lo denotaremos $\mathbb{Z}_n^\star$.
- Un elemento $a \in \mathbb{Z}_n$ distinto de 0 diremos que es un divisor de 0 si existe $b \in \mathbb{Z}_n$, también distinto de 0 tal que $a \cdot b \equiv 0(n)$.

·	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
2	0	2	4	6	8	10	12	14	1	3	5	7	9	11	13
3	0	3	6	9	12	0	3	6	9	12	0	3	6	9	12
4	0	4	8	12	1	5	9	13	2	6	10	14	3	7	11
5	0	5	10	0	5	10	0	5	10	0	5	10	0	5	10
6	0	6	12	3	9	0	6	12	3	9	0	6	12	3	9
7	0	7	14	6	13	5	12	4	11	3	10	2	9	1	8
8	0	8	1	9	2	10	3	11	4	12	5	13	6	14	7
9	0	9	3	12	6	0	9	3	12	6	0	9	3	12	6
10	0	10	5	0	10	5	0	10	5	0	10	5	0	10	5
11	0	11	7	3	14	10	6	2	13	9	5	1	12	8	4
12	0	12	9	6	3	0	12	9	6	3	0	12	9	6	3
13	0	13	11	9	7	5	3	1	14	12	10	8	6	4	2
14	0	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Elementos Singulares II

- En la tabla anterior tenemos la multiplicación en $\mathbb{Z}_{15}$ y hemos marcado los elementos invertibles.

Elementos Singulares II

- En la tabla anterior tenemos la multiplicación en $\mathbb{Z}_{15}$ y hemos marcado los elementos invertibles.
- Los elementos invertibles multiplicados entre sí siempre son elementos invertibles.

Elementos Singulares II

- En la tabla anterior tenemos la multiplicación en $\mathbb{Z}_{15}$ y hemos marcado los elementos invertibles.
- Los elementos invertibles multiplicados entre sí siempre son elementos invertibles.
- Ningún elementno invertible es divisor de 0.

Elementos Singulares II

- En la tabla anterior tenemos la multiplicación en $\mathbb{Z}_{15}$ y hemos marcado los elementos invertibles.
- Los elementos invertibles multiplicados entre sí siempre son elementos invertibles.
- Ningún elementno invertible es divisor de 0.
- Los divisores de cero son precisamente los elementos no invertibles distintos de 0.

·	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	0	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	0	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	0	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	0	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	0	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	0	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	0	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	0	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	0	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	0	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	0	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	0	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	0	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Elementos Singulares III

- Como se puede ver en la tabla de multiplicar de $\mathbb{Z}_{17}$ todos los elementos distintos de 0 son unidades.

Elementos Singulares III

- Como se puede ver en la tabla de multiplicar de $\mathbb{Z}_{17}$ todos los elementos distintos de 0 son unidades.
- La condición necesaria y suficiente para que un elemento b de $\mathbb{Z}_n$ sea unidad es que el máximo común divisor de n y b sea 1.

Elementos Singulares III

- Como se puede ver en la tabla de multiplicar de $\mathbb{Z}_{17}$ todos los elementos distintos de 0 son unidades.
- La condición necesaria y suficiente para que un elemento b de $\mathbb{Z}_n$ sea unidad es que el máximo común divisor de n y b sea 1.
- Además el inverso es precisamente el v que hace que $n \cdot u + b \cdot v = 1$.

Elementos Singulares III

- Como se puede ver en la tabla de multiplicar de $\mathbb{Z}_{17}$ todos los elementos distintos de 0 son unidades.
- La condición necesaria y suficiente para que un elemento b de $\mathbb{Z}_n$ sea unidad es que el máximo común divisor de n y b sea 1.
- Además el inverso es precisamente el v que hace que $n \cdot u + b \cdot v = 1$.
- Los divisores de 0 son precisamente los que tienen $\mathrm{mcd}(n, b) = d \neq 1, 0$ porque $b \cdot (n/d)$ es 0 en $\mathbb{Z}_n$.

- Los elementos $b \in \mathbb{Z}_n$ que son unidades son precisamente los que tienen $\mathrm{mcd}(n, b) = 1$.

- Los elementos $b \in \mathbb{Z}_n$ que son unidades son precisamente los que tienen $\mathrm{mcd}(n, b) = 1$.
- El conjunto de unidades de $\mathbb{Z}_n$ se denota $\mathbb{Z}_n^\star$.

- Los elementos $b \in \mathbb{Z}_n$ que son unidades son precisamente los que tienen $\mathrm{mcd}(n, b) = 1$.
- El conjunto de unidades de $\mathbb{Z}_n$ se denota $\mathbb{Z}_n^\star$.
- El número de elementos de $\mathbb{Z}_n^\star$ se denota $\varphi(n)$ y se llama función φ de Euler.

- Los elementos $b \in \mathbb{Z}_n$ que son unidades son precisamente los que tienen $\mathrm{mcd}(n, b) = 1$.
- El conjunto de unidades de $\mathbb{Z}_n$ se denota $\mathbb{Z}_n^\star$.
- El número de elementos de $\mathbb{Z}_n^\star$ se denota $\varphi(n)$ y se llama función φ de Euler.
- Para todo $b \in \mathbb{Z}_n^\star$ se tiene que $b^{\varphi(n)} \equiv 1(n)$ (Teorema de Euler).

- Si p es un número primo $\varphi(p) = p - 1$.

- Si p es un número primo $\varphi(p) = p - 1$.
- Si p es un primo y $\alpha \geq 1$ se tiene que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ o lo que es lo mismo $p^\alpha(1 - 1/p)$.

- Si p es un número primo $\varphi(p) = p - 1$.
- Si p es un primo y $\alpha \geq 1$ se tiene que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ o lo que es lo mismo $p^\alpha(1 - 1/p)$.
- Si a y b son coprimos entonces $\varphi(ab) = \varphi(a)\varphi(b)$.

- Si p es un número primo $\varphi(p) = p - 1$.
- Si p es un primo y $\alpha \geq 1$ se tiene que $\varphi(p^\alpha) = p^{\alpha-1}(p-1)$ o lo que es lo mismo $p^\alpha(1 - 1/p)$.
- Si a y b son coprimos entonces $\varphi(ab) = \varphi(a)\varphi(b)$.
- Si $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ entonces $\varphi(n) = n(1 - 1/p_1)(1 - 1/p_2) \cdots (1 - 1/p_k)$.

A veces es necesario calcular el valor de x^e módulo n para valores de e muy grandes, tanto que sería imposible calcularlo multiplicando x por x una cantidad de e veces.
Existen varias formas de hacerlo utilizando la representación binaria del exponente $e = e_0 + e_1 2 + e_2 2^2 + \cdots + e_k 2^k$.
Lo primero que necesitamos son los valores de las cifras binarias de e. Supongamos que $e = 12345$ y vamos a calcular sus cifrar binarias calculando los restos sucesivos de dividir por 2.

12345	1	e_0
6172	0	e_1
3086	0	e_2
1543	1	e_3
771	1	e_4
385	1	e_5
192	0	e_6
96	0	e_7
48	0	e_8
24	0	e_9
12	0	e_{10}
6	0	e_{11}
3	1	e_{12}
1	1	e_{13}

Supongamos ahora que queremos calcular 23^{12345} módulo 100.
Para ello vamos a calcular una nueva columna en la tabla en la que pondremos las potencias sucesivas 23^{2^i} módulo 100.
Esto es relativamente sencillo puesto que $23^{2^0} = 23^1 = 23$ y en cada paso $23^{2^{i+1}} = 23^{2^i+2^i} = 23^{2^i} \cdot 23^{2^i}$. Es decir, elevar al cuadrado el paso anterior.
Una cuarta columna la utilizaremos para calcular la columna anterior elevada a e_i, es decir, $\left(23^{2^i}\right)^{e_i}$ que será 1 cuando e_i sea 0 y simplemente copiar el mismo valor cuando elevamos a 1.
El resultado final será el producto modular de todos los elementos de la última columna porque

$$23^e = 23^{\sum_i 2^i e_i} = \prod_i 23^{2^i e_i} = \prod_i \left(23^{2^i}\right)^{e_i}$$

12345	1	23	23	23
6172	0	29	1	23
3086	0	41	1	23
1543	1	81	81	63
771	1	61	61	43
385	1	21	21	3
192	0	41	1	3
96	0	81	1	3
48	0	61	1	3
24	0	21	1	3
12	0	41	1	3
6	0	81	1	3
3	1	61	61	83
1	1	21	21	43

Aunque el método del algoritmo de Euclides extendido es en general más efectivo, es posible utilizar este algoritmo para calcular inversos modulares cuando conocemos el valor de $\varphi(n)$ ya que $x \cdot x^{\varphi(n)-1} = x^{\varphi(n)} = 1(n)$, por lo tanto $x^{\varphi(n)-1}$ es el inverso módulo n de x.