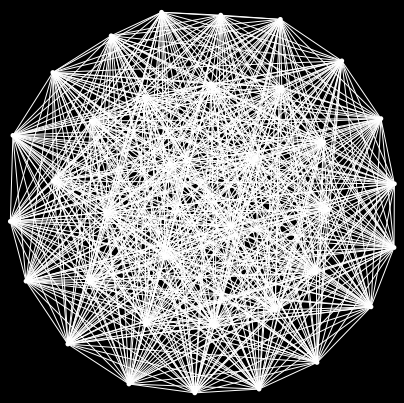
MathCon

The Mathematics Firm

Matemáticas Discretas

Apuntes de Curso



José de Jesús Angel Angel
jjaa@math.com.mx

Contenido

1
Números Enteros

Definición 1 *Los números enteros son el conjunto* $\mathbb{Z} = \{... -2, -1, 0, 1, 2, ...\}$.

Propiedades de los números enteros:

1. Los números enteros esán ordenados, es decir para todo dos números enteros a, b siempre se cumple una y solo una de las siguientes opciones:

   a) $a < b$.

   b) $a > b$.

   c) $a = b$

2. Dado dos números enteros a, b, b divide a a si existe otro número entero c tal que $b = ac$. Se escribe $b|a$. También se dice que a es factor de b, o que b es múltiplo de a. Decimos también que b es divisible por a.

3. Un número (entero diferente de 1) es primo si solo es divisible por si mismo y por 1.

4. Ejemplos de números primos son $= \{2, 3, 5, 7, 11, 13, 17, 19, ...\}$.

5. Hay una cantidad infinita de números primos.

6. Teorema Fundamental de la Aritmética: todo número entero se escribe como producto de potencias de números primos (salvo signo).

7. En los números enteros no hay inversos multiplicativos, no existe la división, sin embargo tenemos el Algoritmo de Euclides: Dados dos números enteros a, b entonces existen números enteros q, r tales que $a = qb + r$, donde $0 \leq r < b$, q es el cociente y r se llama residuo.

8. El máximo común divisor de dos números a, b es un divisor común de a y b que es máximo. Se denota $mcd(a, b)$.

9. $mcd(a, b) = mcd(b, r)$

Proceso del algoritmo de euclides.

$$\begin{aligned}
a &= bq_1 + r_1 && 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 \leq r_3 < r_2 \\
&\cdots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} && 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} &= r_{k-1} q_{k-1} && 0 \leq r_k = 0
\end{aligned}$$

Donde $mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2) = \cdots = mcd(r_{k-2},r_{k-1}) = r_{k-1}$.

1. Encontrar el MCD de 234 y 24

$$\begin{aligned}
234 &= 24 \cdot 9 + 18 \\
24 &= 18 \cdot 1 + 6 \\
18 &= 6 \cdot 3 + 0
\end{aligned}$$

$234 = 2 \cdot 3^2 \cdot 13$
$24 = 2^3 \cdot 3$

2. Encontrar el MCD de 496 y 64

$$\begin{aligned}
496 &= 64 \cdot 7 + 48 \\
64 &= 48 \cdot 1 + 16 \\
48 &= 16 \cdot 3 + 0
\end{aligned}$$

$496 = 2^4 \cdot 31$
$64 = 2^6$

3. Encontrar el MCD de 3564 y 1512

$$\begin{aligned}
3564 &= 1512 \cdot 2 + 540 \\
1512 &= 540 \cdot 2 + 432 \\
540 &= 432 \cdot 1 + 108 \\
432 &= 108 \cdot 4 + 0
\end{aligned}$$

$3564 = 2^2 \cdot 3^4 \cdot 11$
$1512 = 2^3 \cdot 3^3 \cdot 7$

4. Encontrar el MCD de 128304 y 5616

$$\begin{aligned}
128304 &= 5616 \cdot 22 + 4752 \\
5616 &= 4752 \cdot 1 + 864 \\
4752 &= 864 \cdot 5 + 432 \\
864 &= 432 \cdot 2 + 0
\end{aligned}$$

$128304 = 2^4 \cdot 3^6 \cdot 11$
$5616 = 2^4 \cdot 3^3 \cdot 13$

5. Encontrar el MCD de 37908000 y 7344

$$\begin{aligned}
37908000 &= 7344 \cdot 5161 + 5616 \\
7344 &= 5616 \cdot 1 + 1728 \\
5616 &= 1728 \cdot 3 + 432 \\
1728 &= 432 \cdot 4 + 0
\end{aligned}$$

$37908000 = 2^5 \cdot 3^6 \cdot 5^3 \cdot 13$
$7344 = 2^4 \cdot 3^3 \cdot 17$

Ejercicios:

1. Encontrar el MCD (20,16) = 4
2. Encontrar el MCD (45,25) = 5
3. Encontrar el MCD (90,39) = 3
4. Encontrar el MCD (115,35) = 5
5. Encontrar el MCD (3355,64) = 1
6. Encontrar el MCD (111,25) = 1.
7. Encontrar el MCD (3533,1522) = 1.
8. Encontrar el MCD (16848,3672) = 216.

2
Bases de números

Todo número entero $a \in \mathbb{Z}$, se representan en base 10. De hecho la representación usual de los números naturales es en base 10. Esto quiere decir lo siguiente:

1. Los dígitos para representar números enteros son: $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$.
2. Entonces, todo número entero se puede representar con estos dígitos. Esto es por tomar base el diez, y se escriben como suma de potencias de diez.

2.1. Base 10

Para poder entender esto, veamos primero algunos ejemplos. Sabemos que $10^0 = 1$:

Ejemplos de representación de números enteros en base 10:

a.- $17 = 1 \cdot 10^1 + 7 \cdot 10^0$

b.- $83 = 8 \cdot 10^1 + 3 \cdot 10^0$

c.- $123 = 1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0$

d.- $276 = 2 \cdot 10^2 + 7 \cdot 10^1 + 6 \cdot 10^0$

e.- $789 = 7 \cdot 10^2 + 8 \cdot 10^1 + 9 \cdot 10^0$

f.- $4899 = 4 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10^1 + 9 \cdot 10^0$

g.- $5391 = 5 \cdot 10^3 + 3 \cdot 10^2 + 9 \cdot 10^1 + 1 \cdot 10^0$

h.- $3377 = 3 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10^1 + 7 \cdot 10^0$

Si desarrollamos las expresiones de la derecha obtenemos los números de la izquierda, es decir :

a.- $1 \cdot 10^1 + 7 \cdot 10^0 = 10 + 7$

b.- $8 \cdot 10^1 + 3 \cdot 10^0 = 80 + 3$

c.- $1 \cdot 10^2 + 2 \cdot 10^1 + 3 \cdot 10^0 = 100 + 20 + 3$

d.- $2 \cdot 10^2 + 7 \cdot 10^1 + 6 \cdot 10^0 = 200 + 70 + 6$

e.- $7 \cdot 10^2 + 8 \cdot 10^1 + 9 \cdot 10^0 = 700 + 80 + 9$

f.- $4 \cdot 10^3 + 8 \cdot 10^2 + 9 \cdot 10^1 + 9 \cdot 10^0 = 4000 + 800 + 90 + 9$

g.- $5 \cdot 10^3 + 3 \cdot 10^2 + 9 \cdot 10^1 + 1 \cdot 10^0 = 5000 + 300 + 90 + 1$

h.- $3 \cdot 10^3 + 3 \cdot 10^2 + 7 \cdot 10^1 + 7 \cdot 10^0 = 3000 + 300 + 70 + 7$

2.2. base 2

Los números enteros se pueden representarse en cualquier base $b > 1$. Algunas bases no son usadas, sin embargo a causa del desarrollo de las computadoras en los últimos años, los números enteros representados en base 2 han llegado a tener una gran importancia.

Para representar un número entero en base dos se consideran solo los dígitos $\{0, 1\}$.

2.3. de base 10 a base 2

Para pasar un número a representado en base 10 a base 2 se realiza el siguiente procedimiento:

1. Dividir a entre dos, si el resultado es cero entonces éste es el primer dígito de la derecha, si el resultado es uno, entonces éste es el primer dígito de la derecha.
2. Hacer lo mismo con el cociente de la división del paso anterior, para obtener el segundo dígito.
3. el procedimiento se sigue hasta terminar con los cocientes.

Ejemplos:

1. Pasar a 43 de base 10 a base 2.

$$\begin{array}{rcrcr} 43 & = & 21 \cdot 2 & + & 1 \\ 21 & = & 10 \cdot 2 & + & 1 \\ 10 & = & 5 \cdot 2 & + & 0 \\ 5 & = & 2 \cdot 2 & + & 1 \\ 2 & = & 1 \cdot 2 & + & 0 \\ 1 & = & 0 \cdot 2 & + & 1 \end{array}$$

   Por lo tanto $43_{10} = 101011_2$

2. Pasar a 15 de base 10 a base 2.

$$\begin{array}{rcrcr} 15 & = & 7 \cdot 2 & + & 1 \\ 7 & = & 3 \cdot 2 & + & 1 \\ 3 & = & 1 \cdot 2 & + & 1 \\ 1 & = & 0 \cdot 2 & + & 1 \end{array}$$

   Por lo tanto $15_{10} = 1111_2$

3. Pasar a 27 de base 10 a base 2.

$$\begin{array}{rcrcr} 27 & = & 13 \cdot 2 & + & 1 \\ 13 & = & 6 \cdot 2 & + & 1 \\ 6 & = & 3 \cdot 2 & + & 0 \\ 3 & = & 1 \cdot 2 & + & 1 \\ 1 & = & 0 \cdot 2 & + & 1 \end{array}$$

   Por lo tanto $27_{10} = 11011_2$

4. Pasar a 33 de base 10 a base 2.

$$\begin{array}{rcrcr} 33 & = & 16 \cdot 2 & + & 1 \\ 16 & = & 8 \cdot 2 & + & 0 \\ 8 & = & 4 \cdot 2 & + & 0 \\ 4 & = & 2 \cdot 2 & + & 0 \\ 2 & = & 1 \cdot 2 & + & 0 \\ 1 & = & 0 \cdot 2 & + & 1 \end{array}$$

   Por lo tanto $33_{10} = 100001_2$

5. Pasar a 619 de base 10 a base 2.

$$\begin{array}{rcrcr} 619 & = & 309 \cdot 2 & + & 1 \\ 309 & = & 154 \cdot 2 & + & 1 \\ 154 & = & 77 \cdot 2 & + & 0 \\ 77 & = & 38 \cdot 2 & + & 1 \\ 38 & = & 19 \cdot 2 & + & 0 \\ 19 & = & 9 \cdot 2 & + & 1 \\ 9 & = & 4 \cdot 2 & + & 1 \\ 4 & = & 2 \cdot 2 & + & 0 \\ 2 & = & 1 \cdot 2 & + & 0 \\ 1 & = & 0 \cdot 2 & + & 1 \end{array}$$

   Por lo tanto $619_{10} = 1001101011_2$

Ejercicios:

1. Pasar 146_{10} a base 2. (10010010)
2. Pasar 1232_{10} a base 2. (10011010000)
3. Pasar 7594_{10} a base 2. (1110110101010)
4. Pasar 759021_{10} a base 2. (10111001010011101101)

2.4. Base 4,8,16

1. Para representar un número en base $4, 8$ o 16 se sigue el mismo procedimiento que la base 10 o 2. Usando en cada caso los dígitos:

base 4	base 2
0	00
1	01
2	10
3	11

base 8	base 2
0	000
1	001
2	010
3	011
4	100
5	101
6	110
7	111

base 16	base 2
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
a	1010
b	1011
c	1100
d	1101
e	1110
f	1111

2. Para pasar un número de base 10 a base $4, 8$ o 16 se sigue el mismo procedimiento que a base 2, pero se divide por 4,8 o 16 respectivamente.

3. Para pasar de base 2 a base 4,8 o 16, se asocian los dígitos correspondientes y se sustituyen por sus dígitos equivalentes.

   Pasar a 11011011 a base 4, 8 y 16.

   a) $(11)(01)(10)(11) = 3123_4$.

   b) $(011)(011)(011) = 333_8$.

   c) $(1101)(1011) = \mathbf{db}_{16}$.

3
Aritmética Modular

3.1. Introducción

Una de las áreas más divertidas de las matemáticas es la aritmética modular. En la aritmética modular se pueden realizar las mismas operaciones que en los números reales, pero solo con un conjunto finito de elementos.

En esta lección damos una introducción a las congruencias entre números enteros. Listamos las propiedades básicas de las congruencias. Las congruencias tienen una buena cantidad de aplicaciones prácticas, al final damos cuenta de algunas de ellas.

3.2. El conjunto de elementos módulo n, $\mathbb{Z}_n$.

La definición de $\mathbb{Z}_n$, es simple. Primero damos un número entero n mayor a 1. Después definimos a $\mathbb{Z}_n$ como el conjunto de residuos módulo n. Es decir

$$\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-1\}$$

ya que estos son todos los posibles residuos al dividir cualquier número entero por n. Por el teorema de la división para números enteros tenemos que para m y n siempre existen q, r donde $0 \leq r < n$ tal que $m = qn + r$. Lo anterior nos permite identificar a cualquier número entero m con su residuo r, se dice que la clase módulo n de m es r.

En la siguiente tabla podemos dar algunas de las identificaciones para el caso de $n = 5$.

Residuos módulo 5				
-10	-9	-8	-7	-6
-5	-4	-3	-2	-1
0	1	2	3	4
5	6	7	8	9
10	11	12	13	14
15	16	17	18	19

La tabla quiere decir que 17 al dividirlo por 5 deja como residuo 2 (17 está en la columna del 2). También que el 6 al dividirlo por 5 deja como residuo 1.

Se acostumbra a escribirse como $1 \equiv 6 (\text{mod } 5)$, y se lee, 1 es congruente con 6 módulo 5.

Formalmente, $1 \equiv 6 (\text{mod } 5)$, porque 5 divide a $6-1$. Es decir, sean a, b números enteros, entonces a es congruente con b módulo n si $m|(a-b)$.

3.2.1. Propiedades de las congruencias

1. Dado un número n, todo entero m es congruente a uno y solo un residuo módulo n.
2. Se cumple la propiedad reflexiva, es decir todo entero es congruente con si mismo módulo n.
3. Se cumple la propiedad simétrica, es decir, si a es congruente con b, entonces b es congruente con a módulo n.
4. Se cumple la propiedad transitiva, es decir, Si a es congruente con b y b es congruente con c, entonces a es congruente con c módulo n.
5. Las propiedades 2,3,4 dicen que la congruencia es una relación de equivalencia. Equivalentemente que dado un entero n, entonces de la congruencia módulo n se deriva una partición para los números enteros. De manera informal esto quiere decir que con las congruencias podemos ver a los números enteros como un conjunto finito de “números".
6. Se puede definir una suma entre las clases de $\mathbb{Z}_n$, con esta suma $\mathbb{Z}_n$ es un grupo conmutativo.
7. Se puede definir un producto en $\mathbb{Z}_n$, pero para un elemento a existe su inverso multiplicativo sí y solo si $(a, n) = 1$.
8. Si n es número primo, entonces $\mathbb{Z}_n$ es un campo.

3.3. La suma en $\mathbb{Z}_n$

Cuando es necesario distinguir a los elementos de $\mathbb{Z}_n$ se escriben como $[a]$ ó $\overline{a}$.
La suma en $\mathbb{Z}_n$ se realiza de manera natural, si $[a], [b] \in \mathbb{Z}_n$, entonces $[a+b]$ es el residuo correspondiente a $a+b$.

Ejemplos:

1. Sea $n = 2$, entonces la tabla de suma de los elementos de $\mathbb{Z}_2$ es:

$+$	0	1
0	0	1
1	1	0

2. Sea $n = 3$, entonces la tabla de suma de los elementos de $\mathbb{Z}_3$ es:

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

3. Sea $n = 4$, entonces la tabla de suma de los elementos de $\mathbb{Z}_4$ es:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

4. Sea $n = 5$, entonces la tabla de suma de los elementos de $\mathbb{Z}_5$ es:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

3.4. El producto en $\mathbb{Z}_n$

El producto en $\mathbb{Z}_n$ se realiza de manera natural, si $[a], [b] \in \mathbb{Z}_n$, entonces $[a \cdot b]$ es el residuo correspondiente a $a \cdot b$.

Ejemplos:

1. Sea $n = 2$, entonces la tabla de multiplicación de los elementos de $\mathbb{Z}_2$ es:

$\cdot$	0	1
0	0	0
1	0	1

2. Sea $n = 3$, entonces la tabla de multiplicación de los elementos de $\mathbb{Z}_3$ es:

$\cdot$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

3. Sea $n = 4$, entonces la tabla de multiplicación de los elementos de $\mathbb{Z}_4$ es:

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

4. Sea $n = 5$, entonces la tabla de multiplicación de los elementos de $\mathbb{Z}_5$ es:

$\cdot$	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

Obsérvese que en el caso $n = 4$, el producto $2 \cdot 2 = 0$, esto quiere decir que en este caso la clase del 2 no tiene inverso multiplicativo.

Obsérvese también que en los otros casos $n = 2, 3, 5$ todos los elementos tienen inverso multiplicativo.

3.5. Si n es número primo, $\mathbb{Z}_n$ es campo

Si n es un número primo entonces todo elemento de $\mathbb{Z}_n = \{0, 1, 2, ..., n-1\}$ tiene inverso multiplicativo. Es decir $\mathbb{Z}_n$ es un campo. Sea $a \in \mathbb{Z}_n$, como n es primo, entonces $(a, n) = 1$ y por el teorema extendido de Euclides existen enteros b, c tales que $ba + nc = 1$, aplicando la división por n y obteniendo su residuo a la igualdad, obtenemos $ba = 1$. Esto quiere decir que el inverso multiplicativo módulo n de a es b.

3.6. Algunos teoremas importantes

1. Sea p un número primo, entonces $\mathbb{Z}_p$ es un campo finito. De hecho se puede mostrar que cualquier campo finito tiene como base un campo $\mathbb{Z}_p$ es decir, todo campo finito es una extensión de $\mathbb{Z}_p$, o también que todo campo finito tiene la forma $\mathbb{Z}_{p^n}$.

2. El pequeño teorema de Fermat afirma que para todo a y p un primo, entonces $a^p \equiv a(\bmod p)$. Es decir que si p es un número primo entonces $a^{p-1} \equiv 1(\bmod p)$. Esta última desigualdad es usada para probar que un número p presuntamente puede ser primo. Debido a la dificultad para probar realmente que un número p sea primo, se han usado métodos probabilísticos, es decir métodos que arrogan con alta probabilidad a un número primo. A este tipo de números se les conoce como seudoprimos, pero para casos prácticos se ha podido mostrar que estos seudoprimos de hecho son primos. Los métodos esencialmente toman varios “testigos"a y verifican si se cumple la congruencia $a^{p-1} \equiv 1(\bmod p)$, en tal caso se declara a p un seudoprimo.

3.7. Aplicaciones de la aritmética modular.

Entre las aplicaciones más conocidas de las congruencias tenemos:

1. En criptografía, su uso es extenso, en muchos casos los sistemas criptográficos realizan sus operaciones en $\mathbb{Z}_n$, para diferentes tipos de n. Para el sistema RSA n es producto de dos números primos $n = pq$. Para otros sistemas como DH, ElGamal, n es primo.

2. En varios sistemas de verificación de dígitos, la aritmética modular es muy usada. Estos sistemas son usados ampliamente en productos de los supermercados, en servicios postales, en cheques, tarjetas de crédito, etc.

3.7.1. Intercambio de claves Diffie-Hellman.

1. Primero Alice y Bob se ponen de acuerdo en los parámetros públicos. Sea por ejemplo $g = 2$ y $\mathbb{Z}_n = \mathbb{Z}_{19}$.

2. Tanto Bob como Alice generan su parte secreta (clave secreta).

Alice genera	Bob genera
$x = 7$	$y = 9$

3. Ambos ahora calculan g^x para Alice y g^y Bob.

Alice	Bob
$g^x = 2^7 (\bmod 19) = 14$	$g^y = 2^9 (\bmod 19) = 18$

4. Se realiza el intercambio de valores g^x, g^y.

Alice	Bob
$g^x = 14$	$g^y = 18$
18	14

5. Ambos elevan su parte recibida a su clave secreta.

Alice	Bob
$g^x = 14$	$g^y = 18$
18	14
$18^7 (\bmod 19) = 18$	$14^9 (\bmod 19) = 18$

6. Finalmente ambos comparten la misma clave simétrica.

Alice	Bob
$g^x = 14$	$g^y = 18$
18	14
$18^7 (\bmod 19) = 18$	$14^9 (\bmod 19) = 18$
18	18

3.7.2. Calcular logaritmos discretos a fuerza bruta.

1. En $\mathbb{Z}_{17}$ calcular el logaritmo discreto de 4 base 5. Es decir encontrar x tal que $5^x = 4 \bmod 17$. Por fuerza bruta calculamos potencias sucesivas de 5.

$$
\begin{array}{c}
5^1 (\bmod 17) = 5 \\
5^2 (\bmod 17) = 8 \\
5^3 (\bmod 17) = 6 \\
5^4 (\bmod 17) = 13 \\
5^5 (\bmod 17) = 14 \\
5^6 (\bmod 17) = 2 \\
5^7 (\bmod 17) = 10 \\
5^8 (\bmod 17) = 16 \\
5^9 (\bmod 17) = 12 \\
5^{10} (\bmod 17) = 9 \\
5^{11} (\bmod 17) = 11 \\
5^{12} (\bmod 17) = 4
\end{array}
$$

Por lo tanto $\log_5(4) = x = 12$.

3.7.3. Elevar a potencias modulares (Método binario).

En ocasiones la operación $a^b \bmod n$, no es fácil de realizar con pocos recursos como calculadoras de 32 bits. Existe un método (el binario) que nos ayudara a realizar esta operación de manera eficiente.

1. Realizar $a^b \bmod n$.
2. Por ejemplo: $247^{235} \bmod 391$.
3. Escribir en binario a la potancia $235_{10} = 11101011_2$.
4. Por lo tanto

$$
\begin{array}{rcl}
247^{235} & = & 247^{1\cdot 2^7+1\cdot 2^6+1\cdot 2^5+0\cdot 2^4+1\cdot 2^3+0\cdot 2^2+1\cdot 2^1+1\cdot 2^0} \\
& = & 247^{2^7} 247^{2^6} 247^{2^5} 247^{2^3} 247^{2^1} 247^{2^0}
\end{array}
$$

5. Ahora podemos calcular potencias modulares de la siguiente forma:

$$
\begin{array}{rcl}
247^{2^0} \bmod 391 & = & 247 \\
247^{2^1} \bmod 391 & = & 13 \\
247^{2^3} \bmod 391 & = & 18 \\
247^{2^5} \bmod 391 & = & 188 \\
247^{2^6} \bmod 391 & = & 154 \\
247^{2^7} \bmod 391 & = & 256
\end{array}
$$

6. Finalmente calculamos el producto:

$$
\begin{array}{rcl}
247 \cdot 13 \bmod 391 & = & 83 \\
83 \cdot 18 \bmod 391 & = & 321 \\
321 \cdot 188 \bmod 391 & = & 134 \\
134 \cdot 154 \bmod 391 & = & 304 \\
304 \cdot 256 \bmod 391 & = & 15
\end{array}
$$

7. Con todo lo anterior $247^{235} \bmod 391 = 15$.

3.7.4. Método RSA (Rivest, Shamir, Adleman).

El sistema RSA es un método criptográfico de clave pública, que es ampliamente usado en certificados digitales en la actualidad.

1. Sea $n = p \cdot q$ producto de dos números primos.
2. Sea e un número entero.
3. Sea M el mensaje a cifrar.
4. Sea C el mensaje a cifrado.
5. $C = M^e \mod n$ formula de cifrado.
6. $M = C^d \mod n$ formula de descifrado.
7. Donde $d = e^{-1} \mod (p-1)(q-1)$.

Calcular inversos multiplicatimos modulares.
Un inverso multiplicativo modular de a es un número b tal que $a \cdot b \mod n = 1$. El método para calcular inversos multiplicativos es el algoritmo extendido de Euclides. Sin embargo suele ser en algunos casos más rápido calcularlo por ensayo y error.

1. Se sabe que 1 es del número $n+1$, por lo tanto si queremos calcular a $d = e^{-1} \mod n$. Entonces multiplicamos $d \cdot e$ con d tal que su producto este cerca de n, si no es el caso, entonces buscamos a d si el producto $d \cdot e$ esta cerca de $2n+1$, si no, cerca de $3n+1$, etc.
2. Ejemplo: si $p = 17, q = 23$, $e = 3$. Entonces $(p-1)(q-1) = 352$, además si $d = 117$, entonces $d \cdot e = 117 \cdot 3 = 351$que no fue 1. Ahora $d = 235$, $d \cdot e = 235 \cdot 3 = 705$ pero $705 = 352 \cdot 2 + 1$, es decir $d = 235$ es el inverso de $e = 3 \mod 352$.

Ejemplo RSA.

1. Sea $p = 17, q = 19$ y $e = 5$.
2. Entonces $n = 323$, $(p-1)(q-1) = 288$, y $d = 173$.
3. Si $M = 10$, entonces $C = M^e \mod 323 = 193$.
4. $M = C^d \mod 323 = 193^{173} \mod 323 = 10$.

3.8. Ejercicios:

1. Hacer la tabla de suma y producto de $\mathbb{Z}_{11}$.
2. Por ensayo y error calcular $\ln_2(9)$ en $\mathbb{Z}_{11}$.
3. Si $g = 2$ y $\mathbb{Z}_{11}$, son los parámetros públicos en el esquema de intercambio de claves DH (Diffie-Hellman). La parte secreta de Alice es 6, la parte secreta de Bob es 3. Encontrar la clave secreta compartida.
4. Si $g = 2$ y $\mathbb{Z}_{11}$, son los parámetros públicos en el esquema de intercambio de claves DH (Diffie-Hellman). La parte secreta de Alice es 8, la parte secreta de Bob es 9. Encontrar la clave secreta compartida.

5. Si $g = 2$ y $\mathbb{Z}_{11}$, son los parámetros públicos en el esquema de intercambio de claves DH (Diffie-Hellman). La clave compartida es 3. Encontrar posibles claves secretas de Alice y Bob.

6. En el sistema RSA, tomamos $p = 23$, $q = 17$ $e = 3$, cifrar el mensaje $m = 10$, y descifrarlo escribiendo todas sus operaciones modulares.

7. En el sistema RSA, tomamos $p = 23$, $q = 17$ $e = 3$, cifrar el mensaje $m = 25$, y descifrarlo escribiendo todas sus operaciones modulares.

8. En el sistema RSA, tomamos $p = 19$, $q = 17$ $e = 5$, cifrar el mensaje $m = 66$, y descifrarlo escribiendo todas sus operaciones modulares.

9. En el sistema RSA, tomamos $p = 3$, $q = 11$ $e = 3$, se cifro el mensaje M y se obtuvo el mensaje $C = 13$, encontrar el mensaje original. 7

10. En el sistema RSA, tomamos $p = 2$, $q = 5$ $e = 3$, se cifro el mensaje M y se obtuvo el mensaje $C = 3$, encontrar el mensaje original. 7

11. En el sistema RSA, tomamos $p = 2$, $q = 5$ $e = 3$, se cifro el mensaje M y se obtuvo el mensaje $C = 2$, encontrar el mensaje original. 8

12. En el sistema RSA, tomamos $p = 3$, $q = 5$ $e = 3$, se cifro el mensaje M y se obtuvo el mensaje $C = 8$, encontrar el mensaje original. 2

13. En el sistema RSA, tomamos $p = 3$, $q = 5$ $e = 3$, se cifro el mensaje M y se obtuvo el mensaje $C = 13$, encontrar el mensaje original. 7

14. En el sistema RSA, tomamos $p = 3$, $q = 5$ $e = 3$, se cifro el mensaje M y se obtuvo el mensaje $C = 12$, encontrar el mensaje original. 3

15. En el sistema RSA, tomamos $p = 3$, $q = 5$ $e = 3$, se cifro el mensaje M y se obtuvo el mensaje $C = 2$, encontrar el mensaje original. 8

16. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 32$, encontrar el mensaje original. 2

17. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 5$, encontrar el mensaje original. 10

18. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 9$, encontrar el mensaje original. 4

19. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 12$, encontrar el mensaje original. 17

20. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 33$, encontrar el mensaje original. 3

21. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 23$, encontrar el mensaje original. 18

22. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 24$, encontrar el mensaje original. 19

23. En el sistema RSA, tomamos $p = 5$, $q = 7$ $e = 5$, se cifro el mensaje M y se obtuvo el mensaje $C = 11$, encontrar el mensaje original. 16

4 Combinatoria

4.1. Combinaciones y Permutaciones

1. Sean dos conjuntos finitos disjuntos T, S, entonces:
   a) $|S \cup T| = |S| + |T|$(principio de la suma).
   En general $|S \cup T| = |S| + |T| - |S \cap T|$

2. Sean dos conjuntos finitos T, S, entonces: $|T \times S| = |T||S|$(principio del producto).

3. Si S es un conjunto finito de n elementos, y elegimos k de ellos con reemplazamiento. Entonces tenemos
$$n^k$$
posibles elecciones.

4. Si S es un conjunto finito de n elementos, y elegimos k de ellos sin reemplazamiento. Entonces Tenemos
$$n(n-1)(n-2)\cdots(n-(k-1))$$
posibles elecciones.

5. Si S es un conjunto finito de n elementos, y $k < n$ entonces hay $P(n,k)$ permutaciones de k de los n elementos,
$$P(n,k) = \frac{n!}{(n-k)!}$$

6. Sean n, k números enteros, el coeficiente binomial esta definido como:
$$\binom{n}{k} = \frac{n!}{(n-k)!k!}$$
es el número de subconjuntos de k elementos, tomados de un conjunto de n elementos.

7. Se cumple que:
$$\binom{n}{k} = \frac{P(n,k)}{k!}$$
es el número de subconjuntos de k elementos, tomados de un conjunto de n elementos.

8. Si existen n objetos con n_1 de un tipo (iguales), n_2 de otro tipo, y n_r de un r-ésimo tipo, entonces hay
$$\frac{n!}{n_1!n_2!\cdots n_r!}$$
disposiciones de los n objetos dados sin distinguir los del mismo tipo.

4.2. Problemas

Problemas resueltos:

1. Un anuncio de hamburguesas indica que un cliente puede ordenar su hamburguesa con algunos, ninguno o todos de los siguientes ingredientes: catsup, mostaza, mayonesa, lechuga, tomate, cebolla, pepinillos, queso o champiñones. ¿cuántas ordenes diferentes de hamburguesas se pueden servir?
Solución: una orden esta compuesta de cualquier subconjunto de los 9 ingredientes, es decir hay $\binom{9}{0} + \binom{9}{1} + \binom{9}{2} + \cdots + \binom{9}{9}$ posibilidades. Por el teorema del binomio son $(1+1)^9$ de ordenes diferentes.

2. Si lanzamos una moneda 5 veces, cuántos posibles resultados tenemos.
Solución: Al lanzar la primera vez las posibilidades de resultados son 2, al lanzar la segunda vez las posibilidades son igual dos, entonces tenemos 2×2 posibles resultados con dos lanzamientos. Con 5 lanzamientos tenemos $2 \times 2 \times 2 \times 2 \times 2 \times 2 = 2^5 = 32$ posibles resultados.

3. Cuántos posibles números podemos tener de 3 dígitos. (10^3).

4. Cuántos números podemos tener en una máquina de 8 bits. (2^8).

5. De cuantas maneras modemos sentar a 5 niños en 5 sillas. ($5 \cdot 4 \cdots 1$).

6. De cuantás manera podemos sentar a 10 niños en 5 sillas. ($10 \times 9 \times 8 \times 7 \times 6$).

7. ¿cuántas maneras hay de elegir 2 sillas de una fila de 5 sillas ? ($C(10,2)$).

8. De cuántas maneras podemos elegir un comité de 3 personas (presidente, vice presidente y secretario) de un grupo de 9 candidatos. ($P(9,3)$).

9. De cuántas maneras podemos elegir un comité de 3 personas de un grupo de 9 candidatos. ($C(9,3)$).

10. Si un típico número de teléfono tiene la forma $555 - 817 - 4495$. Donde los tres primeros dígitos pertenecen al código del área.

    a) Suponiendo que no hay restricción, cuántos códigos de área hay. (10^3).

    b) Si el dígito de enmedio del código de área solo puede ser 0 o 1, cuántas áreas de código posibles podemos tener. ($10 \times 2 \times 10$)

    c) Si no hay restricciones, cuántos posibles números telefónicos podemos tener. (10^{10}).

    d) Si la restricción es que los dígitos solo podemos usarlos una sola vez. Cuántos números telefónicos podemos tener. ($10!$)

11. Cuántos números pares de dos dígitos podemos formar. (45).

12. Cuántos números enteros positivos menores a 1 millón, tienen exactamente un 3 un 4 y un 5 en surepresentación decimal. $(5 \cdot 4 \cdot 3 \cdot 7 \cdot 7 = 2940)$.

13. Resolver:

    a) De un examen de 10 preguntas, un estudiante solo debe responder 7. De cuántas formas puede resolver el examen. ($C(10,7)$).

    b) Si el estudiante debe resolver 3 preguntas de las primeras 5 y 4 de las otras 5. $C(5,3)C(5,4)$.

    c) Si el estudiante debe resolver 7 de las 10 preguntas, donde almenos 3 deben de seleccionarse de las primeras 5. $C(5,3)C(5,4) + C(5,4)C(5,3) + C(5,5)C(5,2)$.

14. La cafeteria Paty tiene 8 tipos diferentes de pasteles y seis tipos diferentes de bollos. Además de las piezas de pastelería es posible adquirir vasos pequeños, medianos o grandes de las siguientes bebidas: café (negro, con crema, con azúcar, o con crema y azúcar), té (solo, con crema, con azúcar, con crema y azúcar, con limón, o con limón y azúcar), chocolate caliente y jugo de naranja. Cuando carolina va a la cafetería Paty, de cuántas puede ordenar:

    a) una pieza de pastelería y una bebida mediana para ella.

    b) una pieza de pastelería y un vaso de café para ella, y un bollo y un vaso de té para su jefe.

    c) una pieza de pastelería y un vaso de té para ella, un bollo y un jugo de naranja para su jefe y una pieza de pastelería y n vaso de café para cada uno de sus dos asistentes.

    Solución:

    a) Una pieza de pastelería se elige de 8+6= 14 opciones y de 4+6+2=12 opciones de bebidas. Entonces tiene $\binom{14}{1} \cdot \binom{12}{1} = 168$ posibles ordenes.

    b) Una pieza de pastelería se elige de $8+6 = 14$ opciones, y $4 \cdot 3$ opciones de café (3 tamaños y 4 combinaciones). Además 6 posibles bollos y $3 \cdot 6$ opciones de té. Entonces hay $14 \cdot 4 \cdot 3 \cdot 6 \cdot 3 \cdot 6 = 18144$ total de maneras de ordenar.

    c) Una pieza de pastelería y un café para ella son $14 \cdot 3 \cdot 6$. Un bollo y un jugo de naranja para su jefe son $6 \cdot 3$ opciones. Finalmente una pieza de pastelería y un té $14^2 \cdot 3^2 \cdot 4^2$ para los 2 asistentes. Hacen un total de 128024064 posibles ordenes.

15. Pamela tiene 5 libros distintos, ¿de cuántas formas puede colocar sus libros en dos repisas de modo que haya al menos un libro en cada una?

    a) Si solo son 3 libros, entonces tenemos que las únicas opciones son $\frac{1}{2}, \frac{2}{1}$ si el numerador es la primera repisa y el denominador la repisa de abajo. En el primer caso, solo podemos elegir $P(3,1)$ posibilidades el la repisa de arriba y quedan solo dos libros, que podemos ordenar de 2! opciones, entonces tenemos $P(3,1)2!$. Para el segundo caso, tenemos $P(3,2)$ y abajo solo 1!, así tenemos $P(3,2)1!$. En total tenemos $P(3,1)2! + P(3,2)1! = 3! + 3! = 2 \cdot 3! = 12$. Si los libros son A, B, C las opciones son:
    $\frac{A}{BC}, \frac{A}{CB}, \frac{B}{AC}, \frac{B}{CA}, \frac{C}{AB}, \frac{C}{BA}$ y las simétricas.

    b) En el caso de 4 libros, serían $P(4,1)3! + P(4,2)2! + P(4,3)1! = 3 \cdot 4!$.

    c) entonces para 5 libros son $5! \cdot 4$.

16. Encontrar valores para n tales que:

    a) $P(n,2) = 90$

b) $P(n,3) = 3P(n,2)$

c) $2P(n,2) + 50 = P(2n,2)$

17. De cuantas maneras podemos arreglar los símbolos $a, b, c, d, e, e, e, e, e$ de tal manera que no haya letras e juntas.

1. ¿cuántas maneras hay de construir palabras de 5 letras? (26^5).
2. ¿cuántas maneras hay de construir palabras de 5 letras diferentes? ($26 \cdot 25 \cdot 24 \cdot 23 \cdot 22$).
3. ¿cuántas maneras hay de elegir un hombre y una mujer de 3 hombres y 8 mujeres? $\binom{3}{1}\binom{8}{1}$.
4. ¿cuántas maneras hay sentar 2 personas en 5 sillas de una fila? ($5 \cdot 4$).
5. ¿cuántas maneras hay de elegir 2 sillas de 5 sillas de una fila? (10).
6. Pamela tiene 15 libros distintos, ¿de cuántas formas puede colocar sus libros en dos repisas de modo que haya al menos un libro en cada una?. $14 \cdot 15!$.
7. ¿cuántas maneras hay de arreglar 4 diferentes libros de álgebra, 3 diferentes libros de geometría, y 6 diferentes libros de cálculo?
8. ¿cuántas maneras hay de sentar 12 caballeros del rey Arturo en una mesa redonda? ($11!$).
9. De las 26 letras del alfabeto, ¿cuántas permutaciones no tienen 2 vocales juntas? ($21!\binom{22}{5}5!$).
10. Mostrar que:
$$\binom{n}{k} = \binom{n}{n-k}$$
11. Mostrar que:
$$\binom{n}{k+1} = \binom{n}{k}\frac{n-k}{k+1}$$
12. Mostrar que:
$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$
13. Mostrar que:
$$\binom{n}{k} = \frac{n}{k}\binom{n-1}{k-1}$$
14. Mostrar que:
$$\binom{s}{m}\binom{m}{k} = \binom{s}{k}\binom{s-k}{m-k}$$
15. Mostrar que:
$$\sum_{k=0}^{n}\binom{n}{k} = 2^n$$
16. Mostrar que:
$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0$$
17. Si n es un entero positivo mayor a 1, probar que: $\binom{n}{2} + \binom{n-1}{2}$ es un cuadrado perfecto. ($(n-1)^2$).

18. Verificar si $\binom{2n}{n} - \binom{2n}{n-1} = \frac{1}{n+1}\binom{2n}{n}$

19. Cuántos bytes contienen:

    a) Exactamente 2 1_s.
    b) Exactamente 4 1_s.
    c) Al menos 6 1_s
    d) A lo más 3 1_s.

20. ¿Cuál es el valor de la variable `counter` del siguiente algoritmo?

```
counter = 0;
For i=1 to 12 do
counter = counter +1;
For j=5 to 10 do
counter = counter +2;
For k=15 downto 8 do
counter = counter +3;
```

    ¿Qué principio de conteo esta involucrado?

21. ¿Cuantas veces se ejecuta la instrucción `Write`?

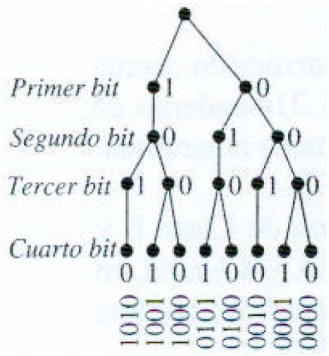
```
For i = 1 to 12 do
For j = 5 to 10 do
For k = 15 downto 3 do
Write ((i-j)*k)
```

    ¿Qué principio de conteo esta involucrado?

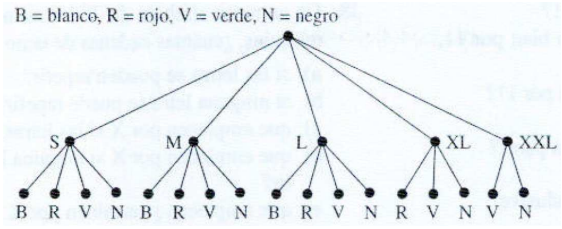
22. Cada usiario tiene una contraseña de longitud entre 6 y 8 caracteres que son o bien un dígito o una letra. Cada contraseña, debe contener almenos un dígito, ¿ cuántas contraseñas distintas admite el sistema?
    Res: $P_6 + P_7 + P_8 = 36^6 - 26^6 + 36^7 - 26^7 + 36^8 - 26^8$.

23. Cuántas cadenas de bits hay que tengan longitud de 8 y que bien comiencen con un 1 o terminen con 00.
    Res: Que inicien con 1 son 2^7 formas distintas, que terminen con 00 hay 2^6, que inicien con 1 y termimen con 00 son 2^5. Por lo tano, lo pedido es $2^7 + 2^6 - 2^5$.

24. Cuántas cadenas de bits de longitud 4 no tienen dos unos consecutivos.



25. Cuántas camisetas diferentes debe haber en un almacen de una tienda si se quiere tener disponible una de cada modelo, y se fabrican de 5 diferentes tallas S,M, L, XL, XXL, además de cada talla se tienen colores; blanco, negro, rojo y verde, pero para la talla XXL solo hay verde y negro.



26. ¿Cuántas cadenas de 10 bits empiezan y terminan con 1?

27. ¿Cuántas cadenas de bits de longitud 6 o menos hay?

28. ¿Cuántas cadenas de bits de longitud n hay que empiezan y terminan con 1?

29. ¿Cuántas cadenas de bits de longitud 6 comienzan con 000 o bien terminan con 00?

30. ¿Cuántas cadenas de bits de longitud 8 contienen bien la cadena 000 o bien la cadena 1111?

4.3. Problemas algoritmos

I

procedure max($a_1, a_2, ..., a_n$)
$max = a_1$;
for $i = 2$ to n
If $max < a_i$ then $max = a_i$;
print (max)

La complejidad es $2(n-1)+1 = 2n-1$ comparaciones, una para saber si es el final y otra para saber si es el elemento. Al final una comparación más para salir del for. Es decir el algoritmo tiene complejidad $O(n)$

II

procedure busqueda de x en ($a_1, a_2, ..., a_n$)
$i = 1$;
while $i \leq n$ & $x \neq a_i$
$i = i + 1$;
If $i \leq n$ then $loc = i$
Else $loc = 0$;
print (loc) (índice de x)

La complejidad es $2n+1$ comparaciones, una para saber si es el final y otra para saber si es el elemento $2n$, más 1 al salir del bucle, ó más 2 si no está (en el peor de los casos), una para salir del bucle y otra fuera del bucle, $(2n+2)$. Es decir el algoritmo tiene complejidad $O(n)$

III

```
procedure                busqueda binaria de x en (a_1, a_2, ..., a_n)
i = 1 (extremo izquierdo);
j = n (extremo derecho);
                         while i < j
                         begin
                         m = ⌊(i + j)/2⌋;
                         If x > a_m then          i = m + 1
                         else                     j = m
                         end
If x = a_i then          loc = i
else loc = 0
print (loc) (índice de x)
```

Supongamos que $n = 2^k$ por simplicidad, observese que $k = \log_2 n$. En cada paso, se compara $i < j$ del while para saber si hay más de un elemento en la lista, entonces se redefinen los extremos de la lista y esta queda con 2^{k-1} elementos. Entonces, hemos hecho dos comparaciones, una $i < j$ y otra para saber en que lado de la lista esta x. De manera recurrente para el siguiente caso, la lista se reduce a 2^{k-2} elementos. Las últimas dos comparaciones se hacen cuando la lista tiene 2 elementos, y finalmente cuando hay un elemento en la lista, una más para salir del while y otra más para saber si está x. Por lo tanto se hacen $2k + 2$ comparaciones o sea $2(\log n) + 2$ comparaciones, es decir el algoritmo tiene una complejidad de $O(\log n)$.

IV

```
procedure                base 10 a base 2
n (número en base 10);
                         while n ≠ 0
                         q = n/2;
                         r = n % 2;
                         n = q;
print (r)
```

Sea n un número entero, n se puede representar en base b, por ejemplo 2. Entonces existe k tal que $b^{k-1} \leq n < b^k$, n tiene k dígitos $k = \log_b n + 1$. El algoritmo realiza $O(\log n)$ pasos, y en cada paso se realiza una división de un número de longitud $k - bits$ eso se lleva a lo más con $O(\log n)$ operaciones, en total el algoritmo tiene una complejidad de $O(\log^2 n)$.

V Algoritmo de Euclides

$$\begin{aligned}
a &= bq_1 + r_1 && 0 \leq r_1 < b \\
b &= r_1 q_2 + r_2 && 0 \leq r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 \leq r_3 < r_2 \\
&\cdots \\
r_{k-3} &= r_{k-2} q_{k-1} + r_{k-1} && 0 \leq r_{k-1} < r_{k-2} \\
r_{k-2} &= r_{k-1} q_{k-1} && 0 \leq r_k = 0
\end{aligned}$$

En este proceso $r_{j+2} < 1/2 r_j$. Si $r_{j+1} \leq 1/2 r_j$, se tiene el resultado, pero si $r_{j+1} > 1/2 r_j$, en

el siguiente paso tenemos $r_j = 1 \cdot r_{j+1} + r_{j+2}$, entonces $r_{j+2} = r_j - r_{j+1} < 1/2 r_j$ como se requiere.

Como en cada dos pasos el residuo se reduce a la mitad de su tamaño, y este solo llega en el peor de los casos a 1, entonces hay a lo más $2 \log_2 a$ divisiones, es decir $O(\log a)$ y cada división requiere no más de $O(\log a)$, entonces $O(log^2 a)$ operaciones.

En el caso de algoritmo extendido de Euclides podemos realizarlo en $O(log^3 a)$ operaciones.

V Exponenciación modular por el método de cuadrados repetidos

La operación b^n mod m tiene una complejidad de $O(\log n)(\log^2 m)$

5 Recurrencia

5.1. Recurrencias lineales de primer orden

$$a_{n+1} = da_n$$

Solución: $a_n = a_0 d^n$

5.2. Recurrencias lineales de segundo orden homogéneas

$$C_n a_n + C_{n-1} a_{n-1} + C_{n-2} a_{n-2} = 0$$

Ecuación característica: $C_n r^2 + C_{n-1} r + C_{n-2} = 0$.

1. Raíces diferentes: $a_n = c_1(r_1^n) + c_2(r_2)^n$.
2. Raíces iguales: $a_n = c_1(r_1^n) + c_2 n(r_2)^n$

5.3. Recurrencias lineales de segundo orden no homogéneas

$a_n^{(p)}$	
parte no-H	forma de $a_n^{(p)}$
C	A
n	$A_1 n + A_0$
n^2	$A_2 n^2 + A_1 n + A_0$
r^n	$A r^n$
$\sin(\alpha n)$	$A\sin(\alpha n) + B\cos(\alpha n)$
$\cos(\alpha n)$	$A\sin(\alpha n) + B\cos(\alpha n)$

5.4. Ejercicios

1. Encontrar la solución general para cada una de las siguientes progresiones geométricas.
   a) $a_{n+1} - 1{,}5a_n = 0$, $n \geq 0$.
   b) $4a_n - 5a_{n-1} = 0$, $n \geq 1$.
   c) $3a_{n+1} - 4a_n = 0$, $n \geq 0$, $a_1 = 5$.
   d) $2a_n - 3a_{n-1} = 0$, $n \geq 1$, $a_4 = 81$.
2. Si a_n, $n \geq 0$, es una solución de la relación de recurrencia $a_{n+1} - da_n = 0$, y $a_3 = 153/49$, $a_5 = 1377/2401$, ¿cuánto vale d?
3. Encontrar la complejidad del algoritmo de la Burbuja.
4. Encontrar la complejidad del algoritmo de las torres de Hanoi.
5. Resolver la recurrencia de los números de Fibonacci.
6. $a_{n+2} + a_n = 0$, $a_0 = 0, a_1 = 3$.
7. $a_n = 5a_{n-1} - 6a_{n-2}$, $a_1 = -1, a_2 = 1$.
8. $a_n = 6a_{n-1} - 9a_{n-2}$, $a_1 = 1, a_2 = 9$.
9. $b_n = b_{n-1} + b_{n-2}$, $n \geq 3$, (ver al número de secuencias de n-dígitos binarios que no contiene dos 0s consecutivos)
10. Definimos a los números de Lucas L_n como $L_1 = 1$, $L_2 = 3$, $L_n = L_{n-1} + L_{n-2}$.
11. $a_{n+2} + 4a_n = 0$, $a_0 = 1, a_1 = 1$.
12. $a_n + 2a_{n-1} + 2a_{n-2} = 0$, $a_0 = 1, a_1 = 3$.
13. $a_{n+2} + 3a_{n+1} + 2a_n = 3^n$, $a_0 = 0, a_1 = 1$.
14. $a_{n+2} + 4a_{n+1} + 4a_n = 7$, $a_0 = 0, a_1 = 2$.
15. $a_{n+2} - a_n = \sin(n\pi/2)$, $a_0 = 1, a_1 = 2$.

5.5. Aplicaciones

5.5.1. Algoritmo de la Burbuja

Algoritmo de la burbuja
Begin
For $i = 1$ to $n - 1$ do
For $j = n$ downto $i + 1$ do
If $x_j < x_{j-1}$ then
Begin (intercambio, swap)
$temp = x_{j-1}$
$x_{j-1} = x_j$
$x_j = temp$
End
End

Número de comparaciones $a_n = a_{n-1} + (n-1)\ n \geq 2\ a_1 = 0$

$a_1 = 0$

$a_2 = a_1 + (2-1) = 1$

$a_3 = a_2 + (3-1) = 1 + 2$

$a_4 = a_3 + (4-1) = 1 + 2 + 3$

.....

$a_n = 1 + 2 + 3 + \cdots + (n-1) = (n-1)n/2 = (n^2 - n)/2$

5.5.2. Torres de Hanoi

Número de comparaciones movimientos:

i) a_n es el número de movimientos de discos de una torre a la otra.

ii) Se hacen a_n movimientos para mover n discos a la torre 3.

iii) Movemos el disco $n+1$ a la torre 2

iv) Se hacen a_n movimientos para mover n discos a la torre 2.

v) Por lo tanto para mover $n+1$ discos hacemos $a_{n+1} = 2a_n + 1$ movimientos.

Tenemos la relación no homogénea $a_{n+1} - 2a_n = 1$

La solución de la parte homogénea $a_n^h = c2^n$

La solución particular de la parte no homogénea es $a_n^p = A$

De donde $A - 2A = 1$, entonces $A = -1$

La solución se convierte en $a_n^h + a_n^p = c(2^n) + A$.

como $a_0 = 0$, entonces $0 = c - 1$, entonces $c = 1$.

Así $a_n = 2^n - 1$

5.5.3. Sucesión de Fibonacci

La sucesión de Fibonacci se define con la relación $F_{n+2} = F_{n+1} + F_n$, con $F_0 = 0, F_1 = 1$. Que da la ecuación característica $r^2 - r - 1$ con raíces $r_{12} = (1 \pm \sqrt{5})/2$. Por lo que la solución tienen la forma $F_n = c_1 \left(\frac{1+\sqrt{5}}{2}\right) + c_2 \left(\frac{1-\sqrt{5}}{2}\right)$. Finalmente $F_n = \frac{1}{\sqrt{5}} \left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n \right]$ $n \geq 0$.

6
Gráficas

Sea V un conjunto finito no vacío y $E \subseteq V \times V$, el par (V, E) es llamada gráfica dirigida, donde V es el conjunto de vértices y E es el conjunto de aristas.

En el caso de que $(a, b) \in E$ se reemplace por $\{a, b\}$, entonces la gráfica no tiene dirección.

Sea $G = (V, E)$ una gráfica sin dirección y $a, b \in V$ un camino de a a b, es una sucesión de vértices tales que $a = x_0, x_1, ..., x_n = b$ donde cada $e_i = \{x_{i-1}, x_i\}$ esta en E. La longitud del camino es el número de aristas del camino. Si $a = b$ se llama camino cerrado, de lo contrario es abierto.

Sea $G = (V, E)$ una gráfica sin dirección y $a - b$ un camino:

1. Si no se repiten aristas, el camino se llama recorrido, si el camino es cerra do el camino se llama circuito.
2. Si no se repiten vértices, el camino se llama camino simple, si el camino es cerrado se llama ciclo.

Vértices repetidos	Aristas Repetidas	abierto	cerrado	nombre
Si	Si	Si		Camino abierto
Si	Si		Si	Camino cerrado
Si	No	Si		Recorrido
Si	No		Si	Circuito
No	No	Si		Camino simple
No	No		Si	Ciclo

1. Una gráfica es conexa si para cualquiera dos puntos existe un camino que los une.
2. Sea V un conjunto de n vértices, la gráfica K_n es aquella que contiene todas las aristas $\{a, b\}$ con $a, b \in V, a \neq b$.
3. Sea G una gráfica de n vértices, el complemento de G, $\overline{G}$, es subgráfica de K_n que tiene todos los n vértices de G, y todas las aristas que no están en G.

4. Sean $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ dos gráficas sin dirección. Una función $f : V_1 \to V_2$ se llama isomorfismo si:
   a) f es biyectiva.
   b) Para todo $a, b \in V_1$ $\{a, b\} \in V_1$ si y sólo si $\{f(a), f(b)\} \in E_2$.
5. El grado de un vértice a es el número de aristas que inciden en a y denotado por $gr(a)$.

6.1. Matrices de Adyacencia e Incidencia

6.2. Caminos eulerianos

Sea $G = (V, E)$ una gráfica sin dirección, entonces $\sum_{v \in V} gr(v) = 2|E|$.

Sea $G = (V, E)$ una gráfica sin dirección, decimos que G tiene un circuito euleriano, si existe un circuito que recorre cada arista de la gráfica exactamente una vez. Si existe un recorrido abierto que recorre cada arista exactamente una vez, se llama recorrido euleriano.

Sea $G = (V, E)$ una gráfica sin dirección. Entonces, G tiene un circuito euleriano si y sólo si G es conexo y todo vértice de G tiene grado par.

Sea $G = (V, E)$ una gráfica sin dirección. Entonces, G tiene un recorrido euleriano si y sólo si G es conexo y tiene exactamente dos vértice de grado impar.

6.3. Gráficas planas

Una gráfica es plana si podemos dibujar G en un plano de modo que sus aristas no se intersecten, salvo en los vértices.

Una gráfica G es bipartita, si $V = V_1 \cup V_2$, $V_1 \cap V_2 = \emptyset$ y cada arista de G es de la forma $\{a, b\}$ donde $a \in V_1$, $b \in V_2$. Si $|V_1| = m, |V_2| = n$, se llama gráfica bipartita completa y se denota $K_{m,n}$.

Sean una gráfica G, una subdivisión elemental de G resulta de sustituir la arista $\{a, b\}$ por $\{a, c\}, \{c, b\}$. Dos gráficas G_1, G_2 son homeomorfas si son isomorfas o si ambas se pueden obtener de la misma gráfica H por medio de subdivisiones elementales.

Teorema 1 *Teorema de Kuratowski: una gráfica no es plana si y sólo si contiene una subgráfica que es homeomorfa a K_5 o $K_{3,3}$.*

Teorema 2 *Teorema de Euler: Sea G una gráfica plana conexa con $|V| = a$ y $|E| = b$, sea r el número de regiones en el plano determinadas por una inmersión de G (dibujo en el plano). Entonces $a - b + r = 2$.*

6.4. Caminos hamiltonianos

Si G es una gráfica con $|G| \geq 3$, decimos que G tiene un ciclo hamiltoniano si existe un ciclo que contenga todos los vértices de G. Un camino hamiltoniano es un camino simple que contiene todos los vértices de G. Observe que aqui no se repiten ni vértices ni aristas.

Si G es una gráfica con $|G| \geq 3$, decimos que G tiene un ciclo hamiltoniano si existe un ciclo que contenga todos los vértices de G. Un camino hamiltoniano es un camino simple que contiene todos los vértices de G. Observe que aqui no se repiten ni vértices ni aristas.

Teorema 3 *Sea G una gráfica, $|V| = n \geq 2$, si $gr(x) + gr(y) \geq n - 1$ para todos los vértices $x, y \in V$ $x \neq y$, entonces G tiene un camino hamltoniano.*

Corolario 1 *Sea G una gráfica, $|V| = n \geq 2$, si $gr(x) \geq (n-1)/2$ para todo $x \in V$, entonces G tiene un camino hamiltoniano.*

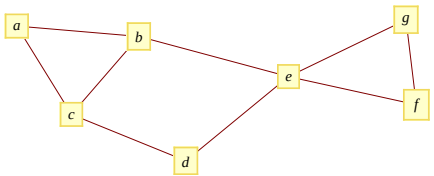
Teorema 4 *Sea G una gráfica, $|V| = n \geq 3$, si $gr(x) + gr(y) \geq n$ para todos los vértices $x, y \in V$ no adyacentes , entonces G tiene un ciclo hamltoniano.*

Corolario 2 *Sea G una gráfica, $|V| = n \geq 3$, si $gr(x) \geq n/2$ para todo $x \in V$, entonces G tiene un ciclo hamiltoniano.*

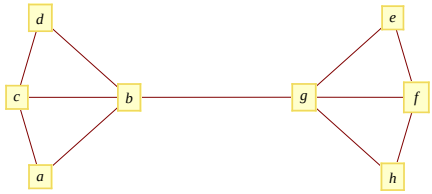
Corolario 3 *Sea G una gráfica, $|V| = n \geq 3$, y $|E| \geq \binom{n-1}{2} + 2$, entonces G tiene un ciclo hamiltoniano.*

6.5. Ejercicios

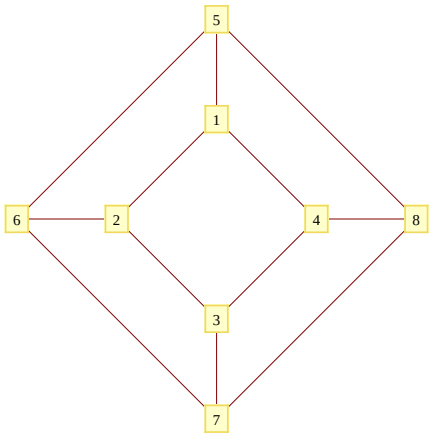
1. Para la siguiente gráfica, determinar si es posible, un camino de b a d que no sea recorrido, un recorrido $b - d$ que no sea camino simple, un camino simple $b - d$, un camino cerrado $b - b$ que no sea un circuito, un circuito $b - b$ que no sea un ciclo, y un ciclo de $b - b$.



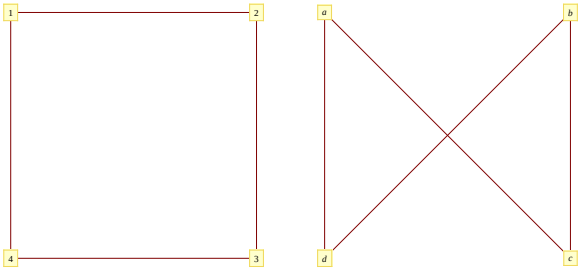
2. Para la siguiente gráfica, determinar si es posible, un camino de b a h que no sea recorrido, un recorrido $b-h$ que no sea camino simple, un camino simple $a-f$, un camino cerrado $a-a$ que no sea un circuito, un circuito $b-b$ que no sea un ciclo, y un ciclo de $b-b$. Determinar, cuántos caminos simples existen entre $a-h$, cuántos de ellos son de longitud 5.



3. Para la siguiente gráfica determinar, sí es posible, un camino de 5 a 7 que no sea recorrido, un recorrido $2-8$ que no sea camino simple, un camino simple $5-3$, un camino cerrado $1-1$ que no sea un circuito, un circuito $5-5$ que no sea un ciclo, y un ciclo de $2-2$. Determinar, cuántos caminos simples existen entre $5-7$.



4. Mostrar que las siguientes gráficas son isomorfas (trivial).



5. Mostrar qué gráficas son isomorfas (Fig 1 y Fig 2 no son isomorfas, Fig 3 si lo es a Fig 1).

Fig 1):

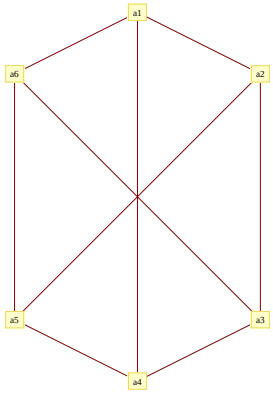


Fig 2):

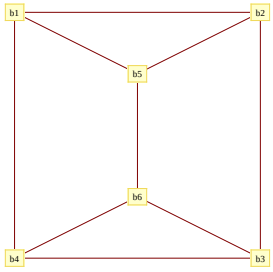
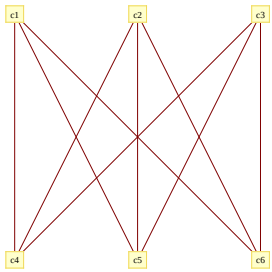


Fig 3):



7
Árboles