EXAMEN MATEMÁTICA DISCRETA JUNIO 2015

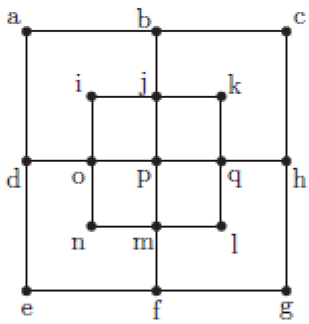
1. Utiliza o teorema chinés dos restos para resolver o seguinte sistema de congruencias e determina cantas solucións teñen valor absoluto entre 150 e 2015.

$$x \equiv 2 (mod\, 3)$$
$$x \equiv 1 (mod\, 4)$$
$$x \equiv 3 (mod\, 5)$$

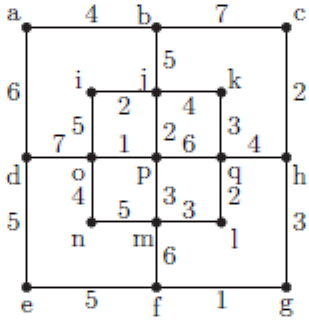
2. Determina o número de 5 caracteres ASCII que conteñen algunha vez o caracter "@".
   Nota: O número de caracteres ASCII é 2^7

3. a) Da unha relación de recurrencia para calcular o número de cadeas de bits de lonxitude n con dous ceros consecutivos.
   b) Cales son as condicións iniciais?
   c) Calcula cantas cadeas de lonxitude 7 conteñen dous ceros consecutivos.

4. Dado o seguinte grafo G



(a) Comprobar o teorema de apertón de mans. Calcular a sucesión de graos do grafo G.
(b) É bipartito? Cal é o número crómatico do grafo G?
(c) É conexo? Describir un camiño simple de lonxitude 6. É isomorfo ao grafo K_5?
(d) É euleriano? É hamiltoniano?
(e) É plano? Comprobar a fórmula de Euler para o grafo G.
(f) Calcular unha árbore xeradora minimal de G usando o algoritmo de Kruskal, sendo os pesos do grafo os que se indican a continuación



Examen Matemática Discreta 13-14

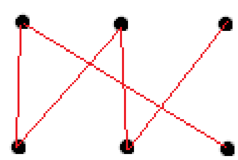
1.
   a) Existe el inverso de 26 mod 265? En caso afirmativo, calcúlalo.
   b) Tiene solución la congruencia 26x≡mod 165? En caso afirmativo calcular las soluciones enteras entre -300 y 300.

2.
   a) Cuantas soluciones tiene la ecuación $x_1+x_2+x_3+x_4=8$ donde x_1, x_2, x_3, x_4 son enteros no negativos?
   b) Probar que entre cualquier grupo de 13 números enteros (no necesariamente consecutivos), hay por lo menos 2 que den el mismo resto cuando se dividen por 12.

3.
   a) Determinar las soluciones de: $an = 6a_{n-1} + 7a_{n-2}$
   b) Determinar la solución del apartado anterior con las condiciones iniciales $a_1=8$ y $a_2=48$.

4. Ejercicio típico de grafos (mirar años anteriores).

5. Justificar razonadamente:
   a) $f(x) = x \log(x)$ es O de (x^2)? Y $g(x)= x^4/2$ es O de (x^2)?
   b) Evaluar -97 mod 141.
   c) Enontrar inverso de 4 mod 9.
   d) Cuantas cadenas de bits de longitud 6 empiezan y acaban con un 1?.
   e) Dar una definición recursiva de (n^2), n=1, 2, 3...
   f) Es el siguiente grafo un árbol?:



Matemática Discreta

1. De dous números, n e m, sábese que os seus restos ó dividilos entre 29, 30 e 31 son, respectivamente, (3,2,1) e (1,2,5). Calcular o produto nxm sabendo que é un número menor que 29x30x31.

2. De cantas maneiras se poden seleccionar 5 billetes dunha caixa rexistradora que contén billetes de 5 €, 10 €, 50 €, 100 €, 200 € e 500 €? (A orde non se ten en conta, hai polo menos 5 billetes de cada tipo e os do mesmo tipo son indistinguibles)

3. a)Determinar as solucións da relación de recorrencia: $a_n = -5 \cdot a_{n-1} - 6 \cdot a_{n-2} + 42 \cdot 4^n$.
   b) Determinar a única solución coas condicións iniciais $a_1 = 56$ e $a_2 = 278$.

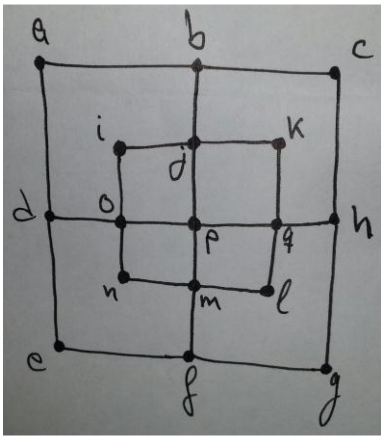
4. a) Comprobar o teorema do apertón de mans.

b) Calcular a sucesión de graos do grafo G.

c) É bipartito? É isomorfo ao K_5?

d) É conexo? É euleriano? É hamiltoniano?

e) É plano? Comprobar a fórmula de Euler para o grafo G.



Escola Técnica Superior de Enxeñaría

ETSE	Curso 21/22	Apelidos e Nome: ______________________
Matemática Discreta	1ª Op.	Data: 16/01/2022

Indícase na cabeceira do exame que se deben **xustificar todas as respostas**

1. **(2 puntos)** Resolve as seguintes cuestións:

   (a) **(1 punto)** Atopar o enteiro positivo máis pequeno que dea restos $1, 3$ e 5 cando se divide por $5, 7$ e 9, respectivamente.

   (b) **(1 punto)** Sabendo que o número $3x5647y2_{(8)}$ é múltiplo 7 e de 9, respectivamente. **O número atopase expresado en base 8**. Calcular x e y.

2. **(2 puntos)** Responde ás seguintes cuestións:

   (a) **(1 punto)** Sexa $\{a_1, a_2, a_3, ..., a_{n-1}, a_n\}$ un conxunto de nove números naturais cuxa suma é 85, Probar que hai necesariamente cartro números cuxa suma é polo menos 38.

   (b) **(0.5 puntos)** De cantas formas se poden repartir 20 exemplares dun mesmo libro entre seis persoas A, B, C, D, E, F se se coñece que A e B deben recibir alomenos 3 exemplares e C e D deben recibir dous exemplares.

   (c) **(0.5 puntos)** De cantas formas se poden repartir 20 exemplares dun mesmo libro entre seis persoas A, B, C, D, E, F nas mesmas condicións que o apartado anterior sabendo que A non pode recibir máis de 10 exemplares.

3. **(2 puntos)** Resolve a seguinte ecuación de recorrencia:

   (a) **(1 punto)** Sexa b_n o número de cadeas de n bits que conteñen tres ceros consecutivos. Calcular unha ecuación de recorrencia para b_n. Da as condicións iniciais Non fai falta resolvela.

   (b) **(1 punto)** Considera a relación de recorrencia $a_n = 4a_{n-1} - 4a_{n-2}$. Cal é a solución xeral? É a sucesión $a_n = 4$ solución da ecuación de recorrencia? É a sucesión $a_n = n2^{n+1}$.

4. **(2 puntos)** Xustificar razonadamente as seguintes cuestións

   (a) **(0.4 puntos)** Ordenar da meneira de que cada función sexa $\mathcal{O}$ (Big-$\mathcal{O}$) da seguinte:
   $\boxed{f(n) = 365nlog_8n + n^3 + 2000n}$ $\boxed{g(n) = n^2log_2n + n(log_8n)^3}$ $\boxed{h(n) = 1000nlog_8n + n^2(log_2n)^3}$

   (b) **(0.4 puntos)** Cántos números teñen inverso multiplicativo (ou unidades) en $\mathbb{Z}/20200\mathbb{Z}$, é dicir, no reloxo de 20200 horas.

   (c) **(0.4 puntos)** O número total de aplicacións inxectivas do conxunto $\{1, 2, 3\}$ nun conxunto A é de 210 posibilidades. Cántos elementos ten A?

   (d) **(0.4 puntos)** Sexa G un grafo simple con 9 vértices. Probar que se G ten 29 arestas entón é conexo.

   (e) **(0.4 puntos)** Todo subgrafo 2-regular de K_4 é isomorfo a K_3.

5. **(2 puntos)** Dado o seguinte grafo responder ás seguintes cuestións:

   (a) **(0.5 puntos)** É bipartito? É plano?

   (b) **(0.5 puntos)** É euleriano? É semieuleriano? No caso afirmativo, construír un circuito ou camiño.

   (c) **(0.5 puntos)** É hamiltoniano? No caso afirmativo construír un circuito.

   (d) **(0.5 puntos)** Calcular unha árbore xeradora de peso minimal empregando o algoritmo de Prim (indicando todos os pasos), sendo os pesos do grafo os que se indican a continuación:

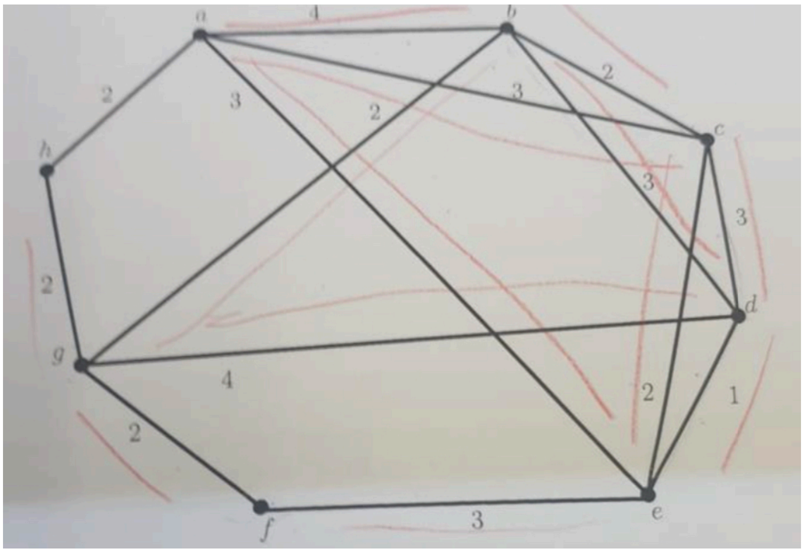


Figura 1: Grafo que foi proposto no exame

SOLUCIONES PRUEBA DE MATEMÁTICA DISCRETA

1.A. Sabiendo que la clave pública es $n = 10553$ ($n = 173 \cdot 61$) y $e = 191$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.

Solución:
Cálculo de la clave privada d: $\phi(n) = \phi(10553) = (173-1)\cdot(61-1) = 172\cdot 60 = 10320$.
d es el inverso multiplicativo de $e = 191$ módulo $\phi(n) = 10320$.
$\gcd(10320, 191) = 1$, ya que

$$\begin{array}{r|l} 10320 & 191 \\ \cline{2-2} 6 & 54 \end{array} \qquad\qquad \begin{array}{r|l} 191 & 6 \\ \cline{2-2} 5 & 31 \end{array} \qquad\qquad \begin{array}{r|l} 6 & 5 \\ \cline{2-2} 1 & 1 \end{array}$$

$6 = 10320 - 54 \cdot 191, \qquad 5 = 191 - 31 \cdot 6, \qquad 1 = 6 - 1 \cdot 5.$

Así:

$$\begin{aligned} 1 &= 6 - 5 = 6 - (191 - 31 \cdot 6) = 32 \cdot 6 - 191 = 32 \cdot (10320 - 54 \cdot 191) - 191 \\ &= 32 \cdot 10320 - 1728 \cdot 191 - 191 = 32 \cdot 10320 - 1729 \cdot 191 \end{aligned}$$

Por lo tanto, el inverso multiplicativo de 191 módulo 10320 es -1729, pero

$$-1729 \equiv 8591 \bmod 10320.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{191} \bmod 10533.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{8591} \bmod 10533.$$

2.A. (a) ¿El número 3914230221 es divisible por 11? ¿Y por 99? (Razonar sin hacer la división !!!)

Solución:
3914230221 es divisible por 11 si, y solo si,

$$-3 + 9 - 1 + 4 - 2 + 3 - 0 + 2 - 2 + 1 \equiv 0 \bmod 11 \iff 19 - 8 = 11 \equiv 0 \bmod 11$$

Por otro lado, es divisible por 99 si, y solo si, es divisible por 11 y 9:
3914230221 es divisible por 9 si, y solo si,

$$3 + 9 + 1 + 4 + 2 + 3 + 0 + 2 + 2 + 1 \equiv 0 \bmod 11 \iff 27 \equiv 0 \bmod 9$$

Por lo tanto 3914230221 es divisible por 99.

(b) ¿La función $30x^2 - 7x^3 \log(x)$ es $\mathcal{O}(x^2)$?

Solución:
No es $\mathcal{O}(x^2)$ ya que $x^3 \notin \mathcal{O}(x^2)$.

(c) Escribir el número $1051_{(6)}$ expresado en base 6 en base 8.

Solución:
$1051_{(6)} = 1 \cdot 6^3 + 0 \cdot 6^2 + 5 \cdot 6^1 + 1 = 247$ expresado en base 10.

$$\begin{array}{l|l} 247 & 8 \\ \hline 7 & 30 \end{array} \qquad \begin{array}{l|l} 30 & 8 \\ \hline 6 & 3 \end{array}$$

Así, el número $1051_{(6)}$ en base 8 es $367_{(8)}$.

(d) ¿Qué enteros positivos menores que 28 tienen inverso multiplicativo en $\mathbb{Z}/28\mathbb{Z}$?

Solución:
$\phi(28) = \phi(2^2) \cdot \phi(7) = 2 \cdot 6 = 12$ elementos tienen inverso multiplicativo en $\mathbb{Z}/28\mathbb{Z}$, que son los números x tales que $\gcd(x, 28) = 1$, es decir,

$$1, 3, 5, 9, 11, 13, 15, 17, 19, 23, 25, 27.$$

1.B. Sabiendo que la clave pública es $n = 9853$ ($n = 167 \cdot 59$) y $e = 187$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.

Solución:
Cálculo de la clave privada d: $\phi(n) = \phi(9853) = (167-1)\cdot(59-1) = 166\cdot 58 = 9628$.
d es el inverso multiplicativo de $e = 187$ módulo $\phi(n) = 9628$.
$\gcd(9628, 187) = 1$, ya que

$$\begin{array}{r|l} 9628 & 187 \\ \hline 91 & 51 \end{array} \qquad \begin{array}{r|l} 187 & 91 \\ \hline 5 & 2 \end{array} \qquad \begin{array}{r|l} 91 & 5 \\ \hline 1 & 18 \end{array}$$

$91 = 9628 - 51 \cdot 187, \qquad 5 = 187 - 2 \cdot 91, \qquad 1 = 91 - 18 \cdot 5.$

Así:

$$\begin{aligned} 1 &= 91 - 18 \cdot 5 = 91 - 18 \cdot (187 - 2 \cdot 91) = 37 \cdot 91 - 18 \cdot 187 \\ &= 37 \cdot (9628 - 51 \cdot 187) - 18 \cdot 187 = 37 \cdot 9628 - 1905 \cdot 187 \end{aligned}$$

Por lo tanto, el inverso multiplicativo de 187 módulo 9628 es -1905, pero

$$-1905 \equiv 7723 \bmod 9628.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{187} \bmod 9853.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{7723} \bmod 9853.$$

2.B. (a) ¿El número 221456838972 es divisible por 11? ¿Y por 3? ¿Y por 33? (Razonar sin hacer la división !!!)

Solución:
221456838972 es divisible por 11 si, y solo si,

$$-2+2-1+4-5+6-8+3-8+9-7+2 \equiv 0 \bmod 11 \Longleftrightarrow 26 - 31 = -5 \equiv 6 \not\equiv 0 \bmod 11$$

Así, no es divisible por 11.

221456838972 es divisible por 3 si, y solo si,

$$2+2+1+4+5+6+8+3+8+9+7+2 \equiv 0 \bmod 3 \Longleftrightarrow 57 \equiv 12 \equiv 3 \equiv 0 \bmod 3$$

Por otro lado, es divisible por 33 si, y solo si, es divisible por 11 y 3, así 221456838972 no es divisible por 33.

(b) ¿La función $26x^3 - 693x^2\log(x)$ es $\mathcal{O}\big(x^3\big)$?

Solución:
Es $\mathcal{O}\big(x^3\big)$ ya que x^3 y x^2 pertenecen a $\mathcal{O}\big(x^3\big)$.

(c) Escribir el número $1342_{(5)}$ expresado en base 5 en base 7.

Solución:
$1342_{(5)} = 1 \cdot 5^3 + 3 \cdot 5^2 + 4 \cdot 5^1 + 2 = 222$ expresado en base 10.

$$\begin{array}{r|l} 222 & 7 \\ \hline 5 & 31 \end{array} \qquad \begin{array}{r|l} 31 & 7 \\ \hline 3 & 4 \end{array}$$

Así, el número $1342_{(5)}$ en base 7 es $435_{(7)}$.

(d) ¿Qué enteros positivos menores que 36 tienen inverso multiplicativo en $\mathbb{Z}/36\mathbb{Z}$?

Solución:
$\phi(36) = \phi(2^2) \cdot \phi(3^2) = 2 \cdot 6 = 12$ elementos tienen inverso multiplicativo en $\mathbb{Z}/36\mathbb{Z}$, que son los números x tales que $\gcd(x, 36) = 1$, es decir,

$$1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35.$$

MATEMÁTICA DISCRETA **21/1/2021**

1. (a) Que enteiros positivos menores que 32 teñen inverso multiplicativo en $\mathbb{Z}/32\mathbb{Z}$? "*$\mathbb{Z}/32\mathbb{Z}$ é o reloxo de 32 horas*".

$32 = 2^5$. Tienen inverso multiplicativo los enteros a tales que $\gcd(a, 32) = 1$, es decir los números impares. Hay 16 enteros positivos menores que 32 que tienen inverso multiplicativo: $1, 3, 5, \ldots, 27, 29, 31$.

(b) Enunciar e probar o criterio de divisibilidade por 11. Que cifra é X na igualdade 14!=871X8291200?

El enunciado y la prueba está hecha en clase.
14!=871X8291200 es múltiplo de todos los números menores o iguales que 14. En particular, podéis aplicar los criterios de divisibilidad del 9 o del 11. Se obtiene que $X = 7$.

(c) Escribe o número $1241_{(6)}$ expresado en base 6 en base 9.

$1241_{(6)} = 313 = 377_{(9)}$.

2. (a) Se se seleccionan 101 enteiros entre $\{1, 2, \ldots, 200\}$, probar que polo menos dous deles son coprimos ou primos entre si.

Consideramos las 100 cajas $\{1, 2\}$, $\{3, 4\}$, $\{5, 6\}$,, $\ldots$, $\{197, 198\}$, $\{199, 200\}$. Si se seleccionan 101 números, por el principio del palomar $\lceil \frac{101}{100} \rceil = 2$, al menos dos de esos números están en el misma caja. Esos dos números son coprimos entres sí.

(b) (i) De cantas formas se poden repartir tres exemplares dun mesmo libro entre oito nenas se ningunha delas pode recibir máis dun?

$C(8, 3) = \binom{8}{3} = \frac{8!}{5!\ 3!} = 56.$

(ii) De cantas formas se poden repartir tres exemplares dun mesmo libro entre oito nenas se calquera delas pode recibir calquera número de exemplares?

$CR(8, 3) = \binom{8+3-1}{3} = \binom{10}{3} = \frac{10!}{7!\ 3!} = 120.$

(iii) De cantas formas se poden repartir oito exemplares dun mesmo libro entre tres nenas se cada unha delas debe recibir, polo menos, un exemplar?

$CR(3, 5) = \binom{3+5-1}{5} = \binom{7}{5} = \frac{7!}{5!\ 2!} = 21.$

3. (a) Ao comezo do primeiro ano existen 2 cabras nunha illa. O número de cabras duplícanse todos os anos por reprodución e ao finalizar o ano n-ésimo son eliminadas n cabras. Determinar unha relación de recorrencia para o número de cabras ao principio do ano n-ésimo. Cales son as condicións iniciais? De que tipo é a relación de recorrencia? Cantas cabras hai ao principio do cuarto ano?

(**Nota**: *Non fai falta resolver a relación de recorrencia*)

$a_n = 2a_{n-1} - (n-1)$. Condición inicial $a_1 = 2$. Es una RRLnHCC: relación de recurrencia lineal no homogénea con coeficientes constantes. Al principio del cuarto año hay 5 cabras.

(b) Considera a relación de recorrencia $a_n = -a_{n-1} + 2a_{n-2}$. Cal é a solución xeral? É a sucesión $a_n = 1$ solución da relación de recorrencia? E a sucesión $a_n = 2^n$?

La ecuación característica es $r^2 + r - 2 = 0$, con soluciones $r_1 = 1$ y $r_2 = -2$. Por lo tanto la solución general es $a_n = \alpha_1(1)^n + \alpha_2(-2)^n$.
1 es solución, ya que tomando $\alpha_1 = 1$ y $\alpha_2 = 0$, obtenemos que $a_n = 1$.
Otra forma, comprobando que es solución directamente en la ecuación de recurrencia $a_n = -a_{n-1} + 2a_{n-2}$: $\quad 1 = -1 + 2 \cdot 1$.
2^n no es solución de la ecuación de recurrencia $a_n = -a_{n-1} + 2a_{n-2}$:

$$2^n = -2^{n-1} + 2 \cdot 2^{n-2} = -2^{n-1} + 2^{n-1} = 0.$$

4. Xustificar razoadamente as seguintes cuestións:

(a) Ordenar as funcións de tal maneira que cada función sexa big-$\mathcal{O}$ da seguinte:
$f(n) = 2021\, n^2 + 2021^{10}, \qquad g(n) = 2021\, n \log(n^3), \qquad h(n) = 2021\, \sqrt[4]{n}$

$f \in \mathcal{O}(n^2), \qquad g \in \mathcal{O}(n \log(n)), \qquad h \in \mathcal{O}(n^{1/4})$.
Por lo tanto, $h \in \mathcal{O}(g), \qquad g \in \mathcal{O}(f)$.

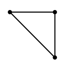
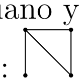
(b) Encontrar un inverso de 11 módulo 186.

El inverso es 17.

(c) Utilizando un alfabeto de 26 letras, cantas palabras de 4 letras empezan pola letra **A** ou non a conteñen?

$26^3 + 25^4$.

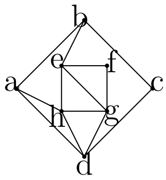
(d) Pon un exemplo dun grafo euleriano que sexa hamiltoniano e outro exemplo dun grafo non euleriano que non sexa hamiltoniano.

Muchos!!! Por ejemplo, es euleriano y hamiltoniano K_3: 
No es euleriano ni hamiltoniano: 

(e) Todo grafo simple, bipartito completo é hamiltoniano?

$K_{m,n}$ es hamiltoniano si y solo si $n = m$.

5. Dado o seguinte grafo G



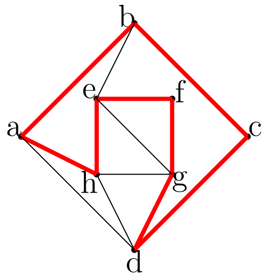
(a) É euleriano? É semieuleriano? No caso afirmativo, construír un circuíto ou un camiño.

No es euleriano, ya que $\partial(a) = \partial(b) = 3$. Es semieuleriano, ya que el resto de los vértices tienen grado par. Un camino euleriano es (de muchos posibles que tienen que empezar y terminar en los vértices de grado impar, se puede construir usando el algoritmo de Fleury):

$$abcdgfeghdaheb$$

(b) É hamiltoniano? No caso afirmativo, construír un circuíto.

Es hamiltoniano ya que tiene circuitos hamiltonianos. Un circuito hamiltoniano es



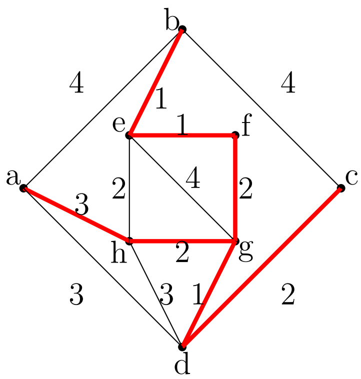
(de muchos posibles) $abcdgfeha$:

(c) Calcular unha árbore xeradora minimal de G usando o algoritmo de Kruskal, sendo os pesos do grafo os que se indican a continuación

Primero se consideran los ejes de menor peso, siempre que no formen un ciclo hasta formar un árbol. Una solución posible es:

- Ejes de peso 1: be, ef, dg.
- Ejes de peso 2: fg, gh, dc.
- Ejes de peso 3: ah.

Es un árbol generador de peso minimal 12.



.

28 – Xuño - 2019

Transcrito por MAD, de Informáticas MAD

Neste maravilloso día de verán uns poucos afortunados e afortunadas puidemos degustar o exame elavorado polos profesores da materia para o control extraordinario, coma nós, da materia. Neste, entraron preguntas moi curiosas de dificil resolución, polo menos á hora de resolver o exame.

Cada pregunta vale 2 ptos.

1- a) Resolver a congruencia lineal 17*x = 3 (mod 19)
   b) Que número deixa como resto 1 ao dividilo por 2, resto 2 ao dividilo por 3 e resto 3 ao dividilo por 7.

2- Considera os números enteiros positivos de catro cifras (1000 <= x <= 9999).

a) Cantos hai divisibles por 9?
b) Cantos non teñen díxitos repetidos?
c) Cales non son divisibles por 3?
d) Cales son divisibles por 5 ou por 7?
e) Cales son divisibles por 5 e por 7?
f) Cales son divisibles por 5 e non por 7?

3- Resolver:

a) X1 + X2 + X3 = 30
b) Considerar X1 >= 3
c) Considerar X1 <= 7 e X2 <= 5

4- Transmitimos mensaxes por unha canle de comunicacións usando dous tipos de sinais. A transmisión dun sinal dos do primeiro tipo ocupa 1 microsegundo e as do segundo tipo ocupa 2 microsegundos.

a) Determinar unha relación de recorrencia para o número de mensaxes diferentes formadas por secuencias de sinais destes dous tipos que se poden enviar en n microsegundos.
b) Condicións iniciais
c) Cantas mensaxes diferentes se poden transmitir en 10 microsegundos?
d) Cantas mensaxes diferentes se poden transmitir en n microsegundos?

5- Para que n pode existir un grafo coa seguinte sucesión de graos?

[2, 2, 3, 3, 4, 4, …, n, n]

a) Cantas arestas tería este grafo?
b) Podería ser algún destes grafos euleriano?
c) Cales, sen ser eulerianos, poderían conter camiños eulerianos?
d) Para que valores de n o grafo non podería ser á vez simple, conexo e plano?

Enxeñaría Informática USC — Matemática Discreta

Transcrito por $\Delta\Psi$

Xaneiro 2019

1. (2,5 puntos) O teorema pequeno de Fermat enuncia que se p é un número primo e a é un número enteiro non divisible entre p, entón $a^{p-1} \equiv 1 \pmod p$
   (a) Utilizar este teorema para calcular $3^{302} \mod 5$, $3^{302} \mod 7$ e $3^{302} \mod 11$
   (b) Usar os resultados do apartado anterior e o teorema chinés dos restos para calcular $3^{302} \mod 385$. Observar que $385 = 5 \cdot 7 \cdot 11$.
2. (2,5 puntos)
   (a) Cantas cadeas hai de 8 bits?
   (b) Cantas cadeas de 8 bits comezan ou rematan por 1?
   (c) Cantas cadeas de 8 bits non conteñen un número par de ceros?
3. (2,5 puntos) Considerar a relación de recorrencia linear $a_n = 9a_{n-2} + 3^n$.
   (a) Probar que $a_n = \frac{n}{2}3^n$ é unha solución desta relación de recorrencia.
   (b) Determinar tódalas solucións desta relación de recorrencia.
   (c) Determinar a solución que verifica $a_0 = 0$ e $a_1 = \frac{5}{2}$.
4. (2,5 puntos) Sendo $K_{3,4}$ o grafo bipartito completo, razoar a resposta a cada unha das seguintes preguntas.
   (a) Cal é a sucesión de graos de $K_{3,4}$?
   (b) Cal é o índice cromático de $K_{3,4}$?
   (c) É $K_{3,4}$ hamiltoniano?
   (d) É $K_{3,4}$ euleriano?
   (e) É $K_{3,4}$ isomorfo ao grafo completo K_7?

SOLUCIONES

1. (a) Existe o inverso de 19 módulo 141? En caso afirmativo, calculalo.
(b) Ten solucións a congruencia $19x \equiv 3 \bmod 141$? En caso afirmativo, calcular as solucións enteiras que hai entre –300 e 300.

Solución.
(a) Tiene inverso, ya que $\gcd(19, 141) = 1$. $1 = 52 \cdot 19 + (-7) \cdot 141$. Así, inverso de 19 es 52.
(b) $19x \equiv 3 \bmod 141 \Leftrightarrow x \equiv 3 \cdot \frac{1}{19} \equiv 3 \cdot 52 = 156 \equiv 15 \bmod 141$.
Otras soluciones son: $141 + 15 = 156$, $\quad 2 \cdot 141 + 15 = 297$,
$-1 \cdot 141 + 15 = -126 \quad - 2 \cdot 141 + 15 = -267$.

2. De cantas formas pódense colocar 6 bólas en tres recipientes en cada un dos seguintes casos?
(a) Cada bóla é dunha cor diferente.
(b) Todas as bólas son iguais. (2 puntos)

Solución.
(a) Se as bólas son todas diferentes a cada unha das 6 bólas asignámoslle unha das 3 eleccións posibles.
Tamén se pode pensar como cadeas de lonxitude 6 formadas con 1, 2 e 3.
VR(3,6)$= 3^6 = 729$.
(b) Se as bólas son iguais, hai que saber cantas bólas haberá en cada recipiente, é dicir, o número de solucións enteiras non negativas de

$$x_1 + x_2 + x_3 = 6.$$

CR(3,6)$= \binom{3+6-1}{6} = \binom{8}{6} = \frac{8!}{6!2!} = \frac{8 \cdot 7}{2} = 28$.

3. (a) Buscar unha relación de recorrencia para o número de cadeas de bits de lonxitude n que conteñen tres ceros consecutivos. Cales son as condicións iniciais?
(b) Resolver a relación de recorrencia $a_n = 5a_{n-1} - 6a_{n-2}$ para $n \geq 2$ coas condicións iniciais $a_0 = 1$, $a_1 = 0$.

Solución.
(a) Sea a_n el número de cadenas de n bits que contienen 3 ceros consecutivos.
- O bien empiezan por 1, seguido de una cadena de longitud $n - 1$ con 3 ceros consecutivos.
- O bien empiezan por 0. En este caso puede ocurrir:
  - 01, seguido de una cadena de longitud $n-2$ con 3 ceros consecutivos.
  - 001, seguido de una cadena de longitud $n-3$ con 3 ceros consecutivos.
  - 000, seguido de una cadena arbitraria de longitud $n - 3$.

Por lo tanto, $a_n = a_{n-1} + a_{n-2} + a_{n-3} + 2^{n-3}$.
(b) La ecuación característica es $r^2 - 5r + 6 = 0$. Las raíces son $r_1 = 3$ y $r_2 = 2$.

La solución general de la ecuación es $a_n = \alpha_1 3^n + \alpha_2 2^n$. $\left\{\begin{array}{rcl} 1 & = & \alpha_1 + \alpha_2 \\ 0 & = & 3\alpha_1 + 2\alpha_2 \end{array}\right.$
Así, tenemos: $\alpha_1 = -2,\ \alpha_2 = 3$. Por lo tanto la solución es $a_n = -2 \cdot 3^n + 3 \cdot 2^n$.

4. Un grafo dise libre de triángulos se non ten circuítos de lonxitude 3. Sexa G un grafo simple, plano e libre de triángulos, con n vértices, $n \geq 3$. Proba que G ten, como máximo, $2n-4$ arestas. Demostra, ademais, que existe un vértice de grao menor ou igual que 3.

Solución.
Como G no contiene circuitos de longitud 3, las regiones están limitadas por ciclos de longitud al menos 4, por tanto: $4r \leq 2|E|$, donde r denota el número de regiones del grafo G. Por otro lado, por el Teorema de Euler, $r = |E| - |V| + 2$, por tanto

$$4r = 4|E| - 4|V| + 8 \leq 2|E| \Rightarrow 2|E| \leq 4|V| - 8 \Rightarrow |E| \leq 2|V| - 4.$$

Para comprobar que, en estas condiciones, existe un vértice de grado menor o igual que 3, supongamos, por el contrario, que todos los vértices son de grado estrictamente mayor que 3 (esto es, $\partial(v) \geq 4, \forall v \in V$). Utilizando el Lema del apretón de manos se tendría

$$2|E| = \sum_{v \in V} \partial(v) \geq 4|V|; \text{ lo que contradice } |E| \leq 2|V| - 4.$$

5. Xustificar razoadamente as seguintes cuestións:
(a) A función $f(x) = 2x^2 + x^3 \log(x)$ é $\mathcal{O}\big(x^3\big)$?
(b) Cantos enteiros positivos menores que 30 son primos relativos con 30?
(c) Cantas cadeas diferentes poden facerse coas letras de $AARDVRAK$, usando todas as letras, se todas as tres A teñen que ser consecutivas?
(d) Un grafo bipartito completo $K_{m,n}$ euleriano sempre é hamiltoniano?

Solución.
(a) No, ya que $\log(x)$ es $\mathcal{O}\big(x\big)$, es decir, $\log(x)$ crece menos que x.
La función sería $\mathcal{O}\big(x^4\big)$.
(b)
$$\phi(30) = \phi(2 \cdot 3 \cdot 5) = \phi(2) \cdot \phi(3) \cdot \phi(5) = 1 \cdot 2 \cdot 4 = 8.$$
(c) Consideramos las tres A consecutivas $AAARDVRK$, es dedir, $\boldsymbol{A}RDVRK$.
$$\frac{6!}{2!1!1!1!1!} = \frac{6!}{2} = \frac{720}{2} = 360.$$
(d) Todo ciclo en un grafo bipartito es de longitud par y alterna entre vértices de V_1 y V_2. Ya que un ciclo hamiltoniano usa todos los vértices en V_1 y V_2, tiene que ocurrir que $m = |V_1| = |V_2| = n$.

SOLUCIONES PRUEBA DE MATEMÁTICA DISCRETA

1. (a) Sabiendo que la clave pública es $n = 10553$ ($n = 173 \cdot 61$) y $e = 191$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.

(b) Calcular A y B sabiendo que el número $119A2692B63$ es múltiplo de 9 y de 11.

Solución:

(a) Cálculo de la clave privada d: $\phi(n) = \phi(10553) = (173 - 1) \cdot (61 - 1) = 172 \cdot 60 = 10320$.

d es el inverso modular de $e = 191$ módulo $\phi(n) = 10320$.

$\gcd(10320, 191) = 1$, ya que

$$\begin{array}{l|l} 10320 & 191 \\ \cline{2-2} 6 & 54 \end{array} \qquad \begin{array}{l|l} 191 & 6 \\ \cline{2-2} 5 & 31 \end{array} \qquad \begin{array}{l|l} 6 & 5 \\ \cline{2-2} 1 & 1 \end{array}$$

$6 = 10320 - 54 \cdot 191, \qquad 5 = 191 - 31 \cdot 6, \qquad 1 = 6 - 1 \cdot 5.$

Así:

$$\begin{aligned} 1 &= 6 - 5 = 6 - (191 - 31 \cdot 6) = 32 \cdot 6 - 191 = 32 \cdot (10320 - 54 \cdot 191) - 191 \\ &= 32 \cdot 10320 - 1728 \cdot 191 - 191 = 32 \cdot 10320 - 1729 \cdot 191 \end{aligned}$$

Por lo tanto, el inverso modular de 191 módulo 10320 es -1729, pero

$$-1729 \equiv 8591 \bmod 10320.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{191} \bmod 10533.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{8591} \bmod 10533.$$

(b)

$$119A2692B63 \equiv A + B + 3 \bmod 9$$

Por lo tanto $119A2692B63$ es divisible por 9 si, y solo si,

$$A + B + 3 \equiv 0 \bmod 9 \Longleftrightarrow A + B \equiv 6 \bmod 9$$

Por otro lado,

$$119A2692B63 \equiv -A + B - 2 \bmod 11$$

Por lo tanto $119A2692B63$ es divisible por 11 si, y solo si,

$$-A + B - 2 \equiv 0 \bmod 11 \Longleftrightarrow B - A \equiv 2 \bmod 11$$

Las posibles soluciones de $A + B \equiv 6 \bmod 9$ son:

A	B
0	6
1	5
2	4
3	3
4	2
5	1
6	0 o 9
7	8
8	7
9	6

La única solución que verifica $B - A \equiv 2 \bmod 11$ es $A = 2$ y $B = 4$. Por lo tanto el número es: 11922692463.

2. (a) Sabiendo que la clave pública es $n = 9853$ ($n = 167 \cdot 59$) y $e = 187$, calcular la clave privada y decir como se encripta y descifra un mensaje con el sistema RSA.
(b) Calcular A y B sabiendo que el número $39A4230B21$ es múltiplo de 3 y de 11.

Solución:

(a) Cálculo de la clave privada d: $\phi(n) = \phi(9853) = (167-1)\cdot(59-1) = 166\cdot 58 = 9628$. d es el inverso modular de $e = 187$ módulo $\phi(n) = 9628$.
$\gcd(9628, 187) = 1$, ya que

$$\begin{array}{r|l} 9628 & 187 \\ \hline 91 & 51 \end{array} \qquad \begin{array}{r|l} 187 & 91 \\ \hline 5 & 2 \end{array} \qquad \begin{array}{r|l} 91 & 5 \\ \hline 1 & 18 \end{array}$$

$91 = 9628 - 51 \cdot 187, \qquad 5 = 187 - 2 \cdot 91, \qquad 1 = 91 - 18 \cdot 5.$

Así:

$$\begin{aligned} 1 &= 91 - 18 \cdot 5 = 91 - 18 \cdot (187 - 2 \cdot 91) = 37 \cdot 91 - 18 \cdot 187 \\ &= 37 \cdot (9628 - 51 \cdot 187) - 18 \cdot 187 = 37 \cdot 9628 - 1905 \cdot 187 \end{aligned}$$

Por lo tanto, el inverso modular de 187 módulo 9628 es -1905, pero

$$-1905 \equiv 7723 \bmod 9628.$$

Para encriptar un mensaje m;

$$m \longrightarrow m^{187} \bmod 9853.$$

Para descifrar el mensaje recibido x;

$$x \longrightarrow x^{7723} \bmod 9853.$$

(b)

$$39A4230B21 \equiv A + B \bmod 3$$

Por lo tanto $39A4230B21$ es divisible por 3 si, y solo si,

$$A + B \equiv 0 \bmod 3$$

Por otro lado,

$$39A4230B21 \equiv -A + B - 1 \bmod 11$$

Por lo tanto $39A4230B21$ es divisible por 11 si, y solo si,

$$-A+B-1 \equiv 0 \bmod 11 \Longleftrightarrow B-A \equiv 1 \bmod 11$$

Las posibles soluciones de $A+B \equiv 0 \bmod 3$ son:

A	B
0	0 o 3 o 6 o 9
1	2 o 5 o 8
2	1 o 4 o 7
3	0 o 3 o 6 o 9
4	2 o 5 o 8
5	1 o 4 o 7
6	0 o 3 o 6 o 9
7	2 o 5 o 8
8	1 o 4 o 7
9	0 o 3 o 6 o 9

Las posibles soluciones que verifica $B-A \equiv 1 \bmod 11$ son:

- $A=1$ y $B=2$. Por lo tanto el número es: 3914230221.
- $A=4$ y $B=5$. Por lo tanto el número es: 3944230521.
- $A=7$ y $B=8$. Por lo tanto el número es: 3974230821.

Por lo tanto los números posibles son:
3914230221, 3944230521, 3974230821.

MATEMÁTICA DISCRETA **20/1/2015**

1. Determinar cantos divisores positivos ten o número $n = 2^4 5^3 11^2$. Cántos deles rematan en 0?

Solución:

Os únicos números primos que dividen a n son 2, 5 e 11, polo que calquera divisor de n será da forma $2^a 5^b 11^c$, con $0 \leq a \leq 4$, $0 \leq b \leq 3$ e $0 \leq c \leq 2$. Polo tanto, para a temos 5 posibilidades, 4 para b e 3 para c, o que, polo principio de multiplicación, nos dá un total de $5 \times 4 \times 3 = 60$ divisores.

Se queremos que un divisor remate en 0, necesariamente será un mútiplo de 10, é dicir, na anterior análise, están excluídas as posibilidades $a = 0$ e $b = 0$. Polo tanto, haberá $4 \times 3 \times 3 = 36$ divisores rematados en 0.

2. Determinar cantos números de 7 cifras hai tales que o producto das súas cifras sexa 15.

Solución:

Para que sete números do 0 ao 9 multiplicados dean 15, a única posibilidade é que sexan 5 uns, 1 tres e 1 cinco. Polo tanto, os números que se poden formar nas condicións pedidas corresponderanse coas permutacións dos elementos da lista $[1, 1, 1, 1, 1, 3, 5]$. Das 7 posibles posicións, 5 corresponden a uns, das dúas restantes, 1 corresponde ao tres e a restante ao 5. Polo tanto

$$\binom{7}{5}\binom{2}{1}\binom{1}{1} = \frac{7!}{5!\ 1!\ 1!} = 42$$

3. Buscar unha relación de recorrencia para a que a sucesión $\{a_n\}$, con $a_n = 1+2+\cdots+n$ para $n \geq 1$, sexa solución. Resolver a relación de recorrencia e dar unha fórmula para a suma dos n primeiros números enteiros positivos.

Solución:

A relación de recorrencia obvia é

$$a_{n+1} = a_n + (n+1),$$

linear con coeficientes constantes non homoxénea.

A relación de recorrencia linear homoxénea asociada é $a_{n+1} = a_n$, que ten por ecuación característica $r - 1 = 0$. A única raíz é $r = 1$, e polo tanto a solución xeral corresponde a

$$a_n^{(h)} = \alpha_1 1^n = \alpha_1.$$

A parte non homoxénea é un polinomio $F(n) = n + 1$, ou se preferimos, para aplicar o caso xeral, un polinómio multiplicado por 1^n. Como 1 é unha das raíces características (con multiplicidade 1), sabemos que hai unha solución particular da forma

$$a_n^{(p)} = (\alpha n + \beta)n^1 = \alpha n^2 + \beta n.$$

Substituindo en $a_{n+1} = a_n + n + 1$, teremos que

$$\alpha(n+1)^2 + \beta(n+1) = \alpha n^2 + \beta n + n + 1,$$

de onde se obtén que
$$(2n+1)\alpha + n\beta = n+1.$$
Dándolle a n, respectivamente, os valores 0 e1, obtéñense as ecuacións:

$$\begin{aligned} \alpha+\beta &= 1 \\ 3\alpha+\beta &= 2, \end{aligned}$$

que podemos resolver para obtermos $\alpha = 1/2$ e $\beta = 1/2$.

A solución xeral será, entón,
$$a_n = a_n^{(p)} + a_n^{(h)} = \alpha_1 + \frac{n^2}{2} + \frac{n}{2}.$$
Tendo en conta as condicións iniciais do problema (para $n = 1$ a suma vale 1), temos que
$$1 = a_1 = \alpha_1 + \frac{1^2}{2} + \frac{1}{2} = \alpha_1 + 1,$$
e, por tanto, $\alpha_1 = 0$, o que nos dá a coñecida fórmula para a suma dos n primeiros enteiros positivos:
$$a_n = \frac{n^2}{2} + \frac{n}{2} = \frac{1+n}{2}n$$

4. Utilizando a fórmula de Euler para grafos planos, determina o número de pentágonos que contén un balón de fútbol, sabendo que está formado exclusivamente por pentágonos e hexágonos regulares.

Solución:

Sexa p o número de pentágonos e h o número de hexágonos. Como cada arista do poliedro está necesariamente en dúas caras, o número de aristas do poliedro será
$$A = \frac{5p+6h}{2}.$$
En canto aos vértices, é claro que en cada un deles se xuntan 3 polígonos. Non poden ser 1 nin 2, obviamente, pero tampouco poden ser máis de 3, porque os ángulos internos tanto dos pentágonos coma dos hexágonos regulares superan os 90 graos. Polo tanto
$$V = \frac{5p+6h}{3}$$
Da fórmula de Euler sabemos que
$$C + V = A + 2,$$
e como $C = p + h$, temos que
$$p + h + \frac{5p+6h}{3} = \frac{5p+6h}{2} + 2,$$
é dicir, $p = 12$.

Dende o punto de vista da fórmula de Euler, valeríanos calquera número de hexágonos, pero pola regularidade do balón de fútbol, todos os vértices deben ser iguais, e posto que en cada vértice se xuntan 3 polígonos, temos dúas posibilidades: 2 pentágonos e

1 hexágono, ou 1 pentágono e 2 hexágonos. Esta segunda opción produce unha figura máis esférica (a suma dos ángulos en cada vértice é maior!) e é a que corresponde ao noso problema.

Polo tanto, tendo en conta que cada hexágono está presente en 6 vértices, e cada pentágono en 5, teremos que

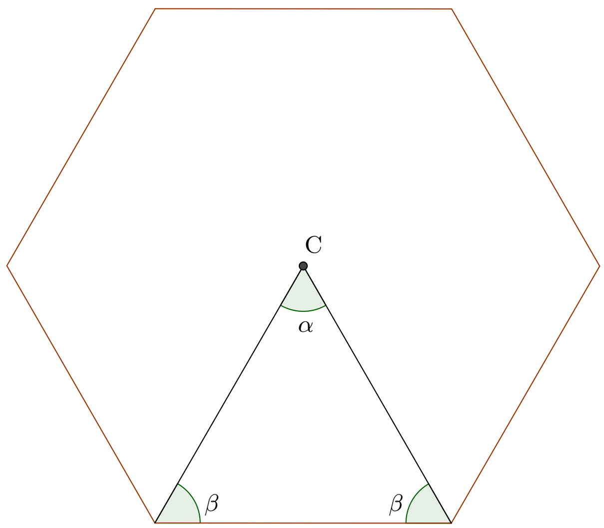
$$h = \frac{V \times 2}{6} \quad \text{e} \quad 12 = p = \frac{V \times 1}{5},$$

de onde

$$h = \frac{5p}{3} = 20$$

NOTA: ***Valor dos ángulos internos dun polígono regular***

Unindo o centro do polígono con dous vértices consecutivos formamos un triángulo isósceles, e chamándolle α ao ángulo no centro e β a cada un dos que se forman nos vértices, temos que $180 = \alpha + 2\beta$.



É claro que $n \times \alpha = 360$, polo que, multiplicando a ecuación anterior por n temos que

$$180n = (\alpha + 2\beta)n = \alpha n + 2\beta n = 360 + 2\beta n,$$

de onde

$$\beta = \frac{180(n-2)}{2n}$$

Polo tanto, dada un dos ángulos interiores do hexágono valerá, $2\beta = 2 \times 180(4/12) = 120$, e no caso do pentágono $2\beta = 2 \times 180(3/10) = 108$.

SOLUCIÓNS DO EXAME DE MATEMÁTICA DISCRETA
24/1/2012

1. (a) Existe o inverso de 19 módulo 141? En caso afirmativo, calculalo.
(b) Ten solucións a congruencia $19x \equiv 3 \bmod 141$? En caso afirmativo, calcular as soluciones que hai entre -200 e 200.

Solución:
(a) mcd(19, 141)=1. O inverso é 52, aplicando o algoritmo de Euclides.
(b) $19x \equiv 3 \bmod 141 \iff x \equiv \frac{1}{19} \cdot 3 \bmod 141 \iff x \equiv 52 \cdot 3 \bmod 141 \iff x \equiv 156 \bmod 141 \iff x \equiv 15 \bmod 141$.
As soluciones que hai entre -200 e 200 son:

$$-141 + 15 = -126, \quad 15, \quad 141 + 15 = 156\,.$$

2. Xustificar a igualdade $\displaystyle\sum_{k=0}^{n}(-1)^k \binom{n}{k} = 0.$

Solución: Polo teorema do binomio: $(x+y)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

En particular, $\big(1+(-1)\big)^n = \displaystyle\sum_{k=0}^{n} \binom{n}{k} (1)^{n-k}(-1)^k = \sum_{k=0}^{n}(-1)^k \binom{n}{k}$.

Pero, $1+(-1) = 0$, e así $\displaystyle\sum_{k=0}^{n}(-1)^k \binom{n}{k} = 0$.

3. (a) Determinar as soluciones da relación de recorrencia

$$a_n = -5a_{n-1} - 6a_{n-2} + 42 \cdot 4^n\,.$$

(b) Determinar a solución do apartado anterior coas condiciones iniciais $a_1 = 56$ e $a_2 = 278$.

Solución:
(a) Ecuación característica: $r^2 + 5r + 6 = 0$. $(r+2)(r+3) = 0$. raíces: -3,-2.
Solución xeral da homoxénea: $a_n = \alpha_1(-3)^n + \alpha_2(-2)^n$.
Solución particular da ecuación no homoxénea: $a_n^p = C \cdot 4^n$.

$$C \cdot 4^n = -5C \cdot 4^{n-1} - 6C \cdot 4^{n-2} + 42 \cdot 4^n\,.$$

Dividindo por 4^{n-2},

$$C \cdot 4^2 = -5C \cdot 4 - 6C + 42 \cdot 4^2 \iff 42 \cdot C = 42 \cdot 4^2 \iff C = 4^2 = 16\,.$$

A solución da ecuación de recorrencia é:

$$a_n = \alpha_1(-3)^n + \alpha_2(-2)^n + 16 \cdot 4^n\,.$$

.

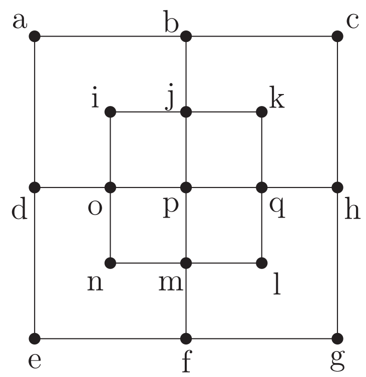
(b) $\left\{ \begin{array}{rcl} 56 & = & \alpha_1(-3) + \alpha_2(-2) + 16 \cdot 4 \\ 278 & = & \alpha_1(-3)^2 + \alpha_2(-2)^2 + 16 \cdot 4^2 \end{array} \right.$

Resolvendo o sistema, obtemos $\alpha_1 = 2, \alpha_2 = 1$.
Así, a solución é:

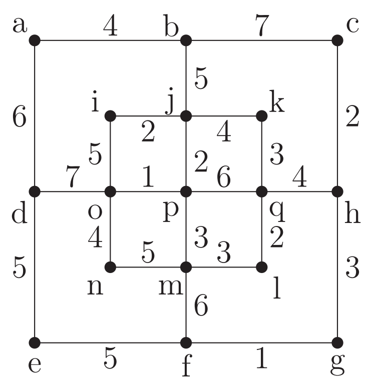
$$a_n = 2(-3)^n + (-2)^n + 16 \cdot 4^n \,.$$

.

4. Dado o seguinte grafo G



(a) Comprobar o teorema de apertón de mans. Calcular a sucesión de graos do grafo G.
(b) É bipartito? Cal é o número crómatico do grafo G?
(c) É conexo? Describir un camiño simple de lonxitude 6. É isomorfo ao grafo K_5?
(d) É euleriano? É hamiltoniano?
(e) É plano? Comprobar a fórmula de Euler para o grafo G.
(f) Calcular unha árbore xeradora minimal de G usando o algoritmo de Kruskal, sendo os pesos do grafo os que se indican a continuación



Solución:
(a) e= número de eixos: 24
Teorema de apertón de mans:

$2e = \text{grao}(a)+\text{grao}(b)+\text{grao}(c)+\text{grao}(d)+\text{grao}(e)+\text{grao}(f)+\text{grao}(g)+\text{grao}(h)+\text{grao}(i)+\text{grao}(j)+\text{grao}(k)+\text{grao}(l)+\text{grao}(m)+\text{grao}(n)+\text{grao}(o)+\text{grao}(p)+\text{grao}(q)$.
$2 \cdot 24 = 48 = 2+3+2+3+2+3+2+3+2+4+2+2+4+2+4+4+4.$

A sucesión de graos é: (2,2,2,2,2,2,2,2,3,3,3,3,4,4,4,4,4).

(b) É bipartito, xa que se pode colorear con dúas cores. O número crómatico é 2.
Unha partición é: $\{a, c, e, g, j, m, o, q\}$ é $\{b, d, f, h, i, k, l, n, p\}$.

(c) G é conexo xa que para cada par de vértices existe un camiño que os une.
Hai moitos, por exemplo: i, j, k, q, l, m, n.
Non é isomorfo a K_5 xa que K_5 ten 5 vértices e G ten 17 vértices.

(d) G non é euleriano xa que ten vértices de grao impar.
G non é hamiltoniano pois $G - \{b, d, f, h\}$ ten 5 compoñentes conexas.

(e) Si, G é plano xa que no debuxo non se cortan ningún par de arestas.
Fórmula de Euler: $r = e - v + 2$. e= eixos = 24 v= vértices = 17.
r= rexións = $24 - 17 + 2 = 9$.

(f) Eliximos os eixos:
$fg, op, \quad ij, ql, ch, jp, \quad gh, lm, pm, qk \quad ab, no, qh, \quad bj, de, ef.$