Álgebra y Matemática Discreta

Aritmética Modular

Grado en Ingeniería Informática - 2019/20

El conjunto $\mathbb{Z}_n$

Sea n un número natural mayor que 1. El conjunto $\mathbb{Z}_n$ es el conjunto de todos los números naturales del 0 a $n-1$, es decir $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

- Es muy útil pensar que estos n números son los distintos restos de dividir cualquier número entre n.

El conjunto $\mathbb{Z}_n$

Sea n un número natural mayor que 1. El conjunto $\mathbb{Z}_n$ es el conjunto de todos los números naturales del 0 a $n-1$, es decir $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

- Es muy útil pensar que estos n números son los distintos restos de dividir cualquier número entre n.
- Veremos como podemos *representar un número cualquiera de* $\mathbb{Z}$ en un número particular de $\mathbb{Z}_n$

El conjunto $\mathbb{Z}_n$

Sea n un número natural mayor que 1. El conjunto $\mathbb{Z}_n$ es el conjunto de todos los números naturales del 0 a $n-1$, es decir $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

- Es muy útil pensar que estos n números son los distintos restos de dividir cualquier número entre n.
- Veremos como podemos *representar un número cualquiera de* $\mathbb{Z}$ en un número particular de $\mathbb{Z}_n$
- Dicho proceso puede entenderse muy bien con el siguiente ejemplo:

El conjunto $\mathbb{Z}_n$

Sea n un número natural mayor que 1. El conjunto $\mathbb{Z}_n$ es el conjunto de todos los números naturales del 0 a $n-1$, es decir $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

- Es muy útil pensar que estos n números son los distintos restos de dividir cualquier número entre n.
- Veremos como podemos *representar un número cualquiera de* $\mathbb{Z}$ en un número particular de $\mathbb{Z}_n$
- Dicho proceso puede entenderse muy bien con el siguiente ejemplo:
- ¿ Que hora marcará las agujas de un reloj analógico si han pasado 125 horas ?

El conjunto $\mathbb{Z}_n$

Sea n un número natural mayor que 1. El conjunto $\mathbb{Z}_n$ es el conjunto de todos los números naturales del 0 a $n-1$, es decir $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

- Es muy útil pensar que estos n números son los distintos restos de dividir cualquier número entre n.
- Veremos como podemos *representar un número cualquiera de* $\mathbb{Z}$ en un número particular de $\mathbb{Z}_n$
- Dicho proceso puede entenderse muy bien con el siguiente ejemplo:
- ¿ Que hora marcará las agujas de un reloj analógico si han pasado 125 horas ?
- En 125 habrán pasado 10 días y el reloj marcará las 5

El conjunto $\mathbb{Z}_n$

Sea n un número natural mayor que 1. El conjunto $\mathbb{Z}_n$ es el conjunto de todos los números naturales del 0 a $n-1$, es decir $\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}$

- Es muy útil pensar que estos n números son los distintos restos de dividir cualquier número entre n.
- Veremos como podemos *representar un número cualquiera de* $\mathbb{Z}$ en un número particular de $\mathbb{Z}_n$
- Dicho proceso puede entenderse muy bien con el siguiente ejemplo:
- ¿ Que hora marcará las agujas de un reloj analógico si han pasado 125 horas ?
- En 125 habrán pasado 10 días y el reloj marcará las 5
- Diremos que 125 coincide con 5 en el conjunto $\mathbb{Z}_{12}$.

El conjunto $\mathbb{Z}_n$

- Sean $n > 1$ y $a \in \mathbb{Z}$. Si $a = q \cdot n + r$, entonces r es el **representante** de a en $\mathbb{Z}_n$.

El conjunto $\mathbb{Z}_n$

- Sean $n > 1$ y $a \in \mathbb{Z}$. Si $a = q \cdot n + r$, entonces r es el **representante** de a en $\mathbb{Z}_n$.
- Diremos que "a es congruente a r módulo n" ("a es igual a r módulo n". Se escribe : $a \equiv r (\text{mod } n)$, tambien que "$a = r$ en $\mathbb{Z}_n$".

El conjunto $\mathbb{Z}_n$

- Sean $n > 1$ y $a \in \mathbb{Z}$. Si $a = q \cdot n + r$, entonces r es el **representante** de a en $\mathbb{Z}_n$.
- Diremos que "a es congruente a r módulo n" ("a es igual a r módulo n" . Se escribe : $a \equiv r (\text{mod } n)$, tambien que "$a = r$ en $\mathbb{Z}_n$".
- En $\mathbb{Z}_n$ los números iguales a 0 son los múltiplos de n (es decir los números del conjunto $n\mathbb{Z} = \{n \cdot k \mid \forall k \in \mathbb{Z}\}$)

El conjunto $\mathbb{Z}_n$

- Sean $n > 1$ y $a \in \mathbb{Z}$. Si $a = q \cdot n + r$, entonces r es el **representante** de a en $\mathbb{Z}_n$.
- Diremos que "a es congruente a r módulo n" ("a es igual a r módulo n" . Se escribe : $a \equiv r (\text{mod } n)$, tambien que "$a = r$ en $\mathbb{Z}_n$".
- En $\mathbb{Z}_n$ los números iguales a 0 son los múltiplos de n (es decir los números del conjunto $n\mathbb{Z} = \{n \cdot k \mid \forall k \in \mathbb{Z}\}$)
- Consecuencia de la definición de representante": Si $a, b \in \mathbb{Z}$, entonces $a = b$ en $\mathbb{Z}_n$ si y sólo si a y b tienen el mismo resto al dividirlos por n.

El conjunto $\mathbb{Z}_n$

- Para ver la igualdad en $\mathbb{Z}_n$, no hay que calcular restos por separado.

El conjunto $\mathbb{Z}_n$

- Para ver la igualdad en $\mathbb{Z}_n$, no hay que calcular restos por separado.
- Dados $a, b \in \mathbb{Z}$, entonces $a = b$ en $\mathbb{Z}_n$ (es decir $a \equiv b (\text{mod } n)$) si y sólo si $a - b$ es un múltiplo de n.

El conjunto $\mathbb{Z}_n$

- Para ver la igualdad en $\mathbb{Z}_n$, no hay que calcular restos por separado.
- Dados $a, b \in \mathbb{Z}$, entonces $a = b$ en $\mathbb{Z}_n$ (es decir $a \equiv b (\text{mod } n)$) si y sólo si $a - b$ es un múltiplo de n.
- $21 \equiv 9 (\text{mod } 4)$ pues $21 - 9 = 12$ es un múltiplo de 4.

El conjunto $\mathbb{Z}_n$

- Para ver la igualdad en $\mathbb{Z}_n$, no hay que calcular restos por separado.
- Dados $a, b \in \mathbb{Z}$, entonces $a = b$ en $\mathbb{Z}_n$ (es decir $a \equiv b (\text{mod } n)$) si y sólo si $a - b$ es un múltiplo de n.
- $21 \equiv 9 (\text{mod } 4)$ pues $21 - 9 = 12$ es un múltiplo de 4.
- $2 \equiv -3 (\text{mod } 5)$ pues $2 - (-3) = 5$ es un múltiplo de 5.

El conjunto $\mathbb{Z}_n$

- Para ver la igualdad en $\mathbb{Z}_n$, no hay que calcular restos por separado.
- Dados $a, b \in \mathbb{Z}$, entonces $a = b$ en $\mathbb{Z}_n$ (es decir $a \equiv b (\text{mod } n)$) si y sólo si $a - b$ es un múltiplo de n.
- $21 \equiv 9 (\text{mod } 4)$ pues $21 - 9 = 12$ es un múltiplo de 4.
- $2 \equiv -3 (\text{mod } 5)$ pues $2 - (-3) = 5$ es un múltiplo de 5.
- En $\mathbb{Z}_2$, todos los pares son 0 y los impares son 1.

El conjunto $\mathbb{Z}_n$

- Para ver la igualdad en $\mathbb{Z}_n$, no hay que calcular restos por separado.
- Dados $a, b \in \mathbb{Z}$, entonces $a = b$ en $\mathbb{Z}_n$ (es decir $a \equiv b (\text{mod } n)$) si y sólo si $a - b$ es un múltiplo de n.
- $21 \equiv 9 (\text{mod } 4)$ pues $21 - 9 = 12$ es un múltiplo de 4.
- $2 \equiv -3 (\text{mod } 5)$ pues $2 - (-3) = 5$ es un múltiplo de 5.
- En $\mathbb{Z}_2$, todos los pares son 0 y los impares son 1.
- En $\mathbb{Z}_3$, todo número es igual a 0, ó a 1 ó a 2. Por ejemplo el 44, como $44 = 14 \cdot 3 + 2$, $44 \equiv 2 (\text{mod } 3)$ y 2 es representante de 44.

Suma en $\mathbb{Z}_n$

- La suma en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.

Suma en $\mathbb{Z}_n$

- La suma en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se suman como enteros y después se calcula su representante (el resto de su división por n).

Suma en $\mathbb{Z}_n$

- La suma en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se suman como enteros y después se calcula su representante (el resto de su división por n).
- En $\mathbb{Z}_5$, $1321 + 415 = 1736 \equiv 1 (\text{mod } 5)$, ya que $1736 = 347 \cdot 5 + 1$.

Suma en $\mathbb{Z}_n$

- La suma en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se suman como enteros y después se calcula su representante (el resto de su división por n).
- En $\mathbb{Z}_5$, $1321 + 415 = 1736 \equiv 1 (\text{mod } 5)$, ya que $1736 = 347 \cdot 5 + 1$.
- Dados los enteros a y b podemos encontrar primero sus representantes y después sumarlos.

Suma en $\mathbb{Z}_n$

- La suma en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se suman como enteros y después se calcula su representante (el resto de su división por n).
- En $\mathbb{Z}_5$, $1321 + 415 = 1736 \equiv 1 (\text{mod } 5)$, ya que $1736 = 347 \cdot 5 + 1$.
- Dados los enteros a y b podemos encontrar primero sus representantes y después sumarlos.
- Siguiendo con el ejemplo, $1321 \equiv 1 (\text{mod } 5)$ y $415 \equiv 0 (\text{mod } 5)$, el representante de la suma es

$$1321 + 415 \equiv 1 + 0 \equiv 1 (\text{mod } 5)$$

Producto en $\mathbb{Z}_n$

- El producto en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.

Producto en $\mathbb{Z}_n$

- El producto en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se multiplican como enteros y después se calcula su representante (el resto de su división por n).

Producto en $\mathbb{Z}_n$

- El producto en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se multiplican como enteros y después se calcula su representante (el resto de su división por n).
- En $\mathbb{Z}_5$, $258 \cdot 48 = 12384 \equiv 4 (\text{mod } 5)$, ya que $12384 = 2476 \cdot 5 + 4$.

Producto en $\mathbb{Z}_n$

- El producto en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se multiplican como enteros y después se calcula su representante (el resto de su división por n).
- En $\mathbb{Z}_5$, $258 \cdot 48 = 12384 \equiv 4 (\text{mod } 5)$, ya que $12384 = 2476 \cdot 5 + 4$.
- Dados los enteros a y b podemos encontrar primero sus representantes y después multiplicarlos.

Producto en $\mathbb{Z}_n$

- El producto en $\mathbb{Z}_n$ es igual que en $\mathbb{Z}$.
- Dados dos enteros a y b se multiplican como enteros y después se calcula su representante (el resto de su división por n).
- En $\mathbb{Z}_5$, $258 \cdot 48 = 12384 \equiv 4 (\text{mod } 5)$, ya que $12384 = 2476 \cdot 5 + 4$.
- Dados los enteros a y b podemos encontrar primero sus representantes y después multiplicarlos.
- Siguiendo con el ejemplo, $258 \equiv 3 (\text{mod } 5)$ y $48 \equiv 3 (\text{mod } 5)$, el representante del producto es

$$258 \cdot 48 \equiv 3 \cdot 3 \equiv 4 (\text{mod } 5)$$

Diferencias entre $\mathbb{Z}$ y $\mathbb{Z}_n$

- La suma y el producto son asociativas y conmutativas tanto en $\mathbb{Z}$ como en $\mathbb{Z}_n$. Existe el 0 y el 1 y el producto es distributivo respecto de la suma: $a \cdot (b + c) = a \cdot b + a \cdot c$.

Diferencias entre $\mathbb{Z}$ y $\mathbb{Z}_n$

- La suma y el producto son asociativas y conmutativas tanto en $\mathbb{Z}$ como en $\mathbb{Z}_n$. Existe el 0 y el 1 y el producto es distributivo respecto de la suma: $a \cdot (b + c) = a \cdot b + a \cdot c$.
- En $\mathbb{Z}_6$, $2 \cdot 3 = 0$ y sin embargo $2 \neq 0$ y $3 \neq 0$.

Diferencias entre $\mathbb{Z}$ y $\mathbb{Z}_n$

- La suma y el producto son asociativas y conmutativas tanto en $\mathbb{Z}$ como en $\mathbb{Z}_n$. Existe el 0 y el 1 y el producto es distributivo respecto de la suma: $a \cdot (b + c) = a \cdot b + a \cdot c$.
- En $\mathbb{Z}_6$, $2 \cdot 3 = 0$ y sin embargo $2 \neq 0$ y $3 \neq 0$.
- ¿ En $\mathbb{Z}_5$ sucede esto ? (comprobar haciendo la tabla de multiplicar de $\mathbb{Z}_5$)

Diferencias entre $\mathbb{Z}$ y $\mathbb{Z}_n$

- La suma y el producto son asociativas y conmutativas tanto en $\mathbb{Z}$ como en $\mathbb{Z}_n$. Existe el 0 y el 1 y el producto es distributivo respecto de la suma: $a \cdot (b + c) = a \cdot b + a \cdot c$.
- En $\mathbb{Z}_6$, $2 \cdot 3 = 0$ y sin embargo $2 \neq 0$ y $3 \neq 0$.
- ¿ En $\mathbb{Z}_5$ sucede esto ? (comprobar haciendo la tabla de multiplicar de $\mathbb{Z}_5$)
- **Definición** En $\mathbb{Z}_n$ un elemento $a \neq 0$ se dice:
  - *divisor de cero* si existe $b \neq 0$ tal que $a \cdot b = 0$
  - *invertible* si existe $b \neq 0$ tal que $a \cdot b = 1$. El número b se llama el inverso de a en $\mathbb{Z}_n$ y se denota por a^{-1}.

Diferencias entre $\mathbb{Z}$ y $\mathbb{Z}_n$

- La suma y el producto son asociativas y conmutativas tanto en $\mathbb{Z}$ como en $\mathbb{Z}_n$. Existe el 0 y el 1 y el producto es distributivo respecto de la suma: $a \cdot (b + c) = a \cdot b + a \cdot c$.
- En $\mathbb{Z}_6$, $2 \cdot 3 = 0$ y sin embargo $2 \neq 0$ y $3 \neq 0$.
- ¿ En $\mathbb{Z}_5$ sucede esto ? (comprobar haciendo la tabla de multiplicar de $\mathbb{Z}_5$)
- **Definición** En $\mathbb{Z}_n$ un elemento $a \neq 0$ se dice:
  - *divisor de cero* si existe $b \neq 0$ tal que $a \cdot b = 0$
  - *invertible* si existe $b \neq 0$ tal que $a \cdot b = 1$. El número b se llama el inverso de a en $\mathbb{Z}_n$ y se denota por a^{-1}.
- Si a es divisor de cero, obviamente no puede se invertible y viceversa.

Inversos y divisores de cero en $\mathbb{Z}_n$

En las definiciones anteriores, si $a \cdot b = 0$, ambos son divisores de cero; y si $b = a^{-1}$, entonces $a = b^{-1}$. Obviamente el inverso es único.

- **Teorema:** Sea $a \in \mathbb{Z}_n$, $a \neq 0$, entonces
  - a es divisor de cero si y sólo si $\text{mcd}(a, n) \neq 1$.

    Si $d = \text{mcd}(a, n) \neq 1$ y tomamos $b = \dfrac{n}{d}$ se tiene que $a \cdot b \equiv 0 (\text{mod } n)$.
  - a es invertible si y sólo si $\text{mcd}(a, n) = 1$.

    Si $\text{mcd}(a, n) = 1$ sabemos que existen enteros u y v tales que $au + nv = 1$. Dicha igualdad en $\mathbb{Z}_n$ es $au \equiv 1 (\text{mod } n)$, de donde el inverso de a en $\mathbb{Z}_n$ es u.

Inversos y divisores de cero en $\mathbb{Z}_n$

En las definiciones anteriores, si $a \cdot b = 0$, ambos son divisores de cero; y si $b = a^{-1}$, entonces $a = b^{-1}$. Obviamente el inverso es único.

- **Teorema:** Sea $a \in \mathbb{Z}_n$, $a \neq 0$, entonces
  - a es divisor de cero si y sólo si $\text{mcd}(a, n) \neq 1$.

    Si $d = \text{mcd}(a, n) \neq 1$ y tomamos $b = \dfrac{n}{d}$ se tiene que $a \cdot b \equiv 0 (\text{mod } n)$.
  - a es invertible si y sólo si $\text{mcd}(a, n) = 1$.

    Si $\text{mcd}(a, n) = 1$ sabemos que existen enteros u y v tales que $au + nv = 1$. Dicha igualdad en $\mathbb{Z}_n$ es $au \equiv 1 (\text{mod } n)$, de donde el inverso de a en $\mathbb{Z}_n$ es u.
- El algoritmo extendido de ecuclides nos ayudará a calcular inversos en $\mathbb{Z}_n$.

Ejemplos

Calcular el inverso de 11 en $\mathbb{Z}_{20}$. Para ello aplicamos el algoritmo extendido de Euclides:

- Tenemos

$$20 = 1 \cdot 11 + 9$$
$$11 = 1 \cdot 9 + 2$$
$$9 = 4 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

Ejemplos

Calcular el inverso de 11 en $\mathbb{Z}_{20}$. Para ello aplicamos el algoritmo extendido de Euclides:

- Tenemos

$$20 = 1 \cdot 11 + 9$$
$$11 = 1 \cdot 9 + 2$$
$$9 = 4 \cdot 2 + 1$$
$$2 = 2 \cdot 1 + 0$$

- Por tanto $1 = \text{mcd}(20, 9)$. Sustituimos de abajo a arriba los restos:

$$1 = 9 + (-4) \cdot \bar{2} = 9 + (-4)[11 + (-1) \cdot 9] = 5 \cdot \bar{9} + (-4) \cdot 11 =$$
$$= 5 \cdot (20 - 11) + (-4) \cdot 11 = 5 \cdot 20 + (-9) \cdot 11$$

Ejemplos

- Pasando a $\mathbb{Z}_{20}$ tendremos

$$1 \equiv 5 \cdot 20 - 9 \cdot 11 \equiv 5 \cdot 0 - 9 \cdot 11 \equiv -9 \cdot 11$$

Por lo tanto $11^{-1} = -9$ y observamos que $-9 = 11$ en $\mathbb{Z}_{20}$.

Ejemplos

- Pasando a $\mathbb{Z}_{20}$ tendremos

$$1 \equiv 5 \cdot 20 - 9 \cdot 11 \equiv 5 \cdot 0 - 9 \cdot 11 \equiv -9 \cdot 11$$

  Por lo tanto $11^{-1} = -9$ y observamos que $-9 = 11$ en $\mathbb{Z}_{20}$.
- En $\mathbb{Z}_8$ calcular los divisores de cero y los inversos de los elementos invertibles.

Ejemplos

- Pasando a $\mathbb{Z}_{20}$ tendremos

$$1 \equiv 5 \cdot 20 - 9 \cdot 11 \equiv 5 \cdot 0 - 9 \cdot 11 \equiv -9 \cdot 11$$

  Por lo tanto $11^{-1} = -9$ y observamos que $-9 = 11$ en $\mathbb{Z}_{20}$.
- En $\mathbb{Z}_8$ calcular los divisores de cero y los inversos de los elementos invertibles.
- Invertibles son los coprimos con 8, a saber: 1, 3, 5, y 7. Teniéndose, $1^{-1} = 1$, $3^{-1} = 3$, $5^{-1} = 5$ y $7^{-1} = 7$.

Ejemplos

- Pasando a $\mathbb{Z}_{20}$ tendremos

$$1 \equiv 5 \cdot 20 - 9 \cdot 11 \equiv 5 \cdot 0 - 9 \cdot 11 \equiv -9 \cdot 11$$

  Por lo tanto $11^{-1} = -9$ y observamos que $-9 = 11$ en $\mathbb{Z}_{20}$.
- En $\mathbb{Z}_8$ calcular los divisores de cero y los inversos de los elementos invertibles.
- Invertibles son los coprimos con 8, a saber: 1, 3, 5, y 7. Teniéndose, $1^{-1} = 1$, $3^{-1} = 3$, $5^{-1} = 5$ y $7^{-1} = 7$.
- Divisores de cero, el resto exceptuando el 0, a saber: 2 ($\text{mcd}(2, 8) = 2$), 4 ($\text{mcd}(4, 8) = 4$) y 6 ($\text{mcd}(6, 8) = 2$).

$\mathbb{Z}_p$ con p primo

En $\mathbb{Z}_p$ con p primo todo elemento es invertible y por tanto no existen divisores de cero.

- Para todo $a \neq 0$ en $\mathbb{Z}$, al ser p primo se verifica que: $\text{mcd}(a, p) = p$ si a es un múltiplo de p, y sino $\text{mcd}(a, p) = 1$.

$\mathbb{Z}_p$ con p primo

En $\mathbb{Z}_p$ con p primo todo elemento es invertible y por tanto no existen divisores de cero.

- Para todo $a \neq 0$ en $\mathbb{Z}$, al ser p primo se verifica que: $\text{mcd}(a, p) = p$ si a es un múltiplo de p, y sino $\text{mcd}(a, p) = 1$.
- Para todo $a \neq 0$ en $\mathbb{Z}_p$, se tiene que $\text{mcd}(a, p) = 1$ y por lo tanto a es invertible.

La función phi (φ) de Euler

Otro método para calcular inversos, nos lo dá la denominada función phi, φ, de Euler.

- Dado $n > 1$, llamaremos $\varphi(n)$ al número de elementos invertibles en $\mathbb{Z}_n$.

La función phi (φ) de Euler

Otro método para calcular inversos, nos lo dá la denominada función phi, φ, de Euler.

- Dado $n > 1$, llamaremos $\varphi(n)$ al número de elementos invertibles en $\mathbb{Z}_n$.
- Para calcular $\varphi(n)$ tenemos en cuenta que:

La función phi (φ) de Euler

Otro método para calcular inversos, nos lo dá la denominada función phi, φ, de Euler.

- Dado $n > 1$, llamaremos $\varphi(n)$ al número de elementos invertibles en $\mathbb{Z}_n$.
- Para calcular $\varphi(n)$ tenemos en cuenta que:
- Si $n = p$, es primo, $\varphi(p) = p - 1$.

La función phi (φ) de Euler

Otro método para calcular inversos, nos lo dá la denominada función phi, φ, de Euler.

- Dado $n > 1$, llamaremos $\varphi(n)$ al número de elementos invertibles en $\mathbb{Z}_n$.
- Para calcular $\varphi(n)$ tenemos en cuenta que:
- Si $n = p$, es primo, $\varphi(p) = p - 1$.
- Si $n = p^r$, con p primo, $\varphi(p^r) = p^r - p^{r-1}$.

La función phi (φ) de Euler

Otro método para calcular inversos, nos lo dá la denominada función phi, φ, de Euler.

- Dado $n > 1$, llamaremos $\varphi(n)$ al número de elementos invertibles en $\mathbb{Z}_n$.
- Para calcular $\varphi(n)$ tenemos en cuenta que:
- Si $n = p$, es primo, $\varphi(p) = p - 1$.
- Si $n = p^r$, con p primo, $\varphi(p^r) = p^r - p^{r-1}$.
- Si $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, con los p_i primos distintos, entonces

$$\varphi(p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}) = \varphi(p_1^{r_1}) \cdot \dots \cdot \varphi(p_k^{r_k})$$

  - Esta última propiedad se debe a que si $\text{mcd}(m, n) = 1$ entonces $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$

La función phi (φ) de Euler

Otro método para calcular inversos, nos lo dá la denominada función phi, φ, de Euler.

- Dado $n > 1$, llamaremos $\varphi(n)$ al número de elementos invertibles en $\mathbb{Z}_n$.
- Para calcular $\varphi(n)$ tenemos en cuenta que:
- Si $n = p$, es primo, $\varphi(p) = p - 1$.
- Si $n = p^r$, con p primo, $\varphi(p^r) = p^r - p^{r-1}$.
- Si $n = p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}$, con los p_i primos distintos, entonces

$$\varphi(p_1^{r_1} p_2^{r_2} \dots p_k^{r_k}) = \varphi(p_1^{r_1}) \cdot \dots \cdot \varphi(p_k^{r_k})$$

  - Esta última propiedad se debe a que si $\text{mcd}(m, n) = 1$ entonces $\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n)$
- Como $108 = 2^2 \cdot 3^3$, se tiene que $\varphi(108) = \varphi(2^2) \cdot \varphi(3^3) = (2^2 - 2) \cdot (3^3 - 3^2) = 2 \cdot 18 = 36$.

φ de Euler

- **Teorema de Euler:** Sean a y n dos enteros con $n > 1$. Si $\text{mcd}(a, n) = 1$, entonces $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.

φ de Euler

- **Teorema de Euler:** Sean a y n dos enteros con $n > 1$. Si $\text{mcd}(a, n) = 1$, entonces $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.
- Si $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, entonces $a \cdot a^{\varphi(n)-1} \equiv 1 (\text{mod } n)$, por tanto el inverso de a en $\mathbb{Z}_n$ es $a^{\varphi(n)-1}$.

φ de Euler

- **Teorema de Euler:** Sean a y n dos enteros con $n > 1$. Si $\text{mcd}(a, n) = 1$, entonces $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.
- Si $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, entonces $a \cdot a^{\varphi(n)-1} \equiv 1 (\text{mod } n)$, por tanto el inverso de a en $\mathbb{Z}_n$ es $a^{\varphi(n)-1}$.
- **Pequeno teorema de Fermat:** Si p es un número primo que no divide al número a, (es decir $a \neq 0$ en $\mathbb{Z}_p$) , entonces $a^{p-1} \equiv 1 (\text{mod } p)$

φ de Euler

- **Teorema de Euler:** Sean a y n dos enteros con $n > 1$. Si $\text{mcd}(a, n) = 1$, entonces $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.
- Si $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, entonces $a \cdot a^{\varphi(n)-1} \equiv 1 (\text{mod } n)$, por tanto el inverso de a en $\mathbb{Z}_n$ es $a^{\varphi(n)-1}$.
- **Pequeno teorema de Fermat:** Si p es un número primo que no divide al número a, (es decir $a \neq 0$ en $\mathbb{Z}_p$) , entonces $a^{p-1} \equiv 1 (\text{mod } p)$
- $3^{4n+1} - 3$ es un múltiplo de 5 para cualquier n.

φ de Euler

- **Teorema de Euler:** Sean a y n dos enteros con $n > 1$. Si $\text{mcd}(a, n) = 1$, entonces $a^{\varphi(n)} \equiv 1 (\text{mod } n)$.
- Si $a^{\varphi(n)} \equiv 1 (\text{mod } n)$, entonces $a \cdot a^{\varphi(n)-1} \equiv 1 (\text{mod } n)$, por tanto el inverso de a en $\mathbb{Z}_n$ es $a^{\varphi(n)-1}$.
- **Pequeno teorema de Fermat:** Si p es un número primo que no divide al número a, (es decir $a \neq 0$ en $\mathbb{Z}_p$) , entonces $a^{p-1} \equiv 1 (\text{mod } p)$
- $3^{4n+1} - 3$ es un múltiplo de 5 para cualquier n.
- Debemos probar que $3^{4n+1} - 3 = 0$ en $\mathbb{Z}_5$.

  Como $\text{mcd}(3, 5) = 1$, existe el invserso de 3 en $\mathbb{Z}_5$. Dicho inverso es $3^{\varphi(5)-1} = 3^4$. Asi pues, en $\mathbb{Z}_5$

$$3^{4n+1} - 3 = (3^4)^n \cdot 3 - 3 \equiv 3 - 3 \equiv 0 (\text{mod } 5)$$

Ecuaciones diofánticas con aritmética modular

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el máximo común divisor de 42 y 32

$$42 = 32 \cdot 1 + 10,\ 32 = 10 \cdot 3 + 2,\ 10 = 2 \cdot 5$$

El máximo común divisor es 2.

Ecuaciones diofánticas con aritmética modular

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el máximo común divisor de 42 y 32

$$42 = 32 \cdot 1 + 10,\ 32 = 10 \cdot 3 + 2,\ 10 = 2 \cdot 5$$

  El máximo común divisor es 2.

- Paso 2: Comprobamos que el máximo común divisor divide al término independientee y dividimos toda la ecuación por dicho valor, para normalizarla, nos queda la ecuación $21x + 16y = 7$.

Ecuaciones diofánticas con aritmética modular

Encuentra las soluciones enteras de la ecuación $42x + 32y = 14$

- Paso 1: Calculamos el máximo común divisor de 42 y 32

$$42 = 32 \cdot 1 + 10,\ 32 = 10 \cdot 3 + 2,\ 10 = 2 \cdot 5$$

  El máximo común divisor es 2.

- Paso 2: Comprobamos que el máximo común divisor divide al término independientee y dividimos toda la ecuación por dicho valor, para normalizarla, nos queda la ecuación $21x + 16y = 7$.
- Paso 3: Convertimos la ecuación en una ecuación modular módulo 16 con lo que queda $21x \equiv 7(\text{mód } 16)$

Ecuaciones diofánticas con aritmética modular

- Paso 4: Calculamos el inverso de 21 módulo 16. Una vez calculado, es 13, multiplicamos la anterior ecuación por dicho número y podemos despejar la variable x. Tenemos

$$x \equiv 13 \cdot 21x \equiv 13 \cdot 7 = 91 \equiv 11(\text{mód } 16)$$

o dicho de otra forma, $x = 11 + 16t$.

Ecuaciones diofánticas con aritmética modular

- Paso 4: Calculamos el inverso de 21 módulo 16. Una vez calculado, es 13, multiplicamos la anterior ecuación por dicho número y podemos despejar la variable x. Tenemos

$$x \equiv 13 \cdot 21x \equiv 13 \cdot 7 = 91 \equiv 11(\text{mód } 16)$$

  o dicho de otra forma, $x = 11 + 16t$.

- Paso 5: Reemplazamos x en la ecuación y despejamos la variable y. Obtenemos $21(11 + 16t) + 16y = 7$ con lo que

$$16y = 7 - 21 \cdot 11 - 21 \cdot 16t = -224 - 21 \cdot 16t,$$

  deduciendo finalmente que $y = -14 - 21t$.