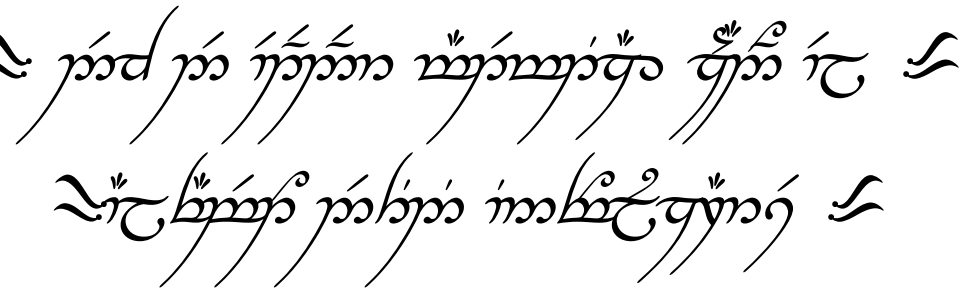
Escuela Técnica Superior de Ingeniería Informática

Asignatura:
Introducción a las Matemáticas Discretas

Autor:
Fernando José Mateos Gómez

Ultima Modificacion: **21 de septiembre de 2021**



Indice

1. Tema 1: Aritmética Entera

1.1. Introducción

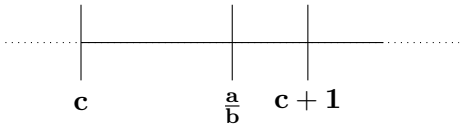
En este tema consideraremos que trabajamos con los conjuntos de los $\mathbb{N}$, $\mathbb{Z}^+$, $\mathbb{Z}^-$ y tomaremos el orden de las operaciones en el orden de prioridad (Potencias $\Rightarrow$) [Multiplicar — División] $\Rightarrow$ [Suma — Resta]).

1.2. División Euclidea

Tomamos dos numeros cualesquiera $\mathbf{a}$, $\mathbf{b} \in \mathbf{Z}$, decimos que hay un $\mathbf{c}$ y un $\mathbf{r}$ que cumplen:

$$a = bc + r \qquad \frac{a}{b} = c + \frac{r}{b} \qquad 0 \leq r < b$$

Podemos ver que $\mathbf{c}$ es el mayor entero tal que es menor o igual que $\frac{\mathbf{a}}{\mathbf{b}}$.
Si lo ponemos en una recta, podemos ver lo siguiente:



Propiedades

1. Si $\mathbf{r = 0} \Leftrightarrow \mathbf{a = bc}$
2. $a|b,\ \ b|c \begin{cases} \exists\, \mathbf{p} \in \mathbb{Z}\ ;\ \mathbf{b = ap} \\ \exists\, \mathbf{q} \in \mathbb{Z}\ ;\ \mathbf{c = bq} \end{cases}$
   Si el producto es conmutativo $\mathbf{c} = (\mathbf{ap})\mathbf{q} = \mathbf{a}(\mathbf{pq})$, por lo que $\mathbf{a|c} \Rightarrow \mathbf{a|b},\ \ \mathbf{b|c}$
3. $\mathbf{a|b},\ \ \mathbf{c|d} \begin{cases} \exists\, \mathbf{p} \in \mathbb{Z}\ ;\ \mathbf{b = ap} \\ mathbf{f} \exists\, q \in \mathbb{Z}\ ;\ d = cq \end{cases}$
   Si el producto es conmutativo $\mathbf{bd} = (\mathbf{ap})(\mathbf{cq}) = (\mathbf{ac})(\mathbf{pq}))$, por lo que $\mathbf{a|b},\ \ \mathbf{c|d} \Rightarrow \frac{\mathbf{ac}}{\mathbf{bd}}$
4. Si $\mathbf{m \neq 0}$ entonces:
   $\mathbf{a|b} \begin{cases} \exists\, \mathbf{k} \in \mathbb{Z}\ ;\ \mathbf{b = ak} \end{cases}$
   Esto implica que $\mathbf{k} = \frac{\mathbf{mb}}{\mathbf{ma}} = \frac{\mathbf{b}}{\mathbf{a}}$
5. No hay divisiones entre cero$\mathbf{a \neq 0}\ \Rightarrow\ \mathbf{ab = 0}\ \Rightarrow\ \mathbf{b = 0}$
6. Propiedad cancelativa: $\mathbf{a \neq 0}\ \Rightarrow\ \mathbf{ab = ac}\ \Rightarrow\ \mathbf{b = c}$

1.2.1. Resto

Aquí veremos el uso de un operador que nos servirá en temas posteriores, el resto, denominado con **mod** y calcula el resto, valga la redundancia, de la división de dos numeros cualesquiera, siempre que sean enteros.

$$r = \boxed{a \mod b} = a - bc$$

1.2.2. Función Suelo

Es una función que abarca el conjunto de los números reales, tal que dado un número $\mathbf{x}$ aproximará al entero más cercano por debajo.
Se representa así:

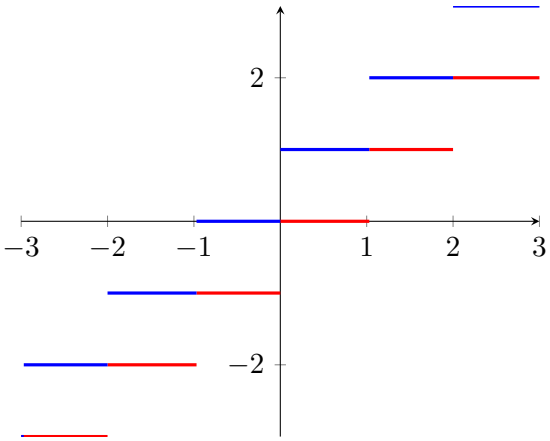
$$\boxed{f(x) = \lfloor x \rfloor}$$

1.2.3. Función Techo

Al contrario que la función suelo, esta función aproximará al entero más cercano por arriba, y se representa así:

$$\boxed{f(x) = \lceil x \rceil}$$

Aquí tenemos una representación gráfica de ambas funciones, siendo la azul la función techo y la roja la suelo.



Propiedades

- $\lfloor -\mathbf{x} \rfloor = -\lceil \mathbf{x} \rceil$ es lo mismo que $\lceil -\mathbf{x} \rceil = -\lfloor \mathbf{x} \rfloor$
- $\lceil \mathbf{x} + \mathbf{n} \rceil = \lceil \mathbf{x} \rceil + \mathbf{n}$ Siendo $\mathbf{n}$ un entero, es lo mismo que $\lfloor \mathbf{x} + \mathbf{n} \rfloor = \lfloor \mathbf{x} \rfloor + \mathbf{n}$

1.2.4. Función Euclidea Modificada

Con todo esto, podemos definir la función Euclidea de una forma un tanto más rigurosa:

$$\boxed{a = \lfloor a|b \rfloor + a \mod b}$$

1.3. Tamaño que puede abarcar un número

Dado un número $\mathbf{n}$, entero y en base m, $\mathbf{B_{m)}}$, decimos que puede dividirse entre la base $\mathbf{B}$ tantas veces como cifras tenga.
Si por ejemplo $\mathbf{n} \in \mathbf{B_{2)}}$:

$$n = \sum_{i=0}^{N} \kappa B^i$$

$$\frac{n}{2} = \sum_{i=0}^{N-1} \kappa B^i$$

Siendo $\mathbf{N}$ la posición y κ el valor que hay en la posición indicada del número $\mathbf{n}$.
Podemos ver que por cada vez que dividimos, el elemento en la posición menos significativa desaparece, por lo que:

$$k \leq \log_2 n < k + 1$$

$$k = \lfloor \log_2 n \rfloor + 1$$

Por lo que $\mathbf{k}$ es el numero de cifras que posee ese número en base 2.
De forma general para cualquier base sería:

$$\boxed{k = \lfloor \log_m n \rfloor + 1}$$

1.4. M.C.D. y el Algoritmo de Euclides

Sabiendo como se define la función Euclidea, podemos definir un algoritmo por el cual podremos calcular el **máximo común divisor**, **M.C.D.**, así:

$$a = bc + r$$

$$\boxed{\text{mcd}(a, b) = \text{mcd}(b, r)}$$

Hasta que $\mathbf{r = 0}$, que será entonces la ultima **b** el **M.C.D.**.

1.4.1. Identidad de Bezout

Mediante esta identidad podemos calcular el **M.C.D.** como combinación lineal entre el numerador y el denominador:

$$\boxed{\text{mcd}(a, b) = a\alpha + b\beta}$$

5328=66*80 + 48	$r = a - 80b$
66=48 + 18	$r_1 = b - r$
48=18*2 + 12	$r_2 = r - 2r_1$
18 = 12 + 6	$r_3 = r_1 - r_2$
12 = 6*2	$r_2 = 2r_3$

$r_3 = r_1 - r_2 = 3r_1 - r = 3b - 4r = -4(a - 80b) + 3b = \boxed{-4a + 323b} \Rightarrow \alpha = -4 \quad \beta = 323$

1.5. Algoritmos y análisis

Hay 3 factores a tener en cuenta a la hora de analizar un algoritmo:

1. Factibilidad (si realiza todas las instrucciones)
2. Si es finito (Tiene un inicio y un final)
3. Eficiencia (Que se suele pone como $\mathcal{O}(\mathbf{f(n)})$

No vamos a profundizar mucho, sin embargo, cabe destacar que los algoritmos cuya $\mathbf{f(n)}$ sea $\mathbf{n!}$ son los más lentos, y los $\mathbf{\log_2 n}$ los más rapidos.

1.5.1. Invariantes

No profundizaremos mucho, pero se explicará lo básico.
Los Invariantes son expresiones **constantes** que analizan el resultado y el comportamiento del algoritmo, indicando el numero de operaciones que hace y el valor que va a devolver siempre.
Si los usaramos a bajo nivel, en programación, veríamos que en las operaciones de bit a bit, no se realizan divisiones o multiplicaciones, y solo usa desplazamientos de bits.

1.6. Ecuaciones Diofanticas

Son aquellas ecuaciones con dos incógnitas cuya solución solo se encuentra dentro del cuerpo de los enteros $\mathbb{Z}$:

$$\boxed{a\text{X} + b\text{Y} = c}$$

Solo tienen soluciones cuando **c** es divisible entre el **M.C.D.** de **a** y **b**, si no lo fuera, no habrían infinitas soluciones, y buscamos una solución única o en un intervalo de enteros.

$$\boxed{\text{mcd}(a,b) = d}$$

$$\boxed{\frac{a}{d}\text{X} + \frac{b}{d}\text{Y} = \frac{c}{d}}$$

Como hemos podido calcular el **M.C.D**, ahora podemos extraer una Identidad de Bezout, lo que nos dará una solución del sistema, siendo cada coeficiente de Bezout por el termino $\frac{\mathbf{c}}{\mathbf{d}}$, lo que satisfacerá el sistema.
Sin embargo, esta puede no ser la solución que buscamos, pueden haber ciertas restricciones, asi que para esto tendremos que buscar un valor para X y Y que abarque todo el rango de valores posibles.
Para esto debemos de sumarle a la solución particular el coeficiente de la incógnita opuesta, por una variable que llamaremos λ, que en una ecuacion tendrá signo positivo y en la otra .negativo:

$$\boxed{\begin{cases} \text{X} = \alpha\frac{c}{d} \pm \frac{b}{d}\lambda \\ \text{Y} = \beta\frac{c}{d} \mp \frac{a}{d}\lambda \end{cases}}$$

Siendo α el coeficiente de la incógnita X para Bezout y β el coeficiente de Y.
Tras esto podremos facilmente aplicar las restricciones que se nos especifiquen.

1.7. Primos

Definimos un número primo, como todo $\mathbb{N} > \mathbf{1}$, y se expresan con el conjunto $\mathbb{P}$.
Propiedades
Partiendo de $\mathbf{p} \in \mathbb{P}$ y $\exists a \in \mathbb{Z}$ tenemos:

- **p** y **a** son coprimos, cuando $\text{mcd}(p,a) = 1$ que es lo mismo que decir que no son divisibles entre si.
- Si $\mathbf{p} > \mathbf{3}$, entonces **p** se puede expresar como $\mathbf{6}\kappa \pm \mathbf{1}$. Podemos demostrar esto por la división Euclídea, de forma que probamos los valores que puede adoptar 1 del 0 $\rightarrow$ 5.
- **p** es primo y divide a un producto, si **p** divide a alguno de los factores del producto.
- Dado un **p** y un conjunto de valores que denominaremos A, diremos que **p** divide almenos un elemento del conjunto, aplicando la propiedad anterior.

1.7.1. Factorización

Todos los numeros, mayores que 1, son divisibles por un primo tal que se encontrará en el intervalo $[1, \ \sqrt{[n]}]$, siendo **n** el número a factorizar.

1.8. Demostraciones

En este apartado veremos dos metodos para realizar demostraciones, son muy comunes.

1.8.1. Metodo de Inducción

1. Partimos de un conjunto **z** que cumplen una condición.
2. Buscamos el caso base del que partir, es decir, comprobamos que la condición sirve para el primer valor posible.
3. Suponemos que existe un **k** que cumple la condición inicial.
4. Ahora a partir de un $\mathbf{k+1}$ tenemos que llegar a la misma expresión del inicio, la condición que debemos demostrar.

Con un ejemplo será más claro:

$$\sum_{n=1}^{p}(2n-1) = n^2$$

Dada una expresión como esta,y sabiendo que es valida para cualquier número superior cero comprobamos que se cumple para $p = 1$

$$\sum_{n=1}^{1}(2n-1) = n^2 \;\Rightarrow\; 2-1 = 1^2 \;\Rightarrow\; 1 = 1$$

Vemos que se cumple, ahora consideraremos la expresión valida hasta un número k.

$$\sum_{n=1}^{k}(2n-1) = k^2$$

$$1 + 3 + ... + (2k-1) = k^2$$

Ahora intentaremos demostrar para $k+1$:

$$\sum_{n=1}^{k+1}(2n-1) = (k+1)^2$$

$$1 + 3 + ... + (2k-1) + (2k+1) = (k+1)^2$$

Vemos que en el primer miembro, podemos utilizar la hipotesis para sustituir todos los elementos hasta $2k-1$:

$$\boxed{(2k-1) + (2k+1) = k^2 + 2k + 1 = (k+1)^2} \quad \text{QDE}$$

1.8.2. Reducción al Absurdo

Nos basamos en que dada una proposición, la negamos, y buscamos encontrar una contradicción. Veamos este ejemplo.
Demostremos que dado un producto de enteros ab es par, entonces a o b es par:

$$2|ab \Rightarrow 2|b \vee 2|a$$

Montamos nuestra proposición, vemos que el primer miembro es la **hipotesis**, y el resto es la **tesis** que negaremos, que debe de cumplirse.
Si la negamos, estaremos diciendo que b y a son impares.
Conociendo como se define un numero impar:

$$\boxed{b = 2k + 1}$$

$$\boxed{a = 2t + 1}$$

Siendo k y t dos numeros cualesquiera positivos y enteros, decimos que el producto de a y b es:

$$\boxed{ab = (2k + 1)(2t + 1) = 4kt + 2k + 2t + 1}$$

Vemos que según la tesis, el producto de ab es un número impar, lo que es imposible, ya que debe de dividir a un número par.
Por lo que queda demostrado que es cierto.

1.9. Números Famosos

Aquí veremos algunas series de números que nos serviran para temas futuros.

1.9.1. Fibonacci

Para obtener un número de Fibonnaci hay que sumar los dos números posteriores al que buscamos, hasta llegar al caso inicial.

$$\boxed{F_n = F_{n-1} + F_{n-2} \quad [F_0 = 0\,, F_1 = 1]}$$

Es una expresión recursiva, y podemos expresarla como una ecuación:

$$\boxed{F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1 + \sqrt{5}}{2} \right)^n - \left(\frac{1 - \sqrt{5}}{2} \right)^n \right)}$$

1.9.2. Mersenne

Son aquellos números que representados en $B_{2)}$ son solo unos:

$$\boxed{M_n = 2^n - 1}$$

1.9.3. Fermat

$$\boxed{Fe_n = 2^{2^n} + 1 \quad n \geq 0}$$

Tiene la característica que los números de $Fe_0 \rightarrow Fe_4$ son primos, y los únicos de esta serie.

1.9.4. Euclides

$$\boxed{e_n = 1 + \prod_{k=1}^{n} e_k}$$

Cada elemento de la serie se obtiene de multiplicar todos los anteriores y sumarle 1. Partiendo de que el primer elemento de la serie es $e_1 = 2$

2. Tema 2: Aritmética Modular

2.1. Congruencia

Considerando un número **n**, que diremos que se comporta como 0 en un sistema $\mathbb{Z}_n$. De esta forma definimos una función tal que:

$$y - x = nk$$

El primer miembro es congruente con cualquier múltiplo k de n
Esto se representa como:

$$\boxed{a \equiv b(\text{mod } n)}$$

De esta forma, el rango posibles de valores, son $\mathbf{n} = 0, ..., n-1$.
Propiedades

- Equivalencia. Teniendo dos congruencias de este tipo:

$$\begin{cases} \mathbf{a} \equiv \mathbf{b}(\mathbf{mod\ n}) \\ \mathbf{b} \equiv \mathbf{c}(\mathbf{mod\ n}) \end{cases}$$

  Entonces:

$$\boxed{\mathbf{a} \equiv \mathbf{c}(\mathbf{mod\ n})}$$

- No existen divisiones por cero, por lo que $ab \not\Rightarrow a = 0 \quad$ ó $\quad b = 0$
- Si existe un $\lambda \in \mathbb{Z}$ entonces:

$$\begin{cases} \mathbf{a} \equiv \mathbf{b}(\mathbf{mod\ } \lambda\mathbf{n}) \\ \lambda\mathbf{a} \equiv \lambda\mathbf{b}(\mathbf{mod\ } \lambda\mathbf{n}) \end{cases}$$

  Será siempre igual a$a \equiv b(\text{mod } n)$, solo si $\lambda \neq 0$.

- Sumar, restar o multiplicar dos congruencias del mismo modulo, será lo mismo que una congruencia, con los terminos a y b iguales a sumar, resta o multiplicar en ambas congruencias.

2.2. Inversas

Existe un modulo inverso cuando existe un único resultado a la ecuación $\boxed{\mathbf{aX = 1}}$ con $\mathbf{a} \in \mathbb{Z}_\mathbf{n}$

2.2.1. Calculo de Inversas

Es un proceso muy simple.
Planteamos una ecuación de congruencia:

$$a\text{X} = 1(\text{mod } n)$$

Si la convertimos a una ecuación diofantica, podemos calcular el coeficiente de la identidad de Bezout correspondiente al termino X.

$$a\text{X} - n\text{Y} = 1$$

Tras resolverlo, obtendremos un α que al calcular su resto respecto a n, obtendremos el inverso $\mathbf{a^{-}1}$.

Podemos expresar entonces el calculo del inverso de la siguiente forma:

$$\boxed{1 \equiv (\alpha(\text{mod } n))(\text{mod } n)}$$

Si quisieramos hacerlo de una forma general entonces a y b deben de ser coprimos en $a \equiv b(\text{mod } n)$, de forma que al obtener α lo multiplicamos por b:

$$\boxed{1 \equiv ((\alpha b)(\text{mod } n))(\text{mod } n)}$$

2.3. Ecuaciones en Congruencias

Partiendo de una congruencia como la vista al principio del tema:

$$\boxed{a \equiv b(\text{mod } n)}$$

Toda ecuación en congruencia se puede resolver como una ecuación diofantica.

2.3.1. Sistemas de Ecuaciones en Congruencias, Teorema Chino del Resto

$$\begin{cases} a_1 X \equiv b_1(\text{mod } n_1) \\ \vdots \\ \vdots \\ a_k X \equiv b_k(\text{mod } n_k) \end{cases}$$

Dado un sistema como el planteado arriba, intentaremos crear una sola ecuación en congruencia que abarque a todas las que conformen el sistema.
Solo se podrá resolver el sistema cuando todas las $\mathbf{n_k}$ sean coprimos entre si.
Veamos un ejemplo:

$$\begin{cases} X \equiv 1(\text{mod } 4) \\ X \equiv 2(\text{mod } 3) \\ X \equiv 3(\text{mod } 5) \end{cases}$$

Dado este sistema deberemos de calcular 4 terminos por cada ecuación del sistema:

$$\boxed{b_k = \frac{b_k}{\text{mcd}(a_k, n_k)}}$$

$$\boxed{c_k = \frac{\prod}{n_k}}$$

$$\boxed{d_k = c_k^{-1}(\text{mod } n_k) \Rightarrow c_k X \equiv 1(\text{mod } n_k)}$$

Y el rango de la congruencia:

$$\boxed{\mathbb{Z}_n \Rightarrow n = \prod_{k=1} n_k}$$

De esta forma ya tendremos todos los valores que nos interesan, por lo que podremos montar nuestro sistema congruente.
Denominaremos **X** a la solución general, ρ a la específica y **N** el rango de congruencia.

$$\boxed{X = X = \sum_{k=1} b_k d_k c_k}$$

$$\boxed{X \equiv \rho(\mathrm{mod}N)}$$

$$\boxed{X = \rho + N\lambda}$$

$$\boxed{\rho = X(\mathrm{mod}N) + N\lambda}$$

Como podemos ver la solución del sistema, que nos interesa se puede expresar como una ecuación como esta, y modificando el parametro λ podemos calcular todas las posibilidades. En el ejemplo, la solución del sistema es la siguiente:

	1	2	3
n_k	4	3	5
b_k	1	2	3
c_k	15	20	12
d_k	3	2	3

$$N = 3 * 4 * 5 = 60$$

$$X = 15 * 3 + 20 * 2 * 2 + 12 * 3 * 3 = 233$$

$$\boxed{\rho = 233(\mathrm{mod}60) + 60\lambda = 53 + 60\lambda}$$

Propiedades

Aqui veremos 3 propiedades que nos ayudarán a simplificar e indicar si el sistema tiene solución:

- Compatibilidad: El mcd entre 2 n_k distintos debe ser divisible entre la diferencia entre sus bases, es decir:

$$\mathrm{mcd}(n_i,\ n_j)\ \mid\ (b_i - b_j)$$

$$\boxed{(b_i - b_j) \equiv 0\ \ (\mathrm{mod}\ \ \mathrm{mcd}(n_i, n_j))}$$

- Reducción, si hay alguna ecuación cuya **n** sea igual a otra, entonces podemos eliminar cualquiera de ellas.
- Expansión, cada ecuación la podemos dividir en sus factores primos, solo modificando el termino del modulo, n.

2.4. Función de Euler

Dado una función $\phi(\mathbf{N})$, que nos indicará el numero de elementos en base N que tienen inverso, podemos calcular los valores en base a las siguientes indicaciones:

- Si $N \in \mathbb{P}$, es decir, N es primo: $\boxed{\phi(\mathbf{N}) = \mathbf{N - 1}}$
- Si N es primo y está elevado a un número m: $\boxed{\phi(\mathbf{N^m}) = \mathbf{N^{m-1}(N - 1)}}$
- Si N lo podemos descomponer en factores primos, entonces $\boxed{\phi(\mathbf{N}) = \phi(\mathbf{A}) \quad \phi(\mathbf{B})}$

De esta forma nos quedarán dos expresiones para calcular $\phi(N)$:

$$\phi(N) = n\prod_{n=t}^{k}(1 - p_n^{-1})$$

$$\boxed{\phi(N) = \prod_{n=t}^{k}(p_n^{m_n - 1})(p_n - 1)}$$

Siendo p_n los factores primos del número en cuestión y m_n el numero de veces que aparece ese factor primo en cuestión.

2.5. Teoremas

Aquí veremos dos teoremas que nos ayudarán a extraer propiedades y conclusiones para temas posteriores.

2.5.1. Teorema de Fermat

Sabemos por definición que dado un conjunto $\mathbb{Z}_n$, no pueden haber elementos repetidos y que existen $n-1$ elementos. De esta forma enunciamos:
Si **p** es primo, $\mathbf{x} > \mathbf{0}$ y $\mathbf{p} \nmid \mathbf{x}$ entonces:

$$\boxed{x^{p-1} \equiv 1 (\text{mod } p)}$$

Si solo ocurriese que **p** es primo y $\mathbf{x} > \mathbf{0}$:

$$\boxed{x^{p} \equiv x (\text{mod } p)}$$

2.5.2. Teorema de Euler

Es una ramificación del Teorema de Fermat, y dice que si x y n son coprimos entonces:

$$\boxed{x^{\phi(n)} \equiv 1 (\text{mod } n)}$$

2.5.3. Potencias de Fermat

Esta es una forma rápida de convertir una potencia a otra, en una congruencia específica:

$$x^k \text{ mod } p = x^{(p-1)\left\lfloor \frac{k}{p-1} \right\rfloor + k \text{ mod } (p-1)} = \boxed{x^{k \text{ mod } (p-1)} \text{mod } p}$$

2.6. Metodo MC, potencias rapidas

Si K es un entero bastante pequeño en $X (\text{mod } n)$ entonces podemos calcular el resultado transformando X a un número binario.
De forma que Al transformar el numero a binario, elevamos al cuadrado entre cada cifra del numero, y los unos, son multiplicaciones por 2, y eliminamos los ceros, es decir:

$$\boxed{70_{10)} = 1000110_{2)} = \text{MCCCCMCMC} = ((((((((((70 * 2)^2)^2)^2)^2) * 2)^2) * 2)^2) * 2)}$$

Tened en cuenta que por cada operación, hay que realizar los modulos.

2.7. Criptografía y RSA

El algoritmo RSA aprovecha los numeros primos y la Función de Euler para calcular claves numéricas extremadamente grandes que facilitan la encriptación.
Si partimos de dos numeros p y q que son primos podemos calcular lo siguiente:

$$\boxed{n = pq}$$

Siendo n el peso de mayor agrupación posible.

$$\boxed{\phi(n) = \phi(p)\phi(q) = (p-1)(q-1)}$$

Esta es la clave publica:

$$\boxed{e = min_{\text{Primo en } \phi(n)}}$$

Esta es la clave privada:

$$\boxed{d = e^{-1} (\text{mod } \phi(n))}$$

Para cifrar y descifrar solo tendremos que hacer lo siguiente:

$$\boxed{\text{Cifrado} \Rightarrow Y \equiv X^e (\text{mod } n)}$$

$$\boxed{\text{Descrifrado} \Rightarrow X \equiv Y^d (\text{mod } n)}$$

3. Tema 3: Combinatoria

3.1. Conjunto

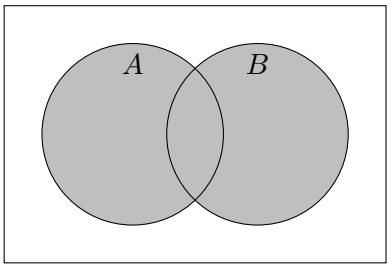
Un conjunto, es una colección definida de objetos que comparten unas propiedades. Pueden ser finitos o infinitos.

$$A = \{a_1, a_2, ...a_k\}$$
$$B = \{b_1, b_2, ...b_k\}$$

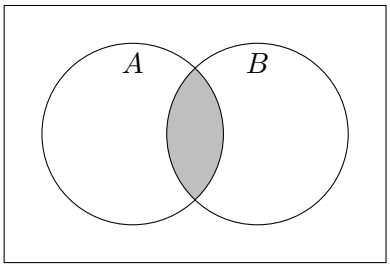
Propiedades

- $A \cap B$ corresponde a la intersección, y abarca a todos los elementos que comparten ambos conjuntos.
- $A \cup B$ corresponde a la unión, y abarca al total de elementos que contienen ambos conjuntos.
- $|A|$ corresponde al cardinal, y son el numero total de elementos que contiene el conjunto.
- $A \subseteq B$ indica que A es un subconjunto de B.
- $A \setminus B$ corresponde a los elementos en A no presentes en B. Se suele escribir como $\overline{A}$.
- $\overline{\overline{A}} = A$
- $\overline{A \cup B} = \overline{A} \cap \overline{B}$
- $\overline{A \cap B} = \overline{A} \cup \overline{B}$
- $A \cup \overline{A} = \emptyset$
- $|P(A)| = 2^{|A|}$ indica el tamaño máximo del conjunto.

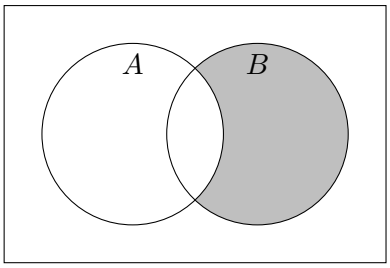
Diagramas de Venn



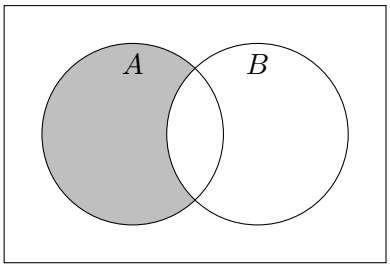
Unión: $\mathbf{A \cup B}$



Intersección: $\mathbf{A \cap B}$



Complemento de A: $\overline{\mathbf{A}} = \mathbf{B} \setminus \mathbf{A}$



Complemento de B: $\overline{\mathbf{B}} = \mathbf{A} \setminus \mathbf{B}$

3.2. Principios

Aquí veremos 4 principios que nos servirán para operar más adelante:

3.2.1. Principio de Adición

Siempre y cuando dos o más conjuntos no tengan ningún elemento en común, la cardinalidad de su intersección dará lugar a la suma de sus cardinalidades:

$$\boxed{A \cap B = \emptyset \;\; \Rightarrow \;\; |A \cap B| = |A| + |B|}$$

3.2.2. Principio de Producto / Ley del Producto

Si hay dos o más conjuntos finitos, en los que multipliques un conjunto con una cardinalidad menor o igual que el consecutivo, entonces el producto entre ambos conjuntos será el producto cartesiano:

$$\boxed{|A \times B| = |A| \times |B|}$$

3.2.3. Principio de Inclusión y Exclusión

Para obtener la cardinalidad de todos los elementos que abarcan dos o más conjuntos, su intersección, se debe de sumar la cardinalidad de todos los conjuntos a la cardinalidad de la intersección de cada 3 elementos, y restarle la intersección de cada par de conjuntos. Aquí podemos ver el caso de dos conjuntos:

$$\boxed{|A \cup B| = |A| + |B| - |A \cap B|}$$

Aquí el de 3:

$$\boxed{|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |A \cap C| + |C \cap B|) + |A \cap B \cap C|}$$

Como podemos observar, la generalización podría llegar a ser más compleja, y no la pondré.

3.2.4. Principio de Distribución / Dirichlet

Si repartimos **n** elementos entre $\mathbf{m} \geq 1$ células, entonces:

- Una célula recibirá hasta $\lceil \frac{n}{m} \rceil$ objetos.
- Una célula recibirá hasta $\lfloor \frac{n}{m} \rfloor$ objetos.

Si consideramos un α como una serie de elementos que comprenden un objeto, podemos decir:

$$n = \sum_{i=1} \alpha_i$$

Y por ende:

- Podemos decir que $\forall i \ \alpha_i < \lceil \frac{n}{m} \rceil$, y $\alpha_i \leq \lceil \frac{n}{m} \rceil - 1$ con lo que $n \leq m \left(\lceil \frac{n}{m} \rceil - 1 \right)$

3.3. Contando Pares

Considerando dos conjuntos X e Y que conforman otro conjunto S llamamos:

- $f_Y(S)$ al número de elementos con la coordenada en las ordenadas.
- $f_X(S)$ al número de elementos con la coordenada en las abcisas.
- $\sum_{y \in Y} f_y(S) = \sum_{x \in X} f_x(S)$

3.4. Combinatoria, casos

3.4.1. Variaciones

Abarca a las distintas formas de agrupar un conjunto, donde el orden importa.

3.4.2. Permutaciones / Biyecciones

Es un caso de las variaciones donde el cada grupo abarcamos todos los elementos, donde el orden importa.

3.4.3. Combinaciones

Agrupación de elementos donde el orden no importa
En general las podemos agrupar en la siguiente tabla:

$$\text{Abarca todos los Elementos} \begin{cases} \text{Si e importa el Orden} \begin{cases} \text{Si} \begin{cases} \text{Se repiten elementos} \begin{cases} \text{Si, Permutaciones} = \mathrm{PR}_m^{t_i} = \frac{m!}{\prod_{i=1} t_i} \\ \text{No, Permutaciones} = \mathrm{P}_m = m! \end{cases} \end{cases} \\ \text{No} \begin{cases} \text{No hay ninguna operación} \end{cases} \end{cases} \\ \text{No e importa el Orden} \begin{cases} \text{Si} \begin{cases} \text{Se repiten elementos} \begin{cases} \text{Si, Variaciones} = \mathrm{VR}_m^n = m^n \\ \text{No, Variaciones} = \mathrm{V}_m^n = \frac{m!}{(m-n)!} \end{cases} \end{cases} \\ \text{No} \begin{cases} \text{Se repiten elementos} \begin{cases} \text{Si, Combinaciones} = \mathrm{CR}_m^n = \binom{m+n-1}{n} \\ \text{No, Combinaciones} = \mathrm{C}_m^n = \binom{m}{n} \end{cases} \end{cases} \end{cases} \end{cases}$$

3.4.4. Emparejamientos, Desarreglos y Circulares

Son un caso particular.
Los emparejamientos, son una ramificación de las combinaciones, donde se calcula el numero de formas que se puede repartir un elemento m en un conjunto de $m \times n$.

$$\boxed{\mathrm{Cm}_m^n = \frac{(mn)!}{(m!)^n n!}}$$

Los desarreglos, son un caso particular de las variaciones donde se calcula el numero de formas que se puede repartir un elemento de formas distintas para que quede en la misma posición:

$$\boxed{\mathrm{D}_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}}$$

Las circulares, son un caso particular de las permutaciones, donde calculamos las formas en las que se puede ordenar un conjunto circular:

$$\boxed{\mathrm{PC}_n = (n-1)!}$$

3.5. Número Binómico

Denominamos al número binómico como $\binom{n}{k}$, tal que n y k son números enteros positivos, tal que equivale a $\frac{n!}{k!(n-k)!}$.
Podemos ver ciertas propiedades que nos servirán a futuro:

- $\binom{0}{0} = \binom{n}{0} = \binom{n}{n} = 1$
- $\binom{n}{k} = \binom{n}{n-k}$
- Sumar dos binómicos cuya parte baja sea el mismo número más uno es: $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$
- La suma de todos los binómicos desde 0 hasta la parte superior equivale a una potencia de dos: $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

3.5.1. Triangulo de Pascal

Fila 0: $\binom{0}{0}$
Fila 1: $\binom{1}{0}$ $\binom{1}{1}$
Fila 2: $\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$
Fila 3: $\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$
Fila 4: $\binom{4}{0}$ $\binom{4}{1}$ $\binom{4}{2}$ $\binom{4}{3}$ $\binom{4}{4}$
Fila 5: $\binom{5}{0}$ $\binom{5}{1}$ $\binom{5}{2}$ $\binom{5}{3}$ $\binom{5}{4}$ $\binom{5}{5}$

3.5.2. Binomio de Newton

Aplicando nuestros conocimientos de los números binómicos, somos capaces de escribir una expresión con la que podemos calcular una expresión del tipo $(X+Y)^n$ con X e Y reales y n un entero positivo:

$$\boxed{\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}}$$

4. Tema 4: Recursividad

4.1. Tipos de Recurrencias

Denominamos a la expresión que define una recurrencia como fórmula explícita, que generaliza el cálculo de la recurrencia y lo simplifica.

4.1.1. Lineales de Coeficientes Constantes

Se les denomina a aquellas expresiones donde existe una expresión que denominamos $f(n)$ que denominaremos como término independiente:

$$a_n = \sum_{n=1}^{t} A_n \alpha_{n-1} + f(n)$$

El grado se indica como el término A_n con mayor n.

4.1.2. Lineales Homogéneas

Es una recurrencia lineal de coeficiente constante, donde $f(n)$ vale cero.

4.1.3. Otras

No las trataremos, pero son aquellas recurrencias como el factorial o el máximo común divisor y también las recurrencias lineales no homogéneas, que no vimos en mi año.

4.2. RLHCC

4.2.1. Primer Grado

Dada la expresión general $a_n = A_0 a_{n-1}$ y conociendo el valor del caso base $a_0 = \alpha$, definimos y nos quedaría lo siguiente:

$$\boxed{a_n = A_0 a_{n-1}}$$

$$\boxed{X = \sqrt[n]{A_0} = r} \quad \boxed{\alpha = A_0 a_0}$$

$$\boxed{a_n = \frac{\alpha}{r^0} r^n}$$

4.2.2. Segundo Grado

Ahora tenemos dos coeficientes y dos valores para el caso base:

$$\boxed{a_n = A_0 a_{n-1} + B_0 a_{n-2}} \quad a_0 = \alpha \quad b_0 = \beta$$

Realizamos los pasos de la de primer grado y obtenemos la siguiente expresión:

$$\boxed{X = \frac{A_0 \pm \sqrt{A_0 + 4B_0}}{2} = r_1, r_2}$$

En caso de que $r_1 \neq r_2$ debemos de resolver una expresión como esta:

$$\boxed{a_n = C r_1^n + D r_2^n}$$

Para resolverla a_n debe de tomar los valores de α y β en función del valor de n.
En caso de que $r_1 = r_2$ debemos de resolverlo de la misma forma, pero con la siguiente expresión:

$$\boxed{a_n = (C + Dn) r^n}$$

De forma que r es igual a cualquiera de las raices.