Universidad Nacional Autónoma de México

Facultad de Ingeniería
Semestre 2021-1
Estructuras discretas
Grupo 3
Camarena Ruiz Diego Henok

Tutorial | Tema 2.3 | Congruencias.

Fecha de entrega: 5 de enero del 2021

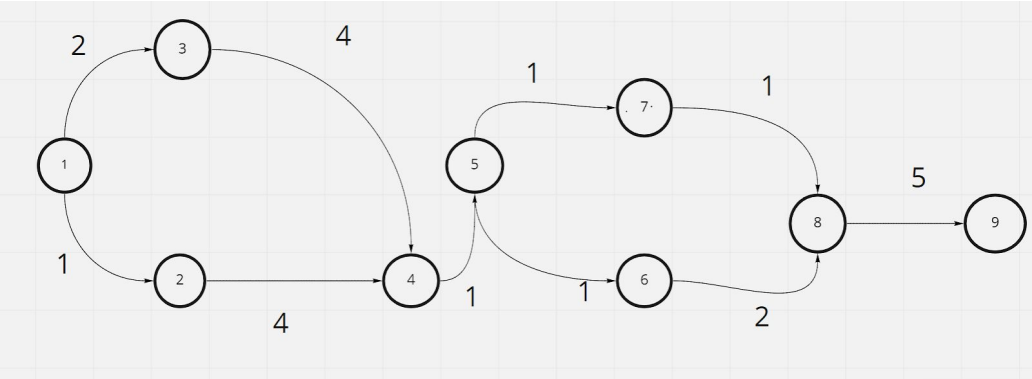
Planteamiento del problema

Se solicitó realizar un tutorial sobre un tema de la materia de Estructuras Discretas impartida por el profesor Orlando Zaldivar Zamorategui, en la Universidad Nacional Autónoma de México (UNAM). El tema a desarrollar es *Congruencias*, el cual es el apartado 3 perteneciente al tema 2, el cual se denomina “Conjuntos, relaciones y pruebas matemáticas”, por tanto, nos referiremos al tema como “el tema 2.3”.

Dicho tutorial debe ser presentado en formato web, es decir, se debe realizar una página web relacionada con el tema 2.3 de la asignatura, el cual debe contener todo lo necesario para lograr el objetivo de aprendizaje. Dicho contenido consta de un temario, ejemplos resueltos por partes, video, cuestionario y bibliografía consultada.

Planeación y metodología

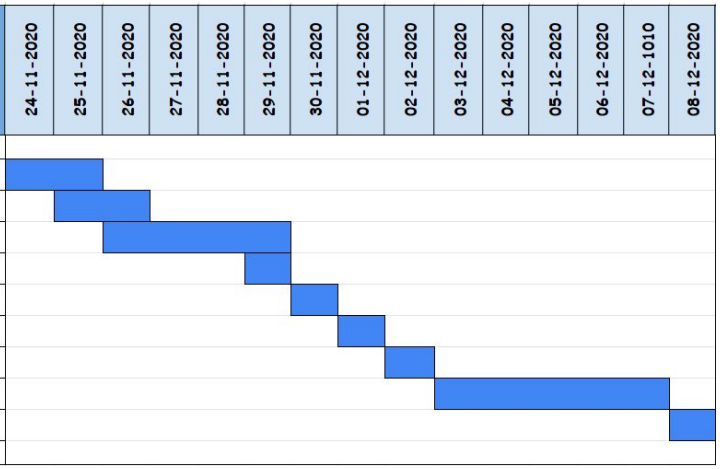
1. **Diagrama de Pert:**



Ruta crítica: 1,3,4,5,7,8,9. Lo que equivale a 15 días (dos semanas).

2. **Diagrama de Gantt:**

Actividad	*Inicio*	*Fin*
Documento de proyecto	24-11-2020	25-11-2020
Redacción de la parte teórica	25-11-2020	26-11-2020
Busqueda de información	26-11-2020	29-11-2020
Redacción de información	29-11-2020	29-11-2020
Creación de video	30-11-2020	30-11-2020
Redacción de ejemplos	01-12-2020	01-12-2020
Cuestionario	02-12-2020	02-12-2020
Desarrollo de código	03-12-2020	07-12-2020
Entrega del proyecto	08-12-2020	08-12-2020



Como se puede observar en los diagramas, la metodología a seguir consiste en la elaboración de un documento formal que incluirá el desarrollo del proyecto, además de otro documento el cual contendrá la información recabada y sintetizada sobre el tema 2.3 de la asignatura, así como ejemplos resueltos y un cuestionario. El siguiente paso será crear el videotutorial correspondiente donde se hablará sobre las aplicaciones del tema.

Una vez logrado esto, se procederá a implementar el proyecto en la página web, teniendo como principal herramienta Visual Studio Code, en donde se escribirá el código fuente necesario en lenguaje de programación HTML y CSS para la parte visual (IGU) y Javascript. En la página se podrán observar los ejemplos, un cuestionario, un videotutorial y la parte teórica del tema.

Secciones del tutorial

El tutorial constará de las siguientes secciones:

- **Página principal:** Breve introducción al tema a tratar.
- **Conceptos:** Toda la teoría necesaria para la comprensión del tema en cuestión.
- **Videotutorial:** Aquí se expondrán algunas de las aplicaciones sobre las congruencias y las funciones de dispersión.
- **Ejemplos resueltos:** Algunos ejemplos prácticos para abordar la resolución de problemas los cuales sirvan de guía para la realización del cuestionario.
- **Cuestionario:** Se trata de un cuestionario con 50 preguntas, de las cuales se elegirán 10 al azar mediante código escrito en Javascript.
- **Bibliografía:** Libros consultados para la creación del tutorial.

Recopilación de la información

2.3. Congruencias

2.3.1. Conceptos

¿Qué es una congruencia?

La RAE define congruencia como una convivencia, coherencia, o relación lógica. Es una característica que se comprende a partir de un vínculo entre dos o más elementos.

En matemáticas discretas, una congruencia puede ser definida como una expresión algebraica que manifiesta la igualdad de los restos de las divisiones de dos números congruentes por su módulo, y suele representarse con tres rayas horizontales (≡).

Una congruencia también es llamada "congruencia módulo", cuya definición es la siguiente:

$Sea\ m \in N\ \&\ a, b \in Z$:

a y b son "congruentes módulo m" si m divide a "a-b". La notación utilizada para expresar lo anterior de forma matemática es la siguiente:

$a \equiv b\ (mod\ m) \Leftrightarrow m \mid (a - b) \in Z$, o lo que es lo mismo, a-b es múltiplo de m: a-b= km, $k \in Z$

Para el estudio de las congruencias debemos conocer sus propiedades, las cuales se enlistan a continuación:

1) $a \equiv b\ (mod\ m)$ *si y sólo si a y b dejan el mismo residuo cuando son divididos entre m*. Es llamada propiedad reflexiva.
2) $a \equiv a(mod\ m),\ pues\ a - a = 0,\ 0\ es\ múltiplo\ de\ m,\ para\ todo\ m \in N$
3) $Si\ a \equiv b(mod\ m)\ y\ c \equiv d(mod\ m),\ entonces\ a + c \equiv b + d(mod\ m)$ $y\ ac \equiv bd(mod\ m)$
4) $Si\ a \equiv b(mod\ m),\ entonces\ b \equiv a(mod\ m)$. Es llamada propiedad simétrica.
5) $Si\ a \equiv b(mod\ m)\ y\ b \equiv c(mod\ m),\ entonces\ a \equiv c(mod\ m)$. Es llamada propiedad transitiva.

Congruencia lineal

Una congruencia lineal es una ecuación, de la forma $ax \equiv b(mod\ m)$

Para resolver congruencias lineales debemos que buscar que la "x" quede "sola", es decir, jugar con las congruencias para obtener una expresión con la forma $x \equiv b(\text{mod } m)$.

Como se puede ver, existen infinidad de soluciones para una congruencia lineal, aunque también puede darse el caso de que no exista solución.

2.3.2. Equivalencias de relaciones

¿Qué es una relación?

La noción de relación entre dos conjuntos de objetos es una noción muy intuitiva. Una definición no formal es la siguiente:

Si A es el conjunto de todos los hombres del mundo y B el conjunto de todas las mujeres del mundo, podemos definir una relación P (padre), la cual puede ser definida entre nuestros conjunto A y B:

Sea $x \in A$ & $y \in B$, podemos decir que x está relacionada a y por la relación P si x es el padre de y (xPy).

Como se puede observar, el orden importa aquí, pues no podemos decir que yPx, pues una mujer no puede ser el padre de un hombre.

Sin embargo, podemos establecer otras relaciones entre $x \in A$ & $y \in B$, como podría ser E(esposa), tal que *y sea la esposa de x, cuya representación sería* : yEx.

Esto puede resultar un poco ambiguo, pues esto no se cumple con todos y cada uno de los elementos de A y B; puede resultar imposible dar pruebas precisas de las propiedades que satisface una relación si tenemos una descripción verbal como la anterior.
Por lo tanto, para resolver este problema, solo necesitamos conocer precisamente cuáles elementos de A se relacionan con los de B.

Supongamos el conjunto A=B={1,2,3,4} y una relación R de A a B.
Sabemos que 1R2, 1R3, 1R4, 2R3, 3R4 y 3R4.

¿Puedes deducir qué relación tienen estos números?

Es fácil ver que la relación R corresponde a la relación "<", "menor que":

1R2, entonces 1<2
1R3, entonces 1<3
1R4, entonces 1<4
2R3, entonces 2<3
2R4, entonces 2<4
3R4, entonces 3<4

De donde podemos obtener la expresión R={(1,2),(1,3),(1,4),(2,3),(2,4),(2,4)}, donde la relación R está completamente especificada para ese conjunto de pares ordenados.

R es un subconjunto del producto cartesiano AxB, cuyo dominio está dado por:
$\{ x \in A \mid (x,y) \in R \, para \, alguna \, y \in B \}$ y el rango:
$\{ y \in A \mid (x,y) \in R \, para \, alguna \, x \in A \}$

Propiedades importantes

- **Simetría**

Una relación R sobre un conjunto A es simétrica si:
$\forall x,y \in A \; \& \; (x,y) \in R, \; entonces \; (y,x) \in R$

- **Reflexividad**

Una relación R sobre un conjunto A es reflexiva si:
$(x,x) \in R, \; \forall x \in A$

- **Transitividad**

Una relación R sobre un conjunto A es transitiva si:
$\forall x,y,z \in A, \; si \; (x,y) \in R, \; entonces \; (x,z) \in R$

Relaciones inversas

Denotamos a la relación inversa como R^{-1}.
Sea R una relación de A a B, R^{-1} es la relación de B a A. Los pares ordenados de R^{-1} son los pares ordenados de R invertidos.

Relaciones equivalentes

Una relación equivalente debe cumplir con las tres propiedades anteriores. Una relación que es reflexiva, simétrica y transitiva en un conjunto X se llama relación de equivalencia sobre X.

2.3.3. Funciones de dispersión

También llamadas hashing, son técnicas usadas principalmente en la rama de la computación, sobre todo en las estructuras de datos, para almacenar datos y poder recuperarlos de una manera eficiente. Es una especie de convención de almacenamiento de datos la cual consiste en relacionar un número entero a un conjunto de datos.
Existen diversas funciones de dispersión, las cuales se enlistan a continuación:

- Función Hash por módulo

Como su nombre lo indica, la función hash por módulo consiste en tomar el residuo de la división del dato a almacenar entre el número de componentes del arreglo donde se están almacenando los datos. H(K)=(K mod N)+1, se le suma 1 al módulo con el objetivo de obtener un valor entre 1 y N.

- Función Hash cuadrado

Consiste en elevar al cuadrado el dato a almacenar y tomar los dígitos centrales como dirección. La función Hash cuadrada queda definida por la siguiente fórmula: H(K)= dígitos centrales de (K^2)+1.

- Función Hash por plegamiento

Consiste en dividir la clave del dato en partes, tomando igual número de dígitos (puede ser que la última parte tenga menos). Una vez hecho esto, las partes se suman o multiplican para usar los dos dígitos menos significativos y así obtener el resultado. La función Hash por plegamiento queda definida por la siguiente fórmula.
H(K)= dig_men_sig(d1...dn)+1

- Función Hash por truncamiento

Consiste en tomar algunos dígitos de la clave del dato y formar la dirección de almacenamiento. Es un método muy sencillo pero no ofrece una uniformidad tan favorable para evitar muchas colisiones.

Elaboración de la escaleta (guión)

1. Bienvenida al video.
2. Explicación sobre las congruencias.
3. Aplicaciones de las congruencias.
4. Ejemplos sobre calendarios y criptografía.
5. Funciones de dispersión.
6. Explicación sobre los usos de las funciones de dispersión.