Contents

1. Evaluación

```
1er, 2do Parcial  ... 40 %
Tareas            ... 10 %

Proyecto          ... 25 %
Examen Final      ... 25 %
```

Correos acepta de 2 am a 2:30 am

2. Conjuntos de números

2.1. $\mathbb{C}$omplejos

Los números complejos son una suma de una parte real $\mathbb{R}$ y una parte imaginaria $\mathbb{I}m$, por ejemplo $2 + 3i$.

2.1.1. $\mathbb{R}$eales

Son un subconjunto de los números complejos $\mathbb{C}$ donde no existe la parte imaginaria, por lo que se puede representar en una recta numérica.

2.1.1.1. Racionales (Q) (a/b)

Se representan con un cociente de dos enteros, por ejemplo $\frac{1}{3} = 0.33\bar{3}$, también tenemos por ejemplo el $2 = \frac{2}{1}$

2.1.1.1.1. Enteros ($\mathbb{Z}$)

Que no tienen parte decimal

2.1.1.1.1.1. Enteros negativos (Z')

2.1.1.1.1.2. Monoide (0)

2.1.1.1.1.3. Naturales (N)

Dependiendo de si se denota $\mathbb{N}_0$ o $\mathbb{N}_1$ se considera si el conjunto incluye al 0 o no, esto depende de si conviene o no para los trabajos de investigación. Entonces $\mathbb{N}_0 = \{0, 1, 2, ...\}$ y $\mathbb{N}_1 = \{1, 2, ...\}$

2.1.1.1.1.3.1. Primo: Divide entre si y 1

2.1.1.1.1.3.2. Compuesto: Los demás, 3+ divisores

2.1.1.2. Fraccionarios (F)

Todos los demás que no son enteros

2.1.2. $\mathbb{I}$rracionales ($\mathbb{I} = \mathbb{R} - Q$)

Entre estos tenemos razones que no son repetitivas en su parte decimal, es decir que no hay patrones en la secuecia de números decimales como con $\pi, \sqrt{2}, \tau, e$

También tenemos aqui todas las raíces de números primos.

2.1.2. $\mathbb{I}m$aginarios

En los números imaginarios se entiende $i = \sqrt{-1}$. Para descartar rápidamente numeros que no están expresados de la forma imaginaria solo tenemos que fijarnos en el *exponente* de la raíz.

$$\sqrt[n]{a}$$

En caso de que a sea un número negativo y n sea par, entonces podemos decir con seguridad que se trata de un número imaginario.

En todos los demás casos el resultado obtenido será $c + 0i$, donde no existe una parte imaginaria.

3. Introducción a conjuntos

3.1. Definición de conjunto

Un conjunto es una colección de *elementos*. Sea A un conjunto de elementos que puede ser finito o infinito se dice que a es elemento de A si, y solo si $a \in A$.

Por lo tanto se puede decir que $A \in \{a\}$.

Simbologia:
- $\exists$ existe
- $\nexists$ no existe
- $\exists!$ existe solo para
- $\in$ pertenece
- $\notin$ no pertenece
- $<, \leq, >, \geq$ menor, menor que, mayor, mayor que
- $\ll, \gg$ super mayor y super menor, se usan para decir que el objeto que se está analizando es tan grande que no cabe en el sistema, por lo tanto se puede simplificar.

Escalamiento: Si se die que un valor es orden a la 1 ($x \approx O(1)$) se da a entender que el valor es muy pequeño. Al programar se puede usar el $\approx O(1)$ para poder aceptar gráficas experimentales resultantes del ruido del sistema y programación que son distintaas a la grafica ideal.

Para definir un conjunto se puede hacer de dos maneras; *exetnsiva* donde se enumeran todos los elementos o *comprensiva*, donde se usa la lógica para poder obtener una expresión sobre los elementos.

Ejemplo:
- Extensiva:
  - $\{a, b, c, d, e\}$
- Comprensiva
  - $\{x \mid x \text{ son las vocales}\}$
  - $\{x \mid x \text{ son las vocales de la palabra casa}\} = \{a\}$, nótese como los conjintos solo pueden tener una vez los elementos
  - $\{x \in \mathbb{N}_0 | -3 \leq x < 2\}$, donde $\mathbb{N}_0$ indica que nuestros naturales van desde el 0, en este caso es igual a $\{0, 1\}$
  - $D \in \{x \in \mathbb{Z} \mid x^2 - 4 = 0\} = \{2, -2\}$
  - $F \in \{x \in \mathbb{R} | x^2 + 9 = 0\} = \emptyset$, debido a que la solución es $x = +-3i$, que no se encuentra en los reales
  - $R \in \{x \in \mathbb{C} \mid x^2 + 2x + 1 = 0\}$ que es $\{-1\}$ porque la solución es repetida $(-1, -1)$

3.2. Operaciones

Unión: Sea $A \wedge B \neq \emptyset$, dos conjuntos no vacíos tal que $A \cup B = \{x \mid x \in A \vee x \in B\}$, donde juntamos los elementos de ambos.

Intersección: $\{x \mid x \in A \wedge x \in B\}$, es decir, los que estan en ambos conjuntos.

Diferencia: $A/B = A - B = \{x \mid x \in A \wedge x \notin B\}$, lo que no tiene el de la derecha la izquierda; los elementos que le faltan a B para ser A

Complemento: $A^c = \{x \mid x \in U \wedge x \notin A\}$, lo que le falta ser a A para ser el universo U

Diferencia simétrica: $A \triangle B$ o $A \oplus B$ que es $(A - B) \cup (B - A)$, es decir, todo lo que no se repite en A y B, es decir, todos los elementos que no son parte de $A \cap B$ pero que esten en $A \vee B$.

3.3. Ejercicio

Sea
- $U = \{x \in \mathbb{N} \mid 1 \leq x < 100\} = \{1, 2, 3, .., 99\}$
- $A = \{x \in \mathbb{N} \mid 3 < x \leq 7 \wedge x^2 - 5x + 6 = 0\} = \emptyset$
- $B = \{5, 6, 10, 11\}$
- $C = \{x \in \mathbb{N} \mid 2 < x \wedge x < 11\} = \{x \in \mathbb{N} \mid 2 < x < 11\} = \{3, 4, 5, 6, 7, 8, 9, 10\}$

a)

$$\begin{aligned}(A \oplus B) \cup (B \cap C) \\ &= \{5, 6, 10, 11\} \cup (5, 6, 10) \\ &= \{5, 6, 10, 11\}\end{aligned}$$

b)

$$
\begin{aligned}
[(B-C)\cup(C-B)]^c \cap (A-B)^c & \\
&= (B \oplus C)^c \cap (A-B)^c \\
&= \{3,4,7,8,9,11\}^c \cap \emptyset^c \\
&= \{3,4,7,8,9,11\}^c \cap E \\
&= \{3,4,7,8,9,11\}^c \\
&= \{1,2,5,6,10,12,13,..,99\}
\end{aligned}
$$

donde E es el universo y por lo tanto $A \cap E = A$

4. Exposisición

10 min, teoria, comporbar con codigo, etc

5. Fuzzy set mapping

Los conjuntos difusos se utilizan más para inteligencia artificial, se establecen dos limites, uno inferior y otro superior

```
"""
Implementa un algoritmo de mapeo de conjuntos difusos

Args:
    x: El valor de entrada
    a: Limite inderior del conjunto difuso
    b: Limite superior del conjunto difuso
    c: La pendiente dle conjunto difuso

Devuelve el valor de salida del mapero de conjunto difuso

Ejemplo fuzzy_set_mapping(0.5, 0, 1, 1)
"""
def fuzzy_set_mapping(x, a, b, c):
    # No se está usando c
    if x < a:
        return 0
    elif x > b:
        return 1
    else:
        return (x - a) / (b - a)
```

El código tiene dos parámetros, el limite inferior y superior (0 y 1), entonces esta función se encarga de decir si alguien está o no en el conjunto, en caso de que no puede dar un intervalo, que puede servir de preferencia.

Ejemplo Taylor Swift tiene una holgura de 0.9, The Weekend 0.7, Peso Pluma 0.5. Es asi que la pendiente nos da una holgura para estar posicionado entre si o no, ser famoso esta distribuido en el intervalo dado de 0 a 1.

En el conjunto difuso se le da la oportunidad de entrar en el limite inferior y superior con una holgura dada.

La holgura se asigna dependiendo de la actividad.

Ejemplo de pedazos de coche, un pistón no puede tener mucha diferencia, ni siquiera milimetrico, este es un ejemplo de diferencia, de holgura que hay entre las piezas. La holgura y tolerancia se la damos para determinar si cierto objeto puede ser elemento a un dado conjunto.

> **Tarea**: En la tarea hay que describir qué está haciendo, están considerados como aptos para pertenecer al conjunto hasta cierto punto, hay que decir de qué nos serviría en nuestra carrera, las modificaciones que haríamos y explicarlo.

6. Temas de investigación

1. Resolver sistemas de ecuaciones lineales con el metodo de gauss no se que acelerado, en cualquier sistema se le puede meter una impedancia para acelerar el procedimiento
2. Integrar funciones multiples por el metodo se simpson 3/4 y 1/2
3. Resolver ecuaciones
4. Ecuaciones lineales por el metodo de roca meta no se que verga
5. Resolver ecuaciones parciales por el metodo de diferencias finitas

- Como hacer el metodo, como se resuleve matematicamente, tenemos que saber el principio, y hacer el código.

1. Como calcular la raiz de un polinomio 2500 iteraciones
1. Explicar qué son los métodos cerrados y métodos abiertos, bien detallado y las condiciones del intervalo que trabajan, de ahi:
   - Metodos cerrados: El método de disección solamente
   - Método abierto: El método de la secante y el método de newton-rapson
   - Apliccación, el código, cómo lo hicimos, qué habilita
   - 2500 iteraciones

7. Teoría de números

La teoría de números es una de las ramas de la matematicas que estudia los números naturales ($\mathbb{N}$) y los enteros, de los enteros ($\mathbb{Z}$) estudia sus propiedades.

Recordemos que:
- Los numeros enteros son $\{..., -1, 0, 1, ...\}$
- Nuestra definición de naturales no invluye 0 por defecto

7.1. Conjetura de Goldbash

En teoría de números cambian las definiciones con respecto a las matemáticas tradicionales. Goldbash dice que
- Para los números pares, los pares mayores a 2 $\mathbb{P} + \mathbb{P}$, se pueden extraer de la suma de dos números primos, ej. $3 > 2 \Leftrightarrow 3 = 2 + 1$
- Para los números impares mayores a 5 $\mathbb{P} + \mathbb{P} + \mathbb{P}$, todos son igualables a la suma de tre números primos, ej $7 = 2 + 2 + 3$

7.2. Teorema de Fermat

Partiendo de Pitágoras $a^2 + b^2 = c^2$, Fermat exploró qué sucede con las expresiones al ser de grado n de la forma $a^n + b^n = c^n$. El dice que es imposible encontrar 3 números enteros positivos tal que $a^n + b^n = c^n$ cuando $n > 2$.

7.3. Ejemplos de demostraciones

La forma para representar $2^2 = 4$ podemos dibujar 4 puntos en un cuadrado, haciendo gráficamente un cuadrado con 4 puntos, si es 3^2 hacemos un cuadrado de 9 puntos.

Asi como vemos que existen números cuadrados pueden existir números *triangulares*, en el caso de los números cuadrados es n^2, para los triangulares tenemos $\{3, 6, 10, 15, ...\}$, en la teoría de números debemos buscar una función que pueda modelar la representación.

$$\frac{(n)(n+1)}{2}$$

Debemos de hacer el análisis que logre describir la serie de números para resolver los problemas que se nos presenten. La teoría de números se emplea en distintos tipos de entrada.

No vamos a estar haciendo en loops sumas, series, que pueden moldearse en una función que permite describir para cualquier posición t el valor.

7.3.1. Suma

Otro ejemplo de fórmula, la fórmula que describe cualquier suma consecutiva de números

$$\frac{n(1+n)}{2}$$

Es decir, vamos a empezar a demostrar de forma inductiva, por medio de una función.

7.3.2. Paridad de enteros

Partiendo de $n \in \mathbb{Z}$, podemos definir:
- Par: $2n$
- Impar: $2n + 1$

Y podemos analizar las propiedades:
- par + par = par
- par + impar = impar
- impar + impar = par
- par $\times$ par = par
- impar $\times$ impar = impar

Y podemos demostrar, por ejemplo par $\times$ par = par de la forma:

$$
\begin{aligned}
(2n+1)(2n+1) & \\
&= (2n+1)^2 \\
&= 4n^2 + 4n + 1 \\
&\therefore \text{impar}
\end{aligned}
$$

7.3.3. Divisores

Sea $a, b \in \mathbb{Z}$ tal que $a \neq 0$ y se dice que a debe ser *divisor* de $b \Rightarrow K$, donde $K \in \mathbb{Z}$ que satisface $b = ka$. Si depejamos $k = \frac{b}{a}$.

El teorema de divisor lleva, naturalmente, a los números primos.

7.3.4. Divisor trivial

Con *trivial* hablamos de proposiciones que no es necesario demostrar, la sola proposición lo demuestra.

El divisor trivial es

Entonces los primos son aquellos que tienen divisores triviales.

7.3.5. Teorema fundamental de la aritmética

Cada entero puede ser factorizado por el producto de números primos, por ejemplo $6 = 3 \times 2$.

7.3.6. Primos de Mersenne

Aquellos números que están derivados de la expresión $M(p) = 2^p - 1$, donde $p \in \mathbb{P}$. Con los primeros 20 primos de la teoría de la aritmética, hallar los 20 primeros números primos de Mersenne.

El código resultante, delegando la generación de los números primos al *crate* `primes`, es:

```rust
use primes::{PrimeSet, Sieve};

fn main() {
    for p in Sieve::new().iter().take(20) {
        println!("{}", 2u128.pow(p as u32) - 1);
    }
}
```

Con la salida del programa:

```
   Compiling primos v0.1.0 (/Users/alejandro/repos/primos)
    Finished dev [unoptimized + debuginfo] target(s) in 0.40s
     Running `target/debug/primos`
3
7
31
127
2047
8191
131071
524287
8388607
536870911
2147483647
137438953471
2199023255551
8796093022207
140737488355327
9007199254740991
576460752303423487
2305843009213693951
147573952589676412927
23611832414348226068 47
```

7.4. Divisores

Sean $a, b \wedge C$ números enteros ($\mathbb{Z}$) donde $a \neq 0$:

1. Si $a|b \wedge a|c \Rightarrow a|(b+c)$, donde $a|b = \frac{b}{a}$, por ejemplo $4|12 = \frac{12}{4} \in \mathbb{Z}, k := 3, b := 12, a := 4$

   Prueba con $b = k_1 a \wedge c = k_2 a$

   $$\begin{aligned} & b + c \\ & \quad = k_1 a + k_2 a \\ & \quad = (k_1 + k_2)a \Rightarrow a \mid (b + c) \end{aligned}$$

2. Sea $a|b \Rightarrow a|bc$, para todo entero c, es decir, que si a es divisor de b, entonces también será divisor de todo bc donde $c \in \mathbb{Z}$

   Ejemplo $2|10 \Rightarrow 2|(10 \times 3) \Rightarrow \frac{30}{2} = 15$

3. Si $a|b \wedge b|c \Rightarrow a|c$, es decir, que si a es divisor de b, y b es divisor de c, entonces a será divisor de c

   Prueba, usando la definición anterior, $a|b \Rightarrow b = k_1 a$ y $b|c \Rightarrow c = k_2 b$:

   Sustituimos b

   $$c = k_2 k_1 a \Rightarrow a|c$$

7.5. Numeros perfectos

Se dice que m es un número perfecto si es que $m \in \mathbb{Z}^+$ y resulta de la suma de sus divisores, a excepción de la base, la suma de todos sus divisores da como resultado la base misma, por ejemplo $6 = 1 + 2 + 3$

Hay 49 números perfectos y 49 primos de Mercenne, para obtenerlo podemos hacer:

$$M = 2^{p-1}(2^p - 1) = 2^{p-1}(M(P))$$

Con esta fórmula podemos obtener números perfectos a partir de primos de Mercenne

$$M_1(p) = 2^2 - 1 = 4 - 1 = 3$$
$$M_2(p) = 2^{2-1}(3) = 2 \times 3 = 6$$

Los números tan grandes son dificiles de manejar, hace que se pierda precisión, que es base, en parte, para la criptografía.

7.5.1. Código

2, 3, 5, 7, 11, 13, 17, Si el número primo de Mercenne es primo, entonces obtener el número perfecto, si no, descartarlo.

Si al evaluar los primos en la función de Mercenne da un primo, entonces al valor que genere le calculamos el perfecto. Debe salir el número original, el de Mersene y el perfecto.

```rust
extern crate primes;
use primes::{PrimeSet, Sieve};

fn main() {
    for p in Sieve::new().iter().take(7) {
        let m = 2u128.pow(p as u32) - 1;
        if Sieve::new().is_prime(m as u64) {
            println!("{p}: {m} ⇒ {}", 2u128.pow((p - 1) as u32) * m)
        }
    }
}
```

7.5.2. Demostración

$$M = 2^{p-1}(2^p - 1)$$

En este caso tenemos 2 elevado a $p-1$, que tiene divisores $1, 2, 4, ..., 2^{p-1}$, si sumáramos todos los valores quedaría $2^0 + 2^1 + 2^2 + ... + 2^{p-1} = 2^p$

Si sus dos triviales son 1 y 2^p y tomando en cuenta que la suma de los divisores debe de dar el número perfecto, entonces, si el número es la suma de los divisores ($1 + 2^p - 1 = 2^p$).

Ahora tenemos $2^p(2^p - 1) - 2^{p-1}(2^p - 1)$, si factorizamos queda $2^{p-1}(2^p - 1)(2 - 1) = 2^{p-1}(2^p - 1)$

7.6. Divisibilidad

Para cualquier $a, c \in \mathbb{Z}^+$, donde $a \neq 0$, entoncesi $a|b \wedge a|c \Rightarrow a|(mb + nc)$ donde $m, n \in \mathbb{Z}^+$

Entonces, se cumple:

$$\begin{aligned} 5|10 \wedge 5|20 &\Rightarrow 5 \mid (2 \times 10 + 20 \times 40) \\ &\Rightarrow 5 \mid (20 + 80) \\ &\Rightarrow 5 \mid 100 \end{aligned}$$

7.7. Def, algoritmo de division

Sea $a, b \in \mathbb{Z}$, y $b \in \mathbb{Z}^+$, tal que al expresar la división se conforma como $a = bq + r$, donde $q, r \in \mathbb{Z}$ y son únicos. Aqui la q es el cociente, r el residuo, donde debe cumplirse $0 \leq r < b$.

Se le llama entero único porque se trabaja con la aritmética regular. Solo habrá una combinación de r, q que cumpla con el intervalo que logre dar el resultado. Por ejemplo $\frac{3}{7}$ solo permite tener un residuo $0 \leq r < 7$.

7.7.1. Prueba de existencia

En esta prueba mostramos que los números $q \wedge r$ cumplen con la igualdad

$$\begin{gathered} -3, -2, -1, 0, 1, 2, 3 \\ -3b, -2b, -1b, 0b, 1b, 2b, 3b \end{gathered}$$

Y vemos que sea $0 \leq r < b$

Partiendo de:

$$\begin{gathered} a = bq + r \\ bq \leq a \leq (q + 1)b \end{gathered}$$

Es decir, que el valor en a debe ser mayor a 0 y debe ser menor al que sigue $((q + 1)b)$ de forma que podamos hacer $r = a - bq$

7.7.2. Prueba Unicidad

En esta prueba verificamos que q, r son únicos.

Si tenemos el teorema de divisibilidad $a = bq + r$, entonces, si nos encontramos con una combinación que da el mismo resultado, $a = bq_1 + r_1 \wedge a = bq + r$. Entonces $r < r_1 < b$, si los dos valores de a son iguales en ambos lados, siendo dos combinaciones diferentes, podemos:

$$bq_1 + r_1 = bq + r$$

Si tenemos $bq_1 + r_1 = bq + r$, podemos despejar de la forma:

$$\begin{aligned} bq_1 + r_1 &= bq + r \\ r_1 - r &= bq - bq_1 \\ r_1 - r &= b(q - q_1) \end{aligned}$$

Entonces, si $0 \leq r_1 - r < b$, se tiene que no es posible tener $b \mid (r_1 - r)$, solo es posible si $r_1 = r \Rightarrow q = q_1$, y particularmente solo con 0.

$$\frac{r_1 - r}{b} \in \mathbb{Q} \Rightarrow \nexists$$

7.8. Aritmética modular

En la igualdad, dada en el algoritmo de división, queda $a = bq + r$, donde:

- a es el *dividendo*
- b es el *divisor*
- q es el *cociente*
- r es el residuo
- A q se le conoce como $q = a$ división $b = \left[\frac{a}{b}\right]$, donde $a \in \mathbb{Z}$

- A r se le conoce como $r = a \text{ modulo } b = a - b$, donde $b \in \mathbb{Z}^+$

Ejemplo, sea $101 \div 12$ quedaría descompuesto de la forma $101 = 12 \times 8 + 5$, donde se cumple la condición de $0 \leq 5 \leq 12$.

Expresado como módulo quedaría $5 = 101 \bmod 12$, y como división $8 = 101 \text{ div } 12$

Ejemplo: $191 \div 3$:
- $191 = 14 \times 13 + 9$
- $14 = 191 \text{ div } 13$
- $9 = 191 \bmod 13$

Ejemplo: $-11 \div 3$:
- $-11 = 3 \times -3 - 2$
  - En este caso $0 \leq -2 < 3$ no se cumple, no es una q válida
- $-11 = 3 \times -4 + 1$
  - En este caso $0 \leq 1 < 3$ si se cumple, es una q válida

Nota: El residuo o resto no puede ser negativo, tener en cuenta que el número entero a es divisible por el número b, sii el ressiduo $r = 0 \Rightarrow \left[\frac{a}{b}\right]$

Sea $a, b \in \mathbb{Z}^+$

- Si $a = bq$ para $q \in \mathbb{Z}^+$, entonces $-a = (-q)b$ En este caso, cuando $-a$ si (< 0) es dividido por un b si (> 0) al cociente es -9 donde (< 0) y el residuo es $r = 0$
- Si $a = bq + r$ para un cociente $q \in \mathbb{N}$ y se encuentra $0 < r < b$ entonces $-a = (-q)b - r$

  En este caso el valor de b tiene que mantenerse absoluto, por lo que: $-a = (-q)b + b - b - r$

  Si los juntamos queda: $-a = (-q)b - b + b - r$

  Estamos sumando/restando b para no modificar la expresión, ahora podemos factorizar:
  $-a = (-q - 1)b + (b - r)$

  Con esto logramos que r entre en el intervalo de $0 < r < b$

  En este caso r nos da positivo porque al restarle el valor de b que es mayor a el queda como positivo, o algo asi.

  Ejemplo:

$$-11 = (-4)(3) + 1$$

7.8.1. Pseudocogido

Para el caso 2, cuando el dividendo $(-a)$ es menor a 0, es dividido por b donde $b > 0$, el cociente es $-q - 1$ y el residuo es $b - r$, siempre y cuando $0 < b - r < b$

```
Donde a, b in ZZ:
q := cociente
r := residuo

si a = 0
    q = 0
    r = 0
si no
    r = abs(a)
    q = 0

    mientras r ⩾ b
        r = r - b
        q = q + 1 #el cociente afecta el sig valor

    si a > 0 #no pasa nada
        q = q
        r = r

    # Ultimos dos casos, donde tenemos valor de divisor negativo y de residuo 0,     # no
necesitamos agregar un resultado maś
    sino si r = 0 # Primer punto de hoy
        q = -q
        r = r
    sino #segundo punto de hoy
        q = -q - 1
        r = b - r
```

```rust
fn div(a: i64, b: i64) → (i64, i64) {
    let mut res = (0, 0);
    let (ref mut q, ref mut r) = res;

    if a == 0 {
        return res;
    }

    *r = a.abs();
```

```
    while *r >= b {
        *r -= b;
        *q += 1
    }

    if a > 0 {
        // Cuando son positivos no hacemos nada
    } else if *r == 0 {
        // Si el residuo es 0 existe la posibilidad
        // de que podamos tener un cociente negativo
        *q = -*q;
    } else {
        // Si no, un residuo
        *q = -*q - 1;
        *r = b - *r;
    }

    res
}
```

7.9. Aritmética modular

Si $a \wedge b$ son números enteros y $m \in \mathbb{Z}^+$, entonces a es congruente con $b \mod n$ si m divide a ab, es decir: $m \mid (a-b) \Rightarrow \frac{a-b}{m} \in \mathbb{Z}$

Vamos a trabajar con puros residuos, donde congruente es *idéntico*, como en JS con $===$

Axiomas:

1. La notación $a \equiv b \mod m$ (donde congruente es $\equiv$) es una congruencia (en geometria, misma forma/tamaño) y que m es su módulo
2. 2 números enteros son congruentes de mod m si y solo si, y solo si, se tienen los mismos residuos cuando se dividen por m.

Determina si 17 es congruente con $5 \mod 6$ y $24\ 14 \mod 5$:

- $a \equiv b \mod m$, entonces $15 \equiv 5 \bmod 6$, si $m \mid (a-b)$: $17 - 5 = \frac{12}{6} \Rightarrow 2$, es congruente
- $24 \equiv 14 \bmod 5$: $24 - 14 = \frac{10}{5} \to 2$, es congruente
- $24 \equiv 14 \bmod 6$: $24 - 14 = \frac{10}{6} \in \mathbb{Q}$, no es congruente $24 \not\equiv 14 \mod 6$

En el examen viene hasta aqui. Viene:

- Teoria de conjuntos
- Codigo, relacionado con divisibilidad. Hay que tener relacionados los divisores de sumas

8. Unidad 2

Gauss, intervino en las leyes de Maxwell y también en teoría de números. El dice

Teorema 2: Sea $m \in \mathbb{Z}^+$ tal que $a \wedge b$ son congruentes para un módulo de m, si existe un $K \in \mathbb{Z}$ que satisface la expresión:

$$a = b + Km$$

8.1. Clase

$$Z_m, \hat{a} = \{b \in \mathbb{Z} \mid a \equiv b \bmod m\}$$

Ejemplo, un número cualquiera dividido entre 2 si da 0 es par, si no es impar, por ejemplo,

Hat se coloca porque puede ser tanto positivo como negativo. Que posibles residuos pude hacer del número

8.2. Operaciones entre modulos

$$a \bmod m + b \bmod m = (a+b) \bmod m a \bmod m * b \bmod m = (a*b) \bmod m$$

$$\begin{aligned}&\hat{5}+\hat{6}\\&\quad=(5+6)\bmod 6\\&\quad=11\bmod 6\\&\quad=5\end{aligned}$$

$$\begin{aligned}&\hat{7}\times\hat{4}\\&\quad=(7\times 4)\bmod 6\\&\quad=23\bmod 6\\&\quad=4\end{aligned}$$

Los espacios vectoriales se rigen en anillos conmutativo, aunque cambiemos la posición de los elementos debe cumplirse la operación.

$$\hat{a}+\hat{b}\in\mathbb{Z}\ \text{(cerradura)}$$
$$\hat{a}+\hat{b}=\hat{b}+\hat{c}\ \text{(conmutativa)}$$
$$\hat{a}+\left(\hat{b}+\hat{c}\right)=\left(\hat{a}+\hat{b}\right)+\hat{c}\ \text{(asociativa)}$$
$$\hat{a}*\left(\hat{b}+\hat{c}\right)=\hat{a}\hat{b}+\hat{a}\hat{c}\ \text{(distributiva)}$$
$$\hat{a}+0=0+\hat{a}=\hat{a}\ \text{(elemento neutro)}$$
$$\hat{a}*1=1*\hat{a}=\hat{a}\ \text{(elemento neutro multiplicativo)}$$

Ejercicios:

$$\begin{aligned}&\hat{5}\left(\hat{2}+\hat{3}\right)+\hat{6}\left(\hat{7}+\hat{4}\right)\frac{z}{\hat{5}}\\&\qquad=\hat{5}*\hat{2}+\hat{5}*\hat{3}+\hat{6}\left(\hat{7}+\hat{4}\right)\\&\qquad=\widehat{10}+\widehat{15}+\hat{6}\left(\hat{7}+\hat{4}\right)\\&\qquad=\widehat{10}+\widehat{15}+\hat{6}*\hat{7}+\hat{6}*\hat{4}\\&\qquad=\widehat{10}+\widehat{15}+\widehat{42}+\widehat{24}\\&\qquad=\widehat{91}\\&\qquad=\widehat{91}\bmod\hat{5}=\hat{1}\end{aligned}$$

$$\begin{aligned}&\hat{4}+\left(\widehat{11}+\hat{3}\right)+\hat{4}\left(\hat{8}+\hat{3}\right)\frac{z}{\hat{4}}\\&\qquad=\widehat{18}+\widehat{32}+\widehat{12}\\&\qquad=\widehat{30}+\widehat{32}\\&\qquad=\widehat{62}\bmod\hat{4}=\hat{2}\end{aligned}$$

Es testado, lo que quiere que va a devolver 0 y 1 Testado quiere decir que viene de la proyección {0, 1, 2, 3, m - 1}. Entonces el primero devuelve 0. El segundo devuelve 0, 1.

z/n es z de cocientes.

Que sea testada quiere decir que va a devolverlos con 0, 1, ..., m-1.

El 0 y 1 que sale quiere decir que son los posibles residuos que pueden salir del modulo.

Inverso modulo m (unidad) y divisores de cero:

Hay numeros primos y co-primos.

Sea $a\in\frac{Z}{m}$, a es una unidad si tiene inverso, es decir, existe un $b\in\frac{Z}{m}$ tal que ab va a ser congruente $ab\equiv ba\equiv 1(\bmod m)$.

O sea $a^{-1}=b\Rightarrow a^{-1}\times a=1$.

Congruente: $a \equiv b \bmod m$ es congruente si $\frac{a-b}{m} \in \mathbb{Z}$

Ejemplo:

$$2 \times a \equiv 1 \bmod 5 \text{ que numero cumple con el inverso y que sea congruente?}$$
$$2 \times 3 \equiv 1 \bmod 5$$
$$6 \equiv 1 \bmod 5$$
$$6 \equiv 1 \bmod 5$$
$$\text{También se cumple que}$$
$$\frac{6-1}{5} \in \mathbb{Z}$$
$$3^{-1} \equiv 2 \bmod 5$$

Aqui los coprimos serían 3 y 5.

Por otra parte $\hat{a} \neq 0$, es divisor de 0 en $\frac{Z}{m}$, si existe $b \in \frac{Z}{m}$ donde $b \neq 0$, tal que $\hat{a}\hat{b} = 0$

Ejemplo:

- Esto nos indica que son divisores si:

$$\hat{2} \times \hat{3} = \hat{0} \bmod(6)$$
$$\hat{6} = \hat{0} \bmod(6)$$

- Este nos indica que ambos son inversos y que el único dividos es 1.

$$\hat{2} - \hat{3} = 1 \bmod 5$$

De esto podemos decir que

$$Z_m \{_{\text{(a) } \hat{a} \text{ es una unidad si y solo si mcd}(a,m)=1)}{}_{\text{b) } \hat{a} \text{ es divisor de 0 si y solo si se encuentra } 1< \text{mcd}(a,m)<m}$$