MOOC de Criptología Matemática. Unidades y Cuerpos Numéricos

Leandro Marín

Módulo II. Sesión 3.
Dificultad Alta

Introducción

- Hemos visto que en los anillos de restos modulares se pueden hacer las operaciones de suma, resta y multiplicación.

Introducción

- Hemos visto que en los anillos de restos modulares se pueden hacer las operaciones de suma, resta y multiplicación.
- La suma y la resta hacen de los conjuntos $\mathbb{Z}_n$ lo que se denomina grupos abelianos. Esa estructura es relativamente simple.

Introducción

- Hemos visto que en los anillos de restos modulares se pueden hacer las operaciones de suma, resta y multiplicación.
- La suma y la resta hacen de los conjuntos $\mathbb{Z}_n$ lo que se denomina grupos abelianos. Esa estructura es relativamente simple.
- La operación de multiplicación nos permite un análisis más complejo e interesante.

Introducción

- Hemos visto que en los anillos de restos modulares se pueden hacer las operaciones de suma, resta y multiplicación.
- La suma y la resta hacen de los conjuntos $\mathbb{Z}_n$ lo que se denomina grupos abelianos. Esa estructura es relativamente simple.
- La operación de multiplicación nos permite un análisis más complejo e interesante.
- Vamos a estudiarla con un poco más de detalle.

Multiplicación en $\mathbb{Z}_5$

- Si ponemos la tabla de multiplicar de $\mathbb{Z}_5$ podemos observar que:

	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

Multiplicación en $\mathbb{Z}_5$

- Si ponemos la tabla de multiplicar de $\mathbb{Z}_5$ podemos observar que:

	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

- Existen pares de números que multiplicados nos dan 1.

Multiplicación en $\mathbb{Z}_5$

- Si ponemos la tabla de multiplicar de $\mathbb{Z}_5$ podemos observar que:

	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

- Existen pares de números que multiplicados nos dan 1.
- A los elementos de $\mathbb{Z}_n$ que tienen otro elemento que multiplicado por ellos nos da 1 los llamaremos unidades.

Multiplicación en $\mathbb{Z}_5$

- Si ponemos la tabla de multiplicar de $\mathbb{Z}_5$ podemos observar que:

	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

- Existen pares de números que multiplicados nos dan 1.
- A los elementos de $\mathbb{Z}_n$ que tienen otro elemento que multiplicado por ellos nos da 1 los llamaremos unidades.
- También diremos que uno es inverso del otro.

Multiplicación en $\mathbb{Z}_5$

- Si ponemos la tabla de multiplicar de $\mathbb{Z}_5$ podemos observar que:

	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

- Existen pares de números que multiplicados nos dan 1.
- A los elementos de $\mathbb{Z}_n$ que tienen otro elemento que multiplicado por ellos nos da 1 los llamaremos unidades.
- También diremos que uno es inverso del otro.
- En este caso todos los elementos distintos de 0 son unidades.

Multiplicación en $\mathbb{Z}_6$

- Observemos ahora la tabla de multiplicar de $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Multiplicación en $\mathbb{Z}_6$

- Observemos ahora la tabla de multiplicar de $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- En este caso nos aparecen también unidades.

Multiplicación en $\mathbb{Z}_6$

- Observemos ahora la tabla de multiplicar de $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- En este caso nos aparecen también unidades.
- Aparecen también elementos no nulos que multiplicados nos dan 0, como por ejemplo 2 y 3.

Multiplicación en $\mathbb{Z}_6$

- Observemos ahora la tabla de multiplicar de $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- En este caso nos aparecen también unidades.
- Aparecen también elementos no nulos que multiplicados nos dan 0, como por ejemplo 2 y 3.
- Cuando en un anillo tengamos dos elementos no nulos que multiplicados nos den 0 diremos que esos elemento son divisores de 0.

Multiplicación en $\mathbb{Z}_6$

- Observemos ahora la tabla de multiplicar de $\mathbb{Z}_6$

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

- En este caso nos aparecen también unidades.
- Aparecen también elementos no nulos que multiplicados nos dan 0, como por ejemplo 2 y 3.
- Cuando en un anillo tengamos dos elementos no nulos que multiplicados nos den 0 diremos que esos elemento son divisores de 0.
- Un elemento no puede ser al mismo tiempo divisor de 0 y unidad.

En el caso de $\mathbb{Z}_{15}$ nos sucede lo mismo:

	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

El Grupo de Unidades

- En la tabla de multiplicar de $\mathbb{Z}_{15}$ podemos observar también que cuando multiplicamos dos unidades, el resultado también es una unidad.

El Grupo de Unidades

- En la tabla de multiplicar de $\mathbb{Z}_{15}$ podemos observar también que cuando multiplicamos dos unidades, el resultado también es una unidad.
- Es fácil demostrarlo, si $u_1 v_1 = 1$ y $u_2 v_2 = 1$ entonces $(u_1 u_2)(v_1 v_2) = u_1 v_1 u_2 v_2 = 1 \cdot 1 = 1$, por lo que el inverso de producto es el producto de los inversos.

El Grupo de Unidades

- En la tabla de multiplicar de $\mathbb{Z}_{15}$ podemos observar también que cuando multiplicamos dos unidades, el resultado también es una unidad.
- Es fácil demostrarlo, si $u_1 v_1 = 1$ y $u_2 v_2 = 1$ entonces $(u_1 u_2)(v_1 v_2) = u_1 v_1 u_2 v_2 = 1 \cdot 1 = 1$, por lo que el inverso de producto es el producto de los inversos.
- Matemáticamente esto se denomina un grupo multiplicativo.

La función φ de Euler

- Dado n, el número de unidades que tiene el anillo $\mathbb{Z}_n$ se denota $\varphi(n)$ y se llama la función φ de Euler.

La función φ de Euler

- Dado n, el número de unidades que tiene el anillo $\mathbb{Z}_n$ se denota $\varphi(n)$ y se llama la función φ de Euler.
- Utilizando el teorema de Bezout podemos deducir qué elementos de $\mathbb{Z}_n$ son unidades.

La función φ de Euler

- Dado n, el número de unidades que tiene el anillo $\mathbb{Z}_n$ se denota $\varphi(n)$ y se llama la función φ de Euler.
- Utilizando el teorema de Bezout podemos deducir qué elementos de $\mathbb{Z}_n$ son unidades.
- Supongamos que a es una unidad, entonces existirá u tal que $au = 1(mod\ n)$, pero por definición de congruencia eso significa que $au = 1 - nt$ para algún $t \in \mathbb{Z}$, o lo que es lo mismo $1 = au + nt$ y por tanto a y n son comprimos por el teorema de Bezout.

La función φ de Euler

- Dado n, el número de unidades que tiene el anillo $\mathbb{Z}_n$ se denota $\varphi(n)$ y se llama la función φ de Euler.
- Utilizando el teorema de Bezout podemos deducir qué elementos de $\mathbb{Z}_n$ son unidades.
- Supongamos que a es una unidad, entonces existirá u tal que $au = 1(mod\ n)$, pero por definición de congruencia eso significa que $au = 1 - nt$ para algún $t \in \mathbb{Z}$, o lo que es lo mismo $1 = au + nt$ y por tanto a y n son comprimos por el teorema de Bezout.
- Pero el Teorema de Bezout nos decía que el recíproco también es cierto, y por lo tanto si a y n son coprimos podremos encontrar u y t tales que $1 = au + nt$ y por lo tanto $au = 1(mod\ n)$.

La función φ de Euler

- Dado n, el número de unidades que tiene el anillo $\mathbb{Z}_n$ se denota $\varphi(n)$ y se llama la función φ de Euler.
- Utilizando el teorema de Bezout podemos deducir qué elementos de $\mathbb{Z}_n$ son unidades.
- Supongamos que a es una unidad, entonces existirá u tal que $au = 1(mod\ n)$, pero por definición de congruencia eso significa que $au = 1 - nt$ para algún $t \in \mathbb{Z}$, o lo que es lo mismo $1 = au + nt$ y por tanto a y n son comprimos por el teorema de Bezout.
- Pero el Teorema de Bezout nos decía que el recíproco también es cierto, y por lo tanto si a y n son coprimos podremos encontrar u y t tales que $1 = au + nt$ y por lo tanto $au = 1(mod\ n)$.
- Esto demuestra que los elementos que son unidades de $\mathbb{Z}_n$ son precisamente aquellos que son coprimos con n.

El caso p primo

- Si p es un número primo, ningún elemento entre 1 y $p-1$ puede tener un factor p y por lo tanto es coprimo con p.

El caso p primo

- Si p es un número primo, ningún elemento entre 1 y $p-1$ puede tener un factor p y por lo tanto es coprimo con p.
- Eso demuestra que el número de unidades es $\varphi(p) = p - 1$.

El caso p primo

- Si p es un número primo, ningún elemento entre 1 y $p-1$ puede tener un factor p y por lo tanto es coprimo con p.
- Eso demuestra que el número de unidades es $\varphi(p) = p - 1$.
- Dicho de otra manera, todos los elementos distintos de cero son unidades.

El caso p primo

- Si p es un número primo, ningún elemento entre 1 y $p-1$ puede tener un factor p y por lo tanto es coprimo con p.
- Eso demuestra que el número de unidades es $\varphi(p) = p - 1$.
- Dicho de otra manera, todos los elementos distintos de cero son unidades.
- Es lo que nos pasaba en $\mathbb{Z}_5$, porque 5 es primo.

El caso $n = pq$ con p y q primos distintos

- Sea $n = pq$ con p y q dos primos distintos. Las unidades de $\mathbb{Z}_n$ serán todas salvo las que tengan un factor p o un factor q (o ambos).

El caso $n = pq$ con p y q primos distintos

- Sea $n = pq$ con p y q dos primos distintos. Las unidades de $\mathbb{Z}_n$ serán todas salvo las que tengan un factor p o un factor q (o ambos).
- Las que tienen un factor p son $p, 2p, 3p, \cdots, (q-1)p$, es decir, hay $q-1$ de ellas.

El caso $n = pq$ con p y q primos distintos

- Sea $n = pq$ con p y q dos primos distintos. Las unidades de $\mathbb{Z}_n$ serán todas salvo las que tengan un factor p o un factor q (o ambos).
- Las que tienen un factor p son $p, 2p, 3p, \cdots, (q-1)p$, es decir, hay $q-1$ de ellas.
- Las que tienen un factor q son $q, 2q, 3q, \cdots, (p-1)q$, es decir, hay $p-1$ de ellas.

El caso $n = pq$ con p y q primos distintos

- Sea $n = pq$ con p y q dos primos distintos. Las unidades de $\mathbb{Z}_n$ serán todas salvo las que tengan un factor p o un factor q (o ambos).
- Las que tienen un factor p son $p, 2p, 3p, \cdots, (q-1)p$, es decir, hay $q-1$ de ellas.
- Las que tienen un factor q son $q, 2q, 3q, \cdots, (p-1)q$, es decir, hay $p-1$ de ellas.
- El 0 es el único que se divide por p y por q que también tendremos que quitarlo.

El caso $n = pq$ con p y q primos distintos

- Sea $n = pq$ con p y q dos primos distintos. Las unidades de $\mathbb{Z}_n$ serán todas salvo las que tengan un factor p o un factor q (o ambos).
- Las que tienen un factor p son $p, 2p, 3p, \cdots, (q-1)p$, es decir, hay $q-1$ de ellas.
- Las que tienen un factor q son $q, 2q, 3q, \cdots, (p-1)q$, es decir, hay $p-1$ de ellas.
- El 0 es el único que se divide por p y por q que también tendremos que quitarlo.
- El número de unidades será pues $\varphi(n) = n-(p-1)-(q-1)-1 = pq-p-q+1 = (p-1)(q-1)$.

El caso $n = pq$ con p y q primos distintos

- Sea $n = pq$ con p y q dos primos distintos. Las unidades de $\mathbb{Z}_n$ serán todas salvo las que tengan un factor p o un factor q (o ambos).
- Las que tienen un factor p son $p, 2p, 3p, \cdots, (q-1)p$, es decir, hay $q-1$ de ellas.
- Las que tienen un factor q son $q, 2q, 3q, \cdots, (p-1)q$, es decir, hay $p-1$ de ellas.
- El 0 es el único que se divide por p y por q que también tendremos que quitarlo.
- El número de unidades será pues $\varphi(n) = n-(p-1)-(q-1)-1 = pq-p-q+1 = (p-1)(q-1)$.
- Esto es lo que pasa en el caso de 15 que tiene $\varphi(3 \cdot 5) = (3-1)(5-1) = 2 \cdot 4 = 8$ unidades o en el caso de 6 que tiene $\varphi(2 \cdot 3) = (2-1)(3-1) = 2$ unidades.

Fórmula de Euler

- Es posible calcular el valor de $\varphi(n)$ si se dispone de la factorización de n. Nosotros lo hemos calculado sólo en dos casos puesto que son los que necesitaremos para las aplicaciones criptográficas.

Fórmula de Euler

- Es posible calcular el valor de $\varphi(n)$ si se dispone de la factorización de n. Nosotros lo hemos calculado sólo en dos casos puesto que son los que necesitaremos para las aplicaciones criptográficas.
- También es posible demostrar por métodos elementales que dada cualquier unidad u de $\mathbb{Z}_n$ se cumple que $u^{\varphi(n)} = 1(mod\ n)$.

Fórmula de Euler

- Es posible calcular el valor de $\varphi(n)$ si se dispone de la factorización de n. Nosotros lo hemos calculado sólo en dos casos puesto que son los que necesitaremos para las aplicaciones criptográficas.
- También es posible demostrar por métodos elementales que dada cualquier unidad u de $\mathbb{Z}_n$ se cumple que $u^{\varphi(n)} = 1(mod\ n)$.
- Esta fórmula se conoce como fórmula de Euler.

Implementación en sage

- La función que nos dice si un elemento es una unidad es `is_unit`, por ejemplo:

```
for x in Zmod(15):
  if x.is_unit():
    print x,
```

nos responderá `1 2 4 7 8 11 13 14`, que son las unidades de $\mathbb{Z}_{15}$.

Implementación en sage

- La función que nos dice si un elemento es una unidad es `is_unit`, por ejemplo:

```
for x in Zmod(15):
  if x.is_unit():
    print x,
```

nos responderá `1 2 4 7 8 11 13 14`, que son las unidades de $\mathbb{Z}_{15}$.

- La función φ se escribe en sage como `euler_phi(n)`, así

```
euler_phi(15)
```

nos responderá 8. La podemos usar para números aunque no sean de la forma pq.

Anillos y Cuerpos I

- A los conjuntos $\mathbb{Z}_n$ los hemos llamado anillos, aunque no hemos visto formalmente la definición de anillo.

Anillos y Cuerpos I

- A los conjuntos $\mathbb{Z}_n$ los hemos llamado anillos, aunque no hemos visto formalmente la definición de anillo.
- Un anillo es una estructura algebraica que tiene una suma y un producto con las propiedades aritméticas habituales (asociativa, conmutativa, etc). Otro ejemplo de un anillo es $\mathbb{Z}$.

Anillos y Cuerpos I

- A los conjuntos $\mathbb{Z}_n$ los hemos llamado anillos, aunque no hemos visto formalmente la definición de anillo.
- Un anillo es una estructura algebraica que tiene una suma y un producto con las propiedades aritméticas habituales (asociativa, conmutativa, etc). Otro ejemplo de un anillo es $\mathbb{Z}$.
- Existen muchos anillos que no son del tipo $\mathbb{Z}_n$.

Anillos y Cuerpos I

- A los conjuntos $\mathbb{Z}_n$ los hemos llamado anillos, aunque no hemos visto formalmente la definición de anillo.
- Un anillo es una estructura algebraica que tiene una suma y un producto con las propiedades aritméticas habituales (asociativa, conmutativa, etc). Otro ejemplo de un anillo es $\mathbb{Z}$.
- Existen muchos anillos que no son del tipo $\mathbb{Z}_n$.
- Cuando en un anillo todos los elementos distintos de cero son unidades diremos que el anillo es en realidad un cuerpo.

Anillos y Cuerpos I

- A los conjuntos $\mathbb{Z}_n$ los hemos llamado anillos, aunque no hemos visto formalmente la definición de anillo.
- Un anillo es una estructura algebraica que tiene una suma y un producto con las propiedades aritméticas habituales (asociativa, conmutativa, etc). Otro ejemplo de un anillo es $\mathbb{Z}$.
- Existen muchos anillos que no son del tipo $\mathbb{Z}_n$.
- Cuando en un anillo todos los elementos distintos de cero son unidades diremos que el anillo es en realidad un cuerpo.
- Hemos visto que si p es un primo se cumple esta propiedad, por lo tanto $\mathbb{Z}_p$ es un cuerpo y como hay infinitos primos distintos, esto nos muestra una infinidad de cuerpos distintos.

Anillos y Cuerpos II

- Existen otros cuerpos que no son del tipo $\mathbb{Z}_p$, pero no son de tipo numérico.

Anillos y Cuerpos II

- Existen otros cuerpos que no son del tipo $\mathbb{Z}_p$, pero no son de tipo numérico.
- Son especialmente importantes en criptografía los cuerpos binarios, pero no podemos profundizar en este aspecto y concentraremos todas nuestras construcciones en los cuerpos del tipo $\mathbb{Z}_p$.

Anillos y Cuerpos II

- Existen otros cuerpos que no son del tipo $\mathbb{Z}_p$, pero no son de tipo numérico.
- Son especialmente importantes en criptografía los cuerpos binarios, pero no podemos profundizar en este aspecto y concentraremos todas nuestras construcciones en los cuerpos del tipo $\mathbb{Z}_p$.
- Un ejemplo de utilización de un cuerpo binario en criptografía es el algoritmo AES que ya hemos visto, aunque pasando por encima de esa propiedad.

Anillos y Cuerpos II

- Existen otros cuerpos que no son del tipo $\mathbb{Z}_p$, pero no son de tipo numérico.
- Son especialmente importantes en criptografía los cuerpos binarios, pero no podemos profundizar en este aspecto y concentraremos todas nuestras construcciones en los cuerpos del tipo $\mathbb{Z}_p$.
- Un ejemplo de utilización de un cuerpo binario en criptografía es el algoritmo AES que ya hemos visto, aunque pasando por encima de esa propiedad.
- Ejemplos de cuerpos infinitos son $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$.

Anillos y Cuerpos II

- Existen otros cuerpos que no son del tipo $\mathbb{Z}_p$, pero no son de tipo numérico.
- Son especialmente importantes en criptografía los cuerpos binarios, pero no podemos profundizar en este aspecto y concentraremos todas nuestras construcciones en los cuerpos del tipo $\mathbb{Z}_p$.
- Un ejemplo de utilización de un cuerpo binario en criptografía es el algoritmo AES que ya hemos visto, aunque pasando por encima de esa propiedad.
- Ejemplos de cuerpos infinitos son $\mathbb{Q}, \mathbb{R}$ y $\mathbb{C}$.
- Vamos a ver la definición, aunque sólo como curiosidad, no es necesario memorizarla ni la utilizaremos.

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b
- $a + 0 = a$ para todo a

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b
- $a + 0 = a$ para todo a
- Para todo a existe $-a$ tal que $a + (-a) = 0$

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b
- $a + 0 = a$ para todo a
- Para todo a existe $-a$ tal que $a + (-a) = 0$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo a, b, c

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b
- $a + 0 = a$ para todo a
- Para todo a existe $-a$ tal que $a + (-a) = 0$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo a, b, c
- $a \cdot b = b \cdot a$ para todo a, b

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b
- $a + 0 = a$ para todo a
- Para todo a existe $-a$ tal que $a + (-a) = 0$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo a, b, c
- $a \cdot b = b \cdot a$ para todo a, b
- $a \cdot 1 = a$ para todo a

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b
- $a + 0 = a$ para todo a
- Para todo a existe $-a$ tal que $a + (-a) = 0$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo a, b, c
- $a \cdot b = b \cdot a$ para todo a, b
- $a \cdot 1 = a$ para todo a
- Para todo a distinto de 0 existe a^{-1} tal que $a \cdot a^{-1} = 1$

Definición de Cuerpo

- Un cuerpo es un conjunto K con dos operaciones $+$ y $\cdot$ y, al menos, dos elementos distintos 0 y 1 que cumplen las siguientes propiedades:
- $a + (b + c) = (a + b) + c$ para todo a, b, c
- $a + b = b + a$ para todo a, b
- $a + 0 = a$ para todo a
- Para todo a existe $-a$ tal que $a + (-a) = 0$
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ para todo a, b, c
- $a \cdot b = b \cdot a$ para todo a, b
- $a \cdot 1 = a$ para todo a
- Para todo a distinto de 0 existe a^{-1} tal que $a \cdot a^{-1} = 1$
- $a \cdot (b + c) = a \cdot b + a \cdot c$ para todo a, b, c

Implementación en sage

- Los cuerpos finitos también se denominan cuerpos de Galois (Galois Fields) y en sage se pueden construir con `GF(n)`.

Implementación en sage

- Los cuerpos finitos también se denominan cuerpos de Galois (Galois Fields) y en sage se pueden construir con `GF(n)`.
- Si el número de elementos es primo, `GF(p)` y `Zmod(p)` son lo mismo y utilizaremos esos símbolos indistintamente.

Implementación en sage

- Los cuerpos finitos también se denominan cuerpos de Galois (Galois Fields) y en sage se pueden construir con `GF(n)`.
- Si el número de elementos es primo, `GF(p)` y `Zmod(p)` son lo mismo y utilizaremos esos símbolos indistintamente.
- En el caso de un número de elementos no primo, `Zmod(n)` y `GF(n)` no son lo mismo, de hecho `GF(n)` no estará definido en muchos casos.

Implementación en sage

- Los cuerpos finitos también se denominan cuerpos de Galois (Galois Fields) y en sage se pueden construir con `GF(n)`.
- Si el número de elementos es primo, `GF(p)` y `Zmod(p)` son lo mismo y utilizaremos esos símbolos indistintamente.
- En el caso de un número de elementos no primo, `Zmod(n)` y `GF(n)` no son lo mismo, de hecho `GF(n)` no estará definido en muchos casos.
- Como curiosidad vamos a ver los elementos del cuerpo de 4 elementos en sage:

```
K = GF(4,'x')
for k in K:
  print k,
```

nos dirá que los elementos de este cuerpo son `0`, `x`, `x + 1` y `1`.