MOOC de Criptología Matemática. Aritmética Modular

Leandro Marín

Módulo II. Sesión 2.
Dificultad Media

Presentación

- Ya hemos estudiado el conjunto de los números enteros, que es un conjunto infinito.

Presentación

- Ya hemos estudiado el conjunto de los números enteros, que es un conjunto infinito.
- Aunque esta construcción nos puede resultar muy natural, en criptografía (y en general en la informática) un conjunto infinito es un problema.

Presentación

- Ya hemos estudiado el conjunto de los números enteros, que es un conjunto infinito.
- Aunque esta construcción nos puede resultar muy natural, en criptografía (y en general en la informática) un conjunto infinito es un problema.
- Los conjuntos se utilizan para representar estados y no son manejables situaciones en las cuales el número de estados es infinito.

Presentación

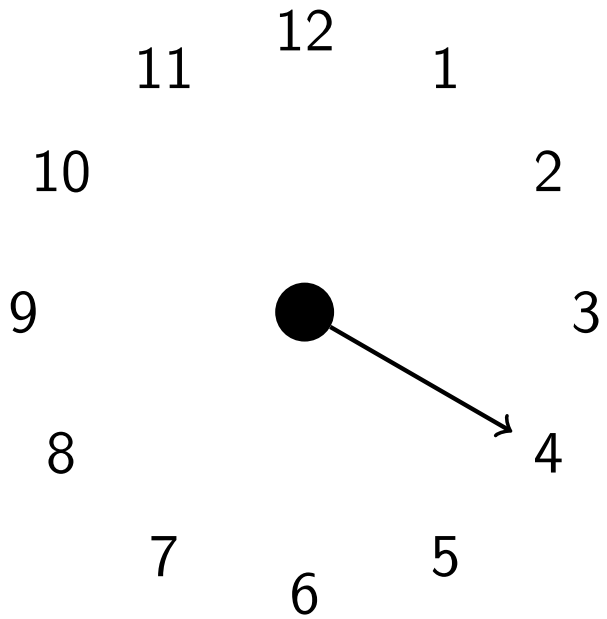
- Ya hemos estudiado el conjunto de los números enteros, que es un conjunto infinito.
- Aunque esta construcción nos puede resultar muy natural, en criptografía (y en general en la informática) un conjunto infinito es un problema.
- Los conjuntos se utilizan para representar estados y no son manejables situaciones en las cuales el número de estados es infinito.
- Siempre tenemos que poner límites (por ejemplo derivados de nuestra limitación de memoria) y eso hace que nos interesen las estructuras finitas.

Presentación

- Ya hemos estudiado el conjunto de los números enteros, que es un conjunto infinito.
- Aunque esta construcción nos puede resultar muy natural, en criptografía (y en general en la informática) un conjunto infinito es un problema.
- Los conjuntos se utilizan para representar estados y no son manejables situaciones en las cuales el número de estados es infinito.
- Siempre tenemos que poner límites (por ejemplo derivados de nuestra limitación de memoria) y eso hace que nos interesen las estructuras finitas.
- Veamos algunos ejemplos.

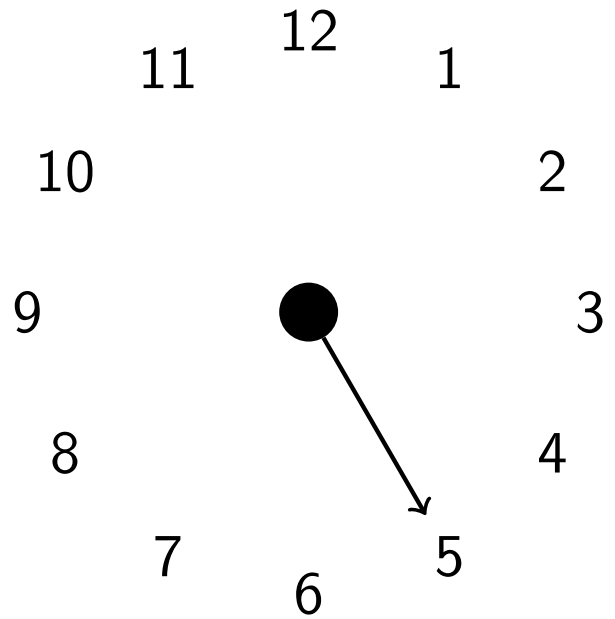
El Reloj I

- Consideremos un reloj que marca las 4.



El Reloj I

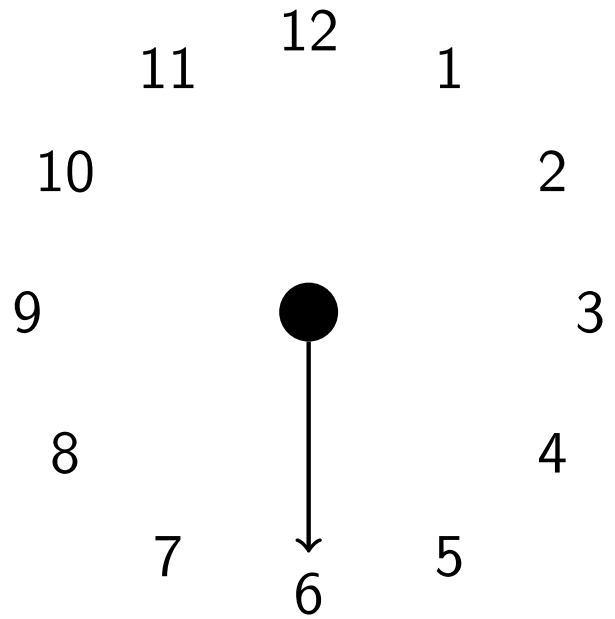
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

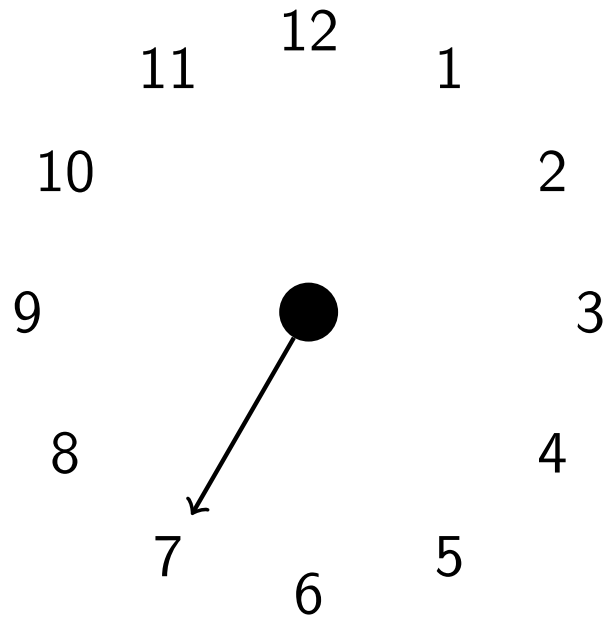
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

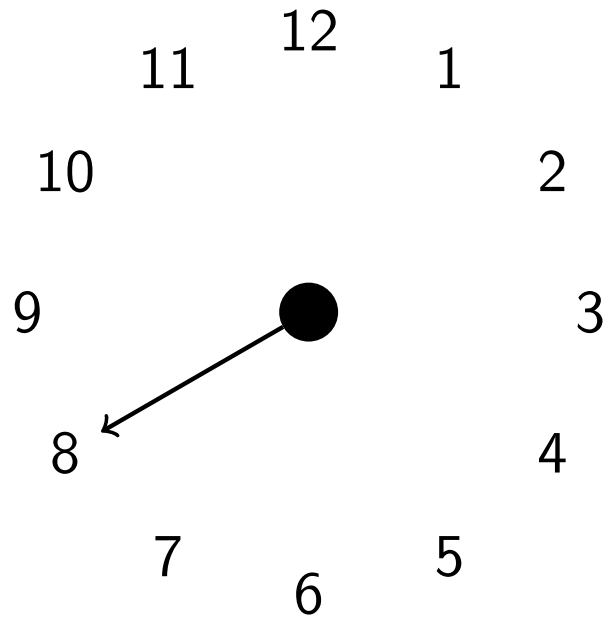
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

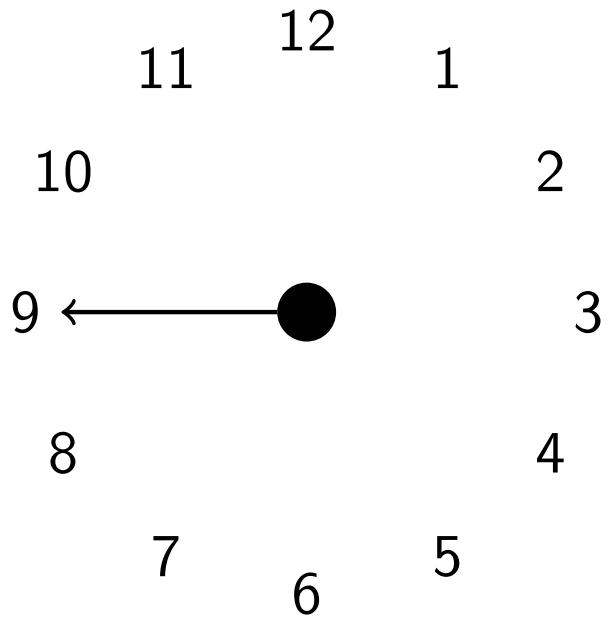
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

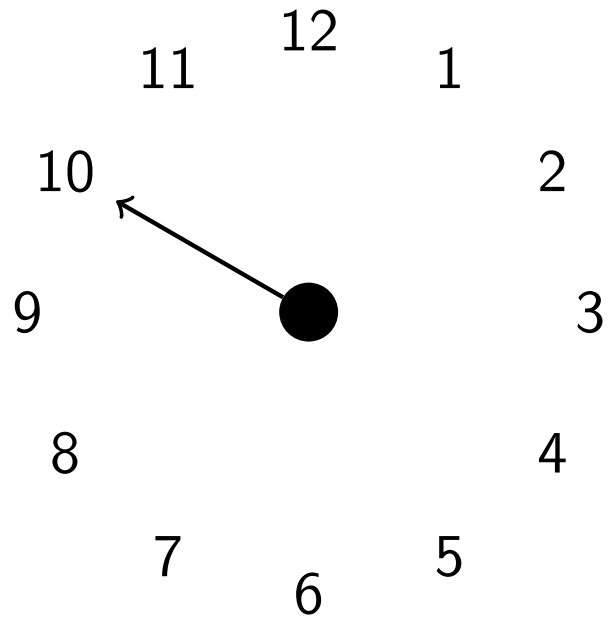
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

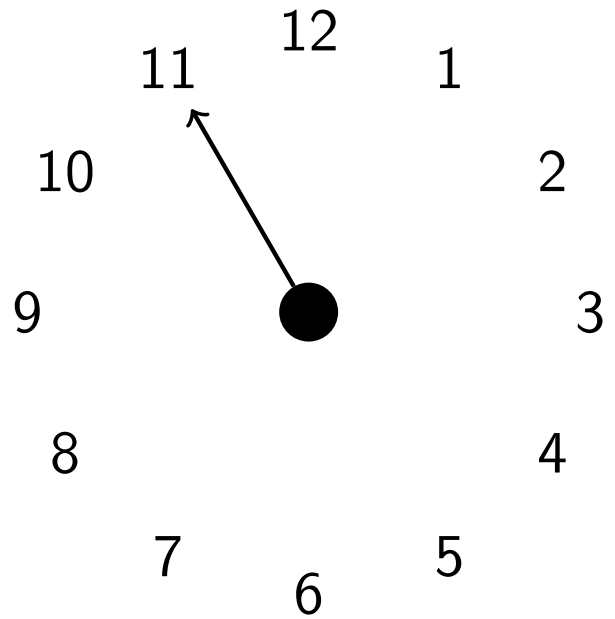
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

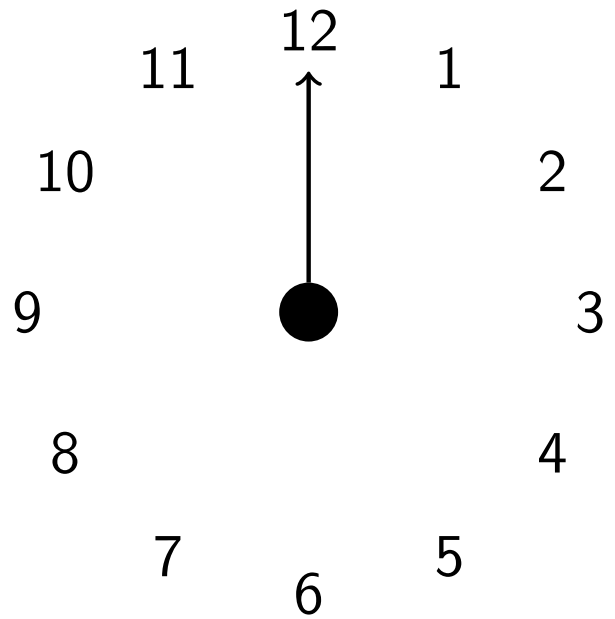
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

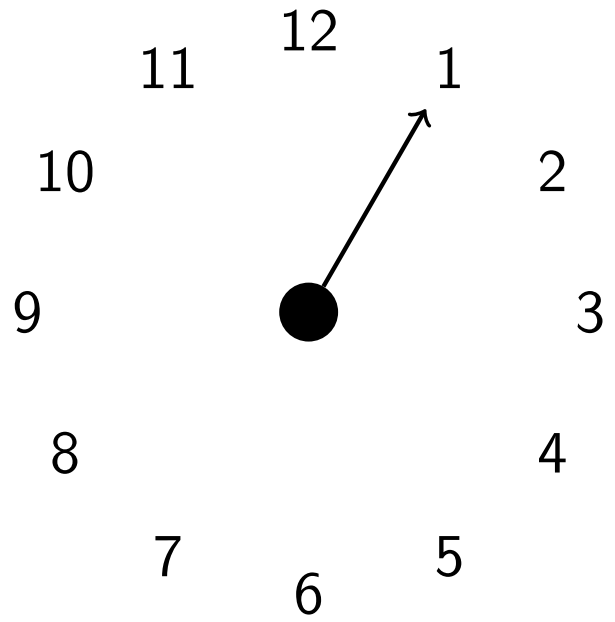
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...

El Reloj I

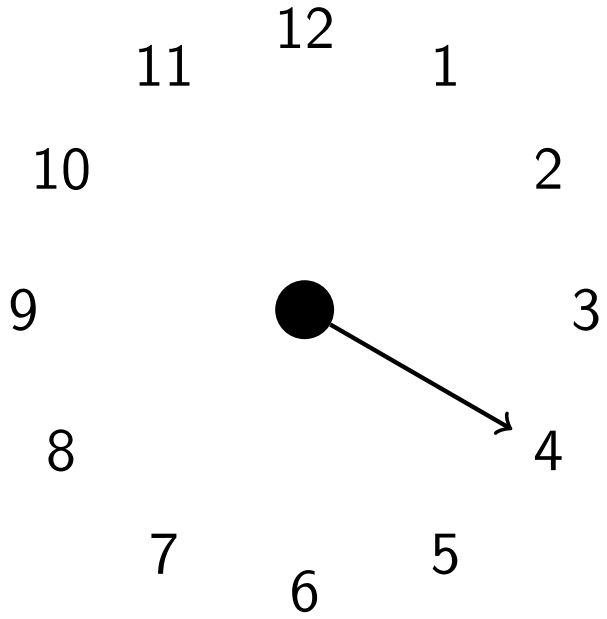
- Consideremos un reloj que marca las 4.



- Si vamos sumando horas una a una iremos obteniendo sucesivamente las 5,6,7,...
- Sin embargo al llegar a las 12, si sumamos 1 no obtenemos 13, sino 1. Hemos completado un ciclo y hemos empezado de nuevo por el principio.

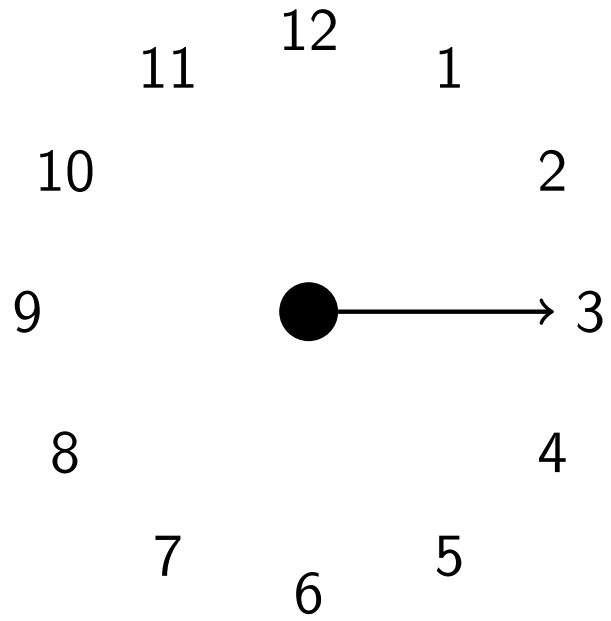
El Reloj II

- Lo mismo sucede si restamos.



El Reloj II

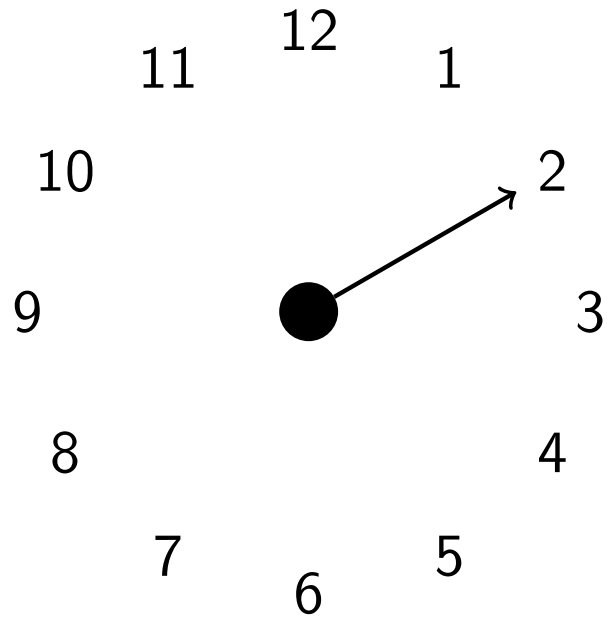
- Lo mismo sucede si restamos.



- Si vamos restando horas iremos obteniendo sucesivamente las 4,3,2,1

El Reloj II

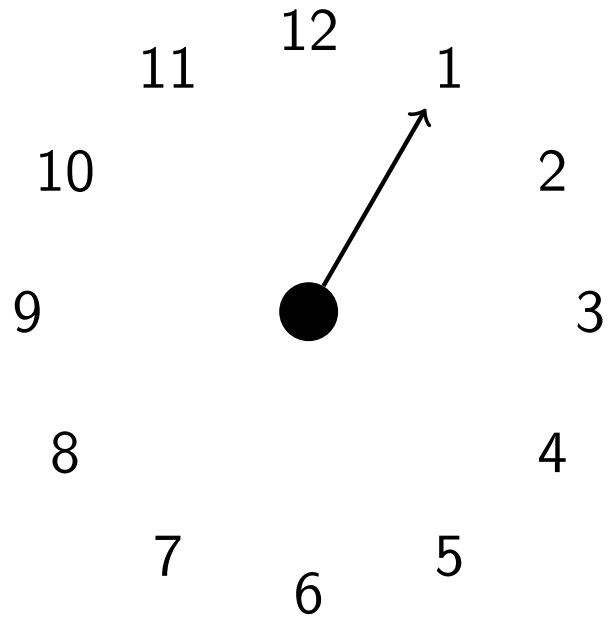
- Lo mismo sucede si restamos.



- Si vamos restando horas iremos obteniendo sucesivamente las 4,3,2,1

El Reloj II

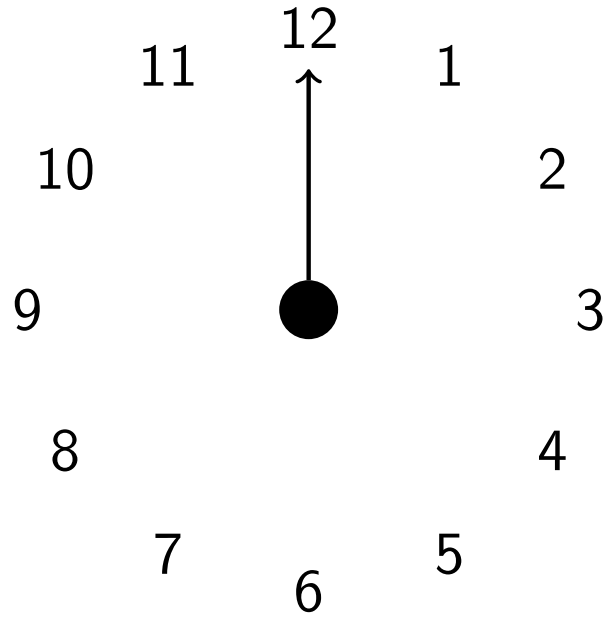
- Lo mismo sucede si restamos.



- Si vamos restando horas iremos obteniendo sucesivamente las 4,3,2,1

El Reloj II

- Lo mismo sucede si restamos.



- Si vamos restando horas iremos obteniendo sucesivamente las 4,3,2,1
- Pero al restar 1 de nuevo obtenemos que son las 12, hemos dado marcha atrás en el ciclo y hemos llegado al final del ciclo anterior.

El Cuentaquilómetros

- Pensemos ahora en el cuentaquilómetros de un coche. Supongamos que dispone de 6 cifras que van marcando desde el kilómetro 000000 hasta el 999999.

El Cuentaquilómetros

- Pensemos ahora en el cuentaquilómetros de un coche. Supongamos que dispone de 6 cifras que van marcando desde el kilómetro 000000 hasta el 999999.
- Cuando superamos la cifra de 999999 kilómetros, el contador vuelve al valor inicial 000000.

El Cuentaquilómetros

- Pensemos ahora en el cuentaquilómetros de un coche. Supongamos que dispone de 6 cifras que van marcando desde el kilómetro 000000 hasta el 999999.
- Cuando superamos la cifra de 999999 kilómetros, el contador vuelve al valor inicial 000000.
- Esto sucede en general con las variables que representan números con un número finito de bits, en esos casos los límites serán potencias de dos cuya representación en binario es del tipo uno seguido de ceros.

El Cuentaquilómetros

- Pensemos ahora en el cuentaquilómetros de un coche. Supongamos que dispone de 6 cifras que van marcando desde el kilómetro 000000 hasta el 999999.
- Cuando superamos la cifra de 999999 kilómetros, el contador vuelve al valor inicial 000000.
- Esto sucede en general con las variables que representan números con un número finito de bits, en esos casos los límites serán potencias de dos cuya representación en binario es del tipo uno seguido de ceros.
- En algunas ocasiones esto es en realidad un error, un contador que no estaba previsto para valores tan grandes, pero en otras ocasiones (especialmente en criptografía) este comportamiento es muy útil y se utiliza para definir aritméticas finitas.

El Cuentaquilómetros

- Pensemos ahora en el cuentaquilómetros de un coche. Supongamos que dispone de 6 cifras que van marcando desde el kilómetro 000000 hasta el 999999.
- Cuando superamos la cifra de 999999 kilómetros, el contador vuelve al valor inicial 000000.
- Esto sucede en general con las variables que representan números con un número finito de bits, en esos casos los límites serán potencias de dos cuya representación en binario es del tipo uno seguido de ceros.
- En algunas ocasiones esto es en realidad un error, un contador que no estaba previsto para valores tan grandes, pero en otras ocasiones (especialmente en criptografía) este comportamiento es muy útil y se utiliza para definir aritméticas finitas.
- Vamos a ver cómo se formaliza matemáticamente.

Congruencias

- Sea n un número entero, $n \geq 1$. Diremos que dos números enteros a y b son congruentes módulo n si $a - b$ es un múltiplo de n.

Congruencias

- Sea n un número entero, $n \geq 1$. Diremos que dos números enteros a y b son congruentes módulo n si $a - b$ es un múltiplo de n.
- En el ejemplo del reloj, $n = 12$ y nos formaliza el hecho de que 13 y 1 tengan la misma representación en nuestro reloj, ya que $13 - 1 = 12$ que es un múltiplo de 12.

Congruencias

- Sea n un número entero, $n \geq 1$. Diremos que dos números enteros a y b son congruentes módulo n si $a - b$ es un múltiplo de n.
- En el ejemplo del reloj, $n = 12$ y nos formaliza el hecho de que 13 y 1 tengan la misma representación en nuestro reloj, ya que $13 - 1 = 12$ que es un múltiplo de 12.
- Del mismo modo 27 y 3 son congruentes, porque su diferencia, 24 es un múltiplo de 12. Esto nos dice que si empezamos a contar desde las 12 y sumamos 27 horas, el reloj nos marcará las 3.

Congruencias

- Sea n un número entero, $n \geq 1$. Diremos que dos números enteros a y b son congruentes módulo n si $a - b$ es un múltiplo de n.
- En el ejemplo del reloj, $n = 12$ y nos formaliza el hecho de que 13 y 1 tengan la misma representación en nuestro reloj, ya que $13 - 1 = 12$ que es un múltiplo de 12.
- Del mismo modo 27 y 3 son congruentes, porque su diferencia, 24 es un múltiplo de 12. Esto nos dice que si empezamos a contar desde las 12 y sumamos 27 horas, el reloj nos marcará las 3.
- La hora 0 y la hora 12 también son congruentes.

Representación de la Congruencia

- Si a y b son congruentes módulo n escribiremos $a \equiv b(mod\ n)$ o bien $a = b(mod\ n)$.

Representación de la Congruencia

- Si a y b son congruentes módulo n escribiremos $a \equiv b(mod\ n)$ o bien $a = b(mod\ n)$.
- En muchas ocasiones en las cuales el valor de n sea claro, escribiremos simplemente $a = b$.

Representación de la Congruencia

- Si a y b son congruentes módulo n escribiremos $a \equiv b(mod\ n)$ o bien $a = b(mod\ n)$.
- En muchas ocasiones en las cuales el valor de n sea claro, escribiremos simplemente $a = b$.
- Por ejemplo, si nuestros números representan posiciones del reloj, podremos escribir $13 = 1$ para indicar que las 13 horas y la 1 son la misma.

Representación de la Congruencia

- Si a y b son congruentes módulo n escribiremos $a \equiv b(mod\ n)$ o bien $a = b(mod\ n)$.
- En muchas ocasiones en las cuales el valor de n sea claro, escribiremos simplemente $a = b$.
- Por ejemplo, si nuestros números representan posiciones del reloj, podremos escribir $13 = 1$ para indicar que las 13 horas y la 1 son la misma.
- Cuando pueda existir duda, escribiremos $(mod\ n)$ para clarificarla.

La Aritmética del Reloj

- Hemos visto que podemos sumar y restar horas del reloj siguiendo la regla de que al final, si el resultado no está entre 1 y 12 sumaremos o restaremos múltiplos de 12 hasta obtener un número congruente con el resultado entre 1 y 12.

La Aritmética del Reloj

- Hemos visto que podemos sumar y restar horas del reloj siguiendo la regla de que al final, si el resultado no está entre 1 y 12 sumaremos o restaremos múltiplos de 12 hasta obtener un número congruente con el resultado entre 1 y 12.
- Esto lo representaremos con las relaciones de congruencia $4 + 9 = 1 (mod\ 12)$ ó $4 - 5 = 11 (mod\ 12)$

La Aritmética del Reloj

- Hemos visto que podemos sumar y restar horas del reloj siguiendo la regla de que al final, si el resultado no está entre 1 y 12 sumaremos o restaremos múltiplos de 12 hasta obtener un número congruente con el resultado entre 1 y 12.
- Esto lo representaremos con las relaciones de congruencia $4 + 9 = 1 (mod\ 12)$ ó $4 - 5 = 11 (mod\ 12)$
- También podemos realizar multiplicaciones con esta misma regla, supongamos que un proceso tarda 5 horas en completarse y el reloj marca las 4, ¿qué hora marcará cuando se haya completado el proceso tres veces?

$$4 + 3 \cdot 5 = 4 + 15 = 19 = 7 (mod\ 12)$$

La Aritmética del Reloj

- Hemos visto que podemos sumar y restar horas del reloj siguiendo la regla de que al final, si el resultado no está entre 1 y 12 sumaremos o restaremos múltiplos de 12 hasta obtener un número congruente con el resultado entre 1 y 12.
- Esto lo representaremos con las relaciones de congruencia $4 + 9 = 1 (mod\ 12)$ ó $4 - 5 = 11 (mod\ 12)$
- También podemos realizar multiplicaciones con esta misma regla, supongamos que un proceso tarda 5 horas en completarse y el reloj marca las 4, ¿qué hora marcará cuando se haya completado el proceso tres veces?

$$4 + 3 \cdot 5 = 4 + 15 = 19 = 7 (mod\ 12)$$

- Por lo tanto el reloj marcará las 7.

La Aritmética del Reloj

- Hemos visto que podemos sumar y restar horas del reloj siguiendo la regla de que al final, si el resultado no está entre 1 y 12 sumaremos o restaremos múltiplos de 12 hasta obtener un número congruente con el resultado entre 1 y 12.
- Esto lo representaremos con las relaciones de congruencia $4 + 9 = 1 (mod\ 12)$ ó $4 - 5 = 11 (mod\ 12)$
- También podemos realizar multiplicaciones con esta misma regla, supongamos que un proceso tarda 5 horas en completarse y el reloj marca las 4, ¿qué hora marcará cuando se haya completado el proceso tres veces?

$$4 + 3 \cdot 5 = 4 + 15 = 19 = 7 (mod\ 12)$$

- Por lo tanto el reloj marcará las 7.
- Fijémonos que en el proceso hemos obtenido un 15 como valor intermedio, si hubiéramos cambiado el 15 por un 3, que es su equivalente módulo 12 habríamos obtenido el mismo resultado:

$$4 + 3 \cdot 5 = 4 + 15 = 4 + 3 = 7 (mod\ 12)$$

La Aritmética del Reloj

- Hemos visto que podemos sumar y restar horas del reloj siguiendo la regla de que al final, si el resultado no está entre 1 y 12 sumaremos o restaremos múltiplos de 12 hasta obtener un número congruente con el resultado entre 1 y 12.
- Esto lo representaremos con las relaciones de congruencia $4 + 9 = 1 (mod\ 12)$ ó $4 - 5 = 11 (mod\ 12)$
- También podemos realizar multiplicaciones con esta misma regla, supongamos que un proceso tarda 5 horas en completarse y el reloj marca las 4, ¿qué hora marcará cuando se haya completado el proceso tres veces?

$$4 + 3 \cdot 5 = 4 + 15 = 19 = 7 (mod\ 12)$$

- Por lo tanto el reloj marcará las 7.
- Fijémonos que en el proceso hemos obtenido un 15 como valor intermedio, si hubiéramos cambiado el 15 por un 3, que es su equivalente módulo 12 habríamos obtenido el mismo resultado:

$$4 + 3 \cdot 5 = 4 + 15 = 4 + 3 = 7 (mod\ 12)$$

- Esta es la regla fundamental que debemos tener siempre presente en la aritmética modular. Si estamos trabajando módulo n, podemos sumar y restar n tantas veces como queramos, tanto en resultados intermedios como en el resultado final, y las operaciones serán correctas en esta aritmética.

El Conjunto de Representantes

- En el caso del reloj hemos visto que cualquier resultado será congruente con alguno del conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.

El Conjunto de Representantes

- En el caso del reloj hemos visto que cualquier resultado será congruente con alguno del conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
- La hora 12 sabemos que es igual a la hora 0, por lo tanto podríamos haber elegido el conjunto de representantes $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ obtenido un conjunto perfectamente válido.

El Conjunto de Representantes

- En el caso del reloj hemos visto que cualquier resultado será congruente con alguno del conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
- La hora 12 sabemos que es igual a la hora 0, por lo tanto podríamos haber elegido el conjunto de representantes $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ obtenido un conjunto perfectamente válido.
- Cuando trabajamos en aritmética módulo n, lo primero que hacemos es elegir un conjunto de n representantes. Hay muchas elecciones posibles, pero son dos las fundamentales, la representación sin signo (unsigned) que corresponde al conjunto $\{0, 1, 2, \cdots, n-1\}$ o la representación con signo (signed) que estaría formada por los valores positivos y negativos más pequeños en valor absoluto.

El Conjunto de Representantes

- En el caso del reloj hemos visto que cualquier resultado será congruente con alguno del conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
- La hora 12 sabemos que es igual a la hora 0, por lo tanto podríamos haber elegido el conjunto de representantes $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ obtenido un conjunto perfectamente válido.
- Cuando trabajamos en aritmética módulo n, lo primero que hacemos es elegir un conjunto de n representantes. Hay muchas elecciones posibles, pero son dos las fundamentales, la representación sin signo (unsigned) que corresponde al conjunto $\{0, 1, 2, \cdots, n-1\}$ o la representación con signo (signed) que estaría formada por los valores positivos y negativos más pequeños en valor absoluto.
- Por ejemplo, en el caso de $n = 5$ la representación sin signo sería $\{0, 1, 2, 3, 4\}$ y la representación con signo $\{-2, -1, 0, 1, 2\}$

El Conjunto de Representantes

- En el caso del reloj hemos visto que cualquier resultado será congruente con alguno del conjunto $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$.
- La hora 12 sabemos que es igual a la hora 0, por lo tanto podríamos haber elegido el conjunto de representantes $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$ obtenido un conjunto perfectamente válido.
- Cuando trabajamos en aritmética módulo n, lo primero que hacemos es elegir un conjunto de n representantes. Hay muchas elecciones posibles, pero son dos las fundamentales, la representación sin signo (unsigned) que corresponde al conjunto $\{0, 1, 2, \cdots, n-1\}$ o la representación con signo (signed) que estaría formada por los valores positivos y negativos más pequeños en valor absoluto.
- Por ejemplo, en el caso de $n = 5$ la representación sin signo sería $\{0, 1, 2, 3, 4\}$ y la representación con signo $\{-2, -1, 0, 1, 2\}$
- El el caso $n = 256$ tendríamos la representación sin signo $\{0, 1, \cdots, 255\}$ y la representación con signo $\{-128, -127, \cdots, -1, 0, 1, \cdots, 127\}$.

Definición de la Aritmética Modular

- Sea n un número entero mayor que 1 que llamaremos módulo y elijamos un conjunto de representantes, por ejemplo $\{0, 1, \cdots, n-1\}$.

Definición de la Aritmética Modular

- Sea n un número entero mayor que 1 que llamaremos módulo y elijamos un conjunto de representantes, por ejemplo $\{0, 1, \cdots, n-1\}$.
- Dados a y b en el conjunto de representantes, podemos sumarlos, restarlos o multiplicarlos módulo n aplicando la regla de que si el resultado final está fuera del conjunto de representantes, sumaremos o restaremos n hasta tenerlo dentro del conjunto.

Definición de la Aritmética Modular

- Sea n un número entero mayor que 1 que llamaremos módulo y elijamos un conjunto de representantes, por ejemplo $\{0, 1, \cdots, n-1\}$.
- Dados a y b en el conjunto de representantes, podemos sumarlos, restarlos o multiplicarlos módulo n aplicando la regla de que si el resultado final está fuera del conjunto de representantes, sumaremos o restaremos n hasta tenerlo dentro del conjunto.
- Una forma rápida de hacerlo es dividir el resultado final por n y quedarnos con el resto de la división, que siempre estará entre 0 y $n-1$.

Definición de la Aritmética Modular

- Sea n un número entero mayor que 1 que llamaremos módulo y elijamos un conjunto de representantes, por ejemplo $\{0, 1, \cdots, n-1\}$.
- Dados a y b en el conjunto de representantes, podemos sumarlos, restarlos o multiplicarlos módulo n aplicando la regla de que si el resultado final está fuera del conjunto de representantes, sumaremos o restaremos n hasta tenerlo dentro del conjunto.
- Una forma rápida de hacerlo es dividir el resultado final por n y quedarnos con el resto de la división, que siempre estará entre 0 y $n-1$.
- Al conjunto $\{0, 1, \cdots, n-1\}$ dotado de estas operaciones lo llamaremos anillo de restos módulo n y lo denotaremos $\mathbb{Z}_n$.

Implementación en sage

- El anillo de restos módulo n en sage se escribe `Zmod(n)`, así podemos poner por ejemplo:

```
for x in Zmod(5):
  print x,
```

Implementación en sage

- El anillo de restos módulo n en sage se escribe `Zmod(n)`, así podemos poner por ejemplo:

```
for x in Zmod(5):
  print x,
```

- y nos escribirá todos los elementos de este conjunto, es decir, $\{0, 1, 2, 3, 4\}$.

Implementación en sage

- El anillo de restos módulo n en sage se escribe `Zmod(n)`, así podemos poner por ejemplo:

```
for x in Zmod(5):
  print x,
```

- y nos escribirá todos los elementos de este conjunto, es decir, $\{0, 1, 2, 3, 4\}$.
- Podemos hacer operaciones con ellos y el resultado nos lo dará siempre en el rango adecuado, por ejemplo

```
for x in Zmod(5):
  print 3*x,
```

Implementación en sage

- El anillo de restos módulo n en sage se escribe `Zmod(n)`, así podemos poner por ejemplo:

```
for x in Zmod(5):
  print x,
```

- y nos escribirá todos los elementos de este conjunto, es decir, $\{0, 1, 2, 3, 4\}$.
- Podemos hacer operaciones con ellos y el resultado nos lo dará siempre en el rango adecuado, por ejemplo

```
for x in Zmod(5):
  print 3*x,
```

- Nos dará los valores
  `0 = 3*0,3 = 3*1, 1 = 3*2, 4 = 3*3, 2 = 3*4.`

Asignación a Variables

- En sage el conjunto `Zmod(n)` no es un tipo de datos, sino un objeto del lenguaje.

Asignación a Variables

- En sage el conjunto `Zmod(n)` no es un tipo de datos, sino un objeto del lenguaje.
- Esto hace que sea totalmente correcto asignarlo a una variable e incluso pasarlo como parámetro en funciones. Por ejemplo:

```
K = Zmod(5)
for x in K:
  print x+1,
```

Asignación a Variables

- En sage el conjunto `Zmod(n)` no es un tipo de datos, sino un objeto del lenguaje.
- Esto hace que sea totalmente correcto asignarlo a una variable e incluso pasarlo como parámetro en funciones. Por ejemplo:

```
K = Zmod(5)
for x in K:
  print x+1,
```

- Nos dará $\{1, 2, 3, 4, 0\}$ exactamente lo mismo que si hubiéramos puesto

```
for x in Zmod(5):
  print x+1,
```