Exàmens resolts de Fonaments Matemàtics

Edició a càrrec de José Luis Ruiz

Juliol 2017

Departament de Matemàtiques
Facultat d'Informàtica de Barcelona
Universitat Politècnica de Catalunya

Col·lecció de problemes apareguts en diferents actes d'avaluació de l'assignatura *Fonaments Matemàtics* del *Grau en Enginyeria Informàtica* de la Facultat d'Informàtica de Barcelona, U.P.C., des del setembre de 2010. Problemes proposats i recopilats per:

Daniel Barrera
Josep Elgueta
Rafel Farré
Jaume Martí
Fernando Martínez
Montserrat Maureso
Mercè Mora
Francesc Prats
Victor Rotger
José Luis Ruiz
Carlos Seara
Pilar Sobrevilla
Francesc Tiñena
Joan Trias

Les solucions han estat redactades per José Luis Ruiz amb contribucions de Fernando Martínez, Joan Trias, Francesc Prats i Francesc Tiñena.

Índex

1

Enunciats

1.1 Exàmens de taller 2010–2011 Q1

Raonament

1 Considereu la connectiva $\oplus$ definida de la manera següent:

$$p \oplus q := (p \wedge \neg q) \vee (q \wedge \neg p)$$

1) Feu la taula de veritat de la proposició $(p \oplus (p \to p)) \to q$.

2) Doneu una proposició equivalent a $(p \oplus (p \to p)) \to q$ que no contingui la connectiva $\oplus$ i que contingui el mínim nombre possible de connectives.

2 Considereu la connectiva $\downarrow$ definida de la manera següent:

$$p \downarrow q := \neg p \wedge \neg q$$

1) Feu la taula de veritat de la proposició $((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$.

2) Doneu una proposició equivalent a $((p \downarrow p) \downarrow q) \downarrow ((p \downarrow p) \downarrow q)$ que no contingui la connectiva $\downarrow$ i que contingui el mínim nombre possible de connectives.

3 Considereu la connectiva $|$ definida de la manera següent:

$$p|q := p \vee q$$

1) Feu les taules de veritat de les proposicions $(p|p)|(q|q)$ i $(p|q)|(p|q)$.

2) Doneu una proposició equivalent a $(p|p)|(q|q)$ que no contingui la connectiva $|$ i que contingui el mínim nombre possible de connectives.

3) Doneu una proposició equivalent a $(p|q)|(p|q)$ que no contingui la connectiva $|$ i que contingui el mínim nombre possible de connectives.

4 Considereu les connectives $\downarrow$ i $|$ definides de la manera següent:

$$p \downarrow q := p \wedge q, \quad p|q := p \vee q$$

1) Feu la taula de veritat de les proposicions $p|q$ i $(p \downarrow p) \downarrow (q \downarrow q)$ i doneu una proposició equivalent a $p|q$ que només contingui les connectives i $\downarrow$.

2) Feu la taula de veritat de les proposicions $p \downarrow q$ i $(p|p)|(q|q)$ i doneu una proposició equivalent a $p \downarrow q$ que només contingui les connectives $\neg$ i $|$.

3) Doneu una proposició equivalent a $p \downarrow p$ on només intervinguin connectives clàssiques (negació, conjunció, disjunció, condicional, bicondicional) i doneu una proposició equivalent a $p|q$ que només contingui la connectiva $\downarrow$.

4) Doneu una proposició equivalent a $p|p$ on només intervinguin connectives clàssiques (negació, conjunció, disjunció, condicional, bicondicional) i doneu una proposició equivalent a $p \downarrow q$ que només contingui la connectiva $|$.

5 Trobeu una proposició equivalent a $p \leftrightarrow q$ on hi apareguin exclusivament:

1) Les connectives $\neg$ i $\vee$.

2) Les connectives $\neg$ i $\wedge$.

3) Les connectives $\neg$ i $\rightarrow$.

6 Simbolitzeu en el llenguatge del càlcul de predicats els enunciats que segueixen. Ho heu de fer de dues maneres:

a) sense utilitzar quantificadors universals ($\forall$) ni condicionals ($\rightarrow$) i amb el mínim nombre possible de negacions ($\neg$);

b) sense utilitzar quantificadors existencials ($\exists$) i utilitzant condicionals ($\rightarrow$).

Els enunciats són:

1) No tota funció té derivada.

2) Hi ha funcions contínues no derivables.

3) Cap nombre enter és parell i senar alhora.

4) Tot nombre enter és parell o senar.

Useu els predicats: F: "ser funció"; C: "ser contínua"; D: "ser derivable"; N: "ser nombre enter"; P: "ser parell"; S: "ser senar".

7 Simbolitzeu:

1) Hi ha un únic objecte que té la propietat P.

2) Hi ha exactament dos objectes que tenen la propietat P.

3) Hi ha com a màxim un objecte que té la propietat P.

4) Hi ha com a mínim dos objectes que tenen la propietat P.

Conjunts

8 Siguin A, B i C conjunts arbitraris. Demostreu que $A-(B\cap C)\subseteq A-B$ si, i només si, $A\cap B\subseteq A\cap C$.

9 Siguin A i B conjunts arbitraris. Demostreu que $(A-B)\cup(B-A)=A$ si, i només si, $B=\emptyset$.

10 Siguin A i B conjunts arbitraris. Demostreu que $(A-B)\cup(B-A)=A\cup B$ si, i només si, $A\cap B=\emptyset$.

11 Siguin Ω un conjunt i $A,B,C\subseteq\Omega$ subconjunts tals que $A\cap B^c\subseteq C$ i $C^c\cap B=\emptyset$. Demostreu que $A\subseteq C$.

12 Siguin Ω un conjunt i $A,B,C\subseteq\Omega$ subconjunts tals que $B\cap C^c=\emptyset$. Demostreu que $A-(A-B)\subseteq A\cap C$.

13 Siguin Ω un conjunt i $A,B,C\subseteq\Omega$ subconjunts no buits tals que $A\cap B\cap C=\emptyset$. Proveu que si $D\subseteq\Omega$ és un subconjunt tal que $D\cap A\subseteq D\cap B$, aleshores $D\cap C\subseteq A^c$.

14 Siguin A, B i C conjunts tals que $A\cup B\subseteq A\cup C$ i $A\cap B\subseteq A\cap C$. Demostreu que $B\subseteq C$.

15 Siguin Ω un conjunt i $A,B,C\subseteq\Omega$ subconjunts tals que $A\cap B\neq\emptyset$ i $B\cap C^c=\emptyset$. Demostreu que $A\cap C\neq\emptyset$.

16 Siguin Ω un conjunt i $A,B,C\subseteq\Omega$ subconjunts. Demostreu que $C\subseteq A\cap B$ si, i només si, $C\cap A^c=\emptyset$ i $C\cap B^c=\emptyset$.

Aplicacions

17 Considerem l'aplicació $f\colon\mathbb{N}\to\mathbb{N}$ definida per:

$$f(n)=\begin{cases} n, & \text{si } n \text{ és parell}\\ n+1, & \text{si } n \text{ és senar}\end{cases}$$

1) Proveu que $f \circ f = f$.

2) Calculeu $f[\{1, 2, 3, 4\}]$. Deduïu que f no és injectiva.

3) Calculeu $f^{-1}[\{0, 1, 2\}]$. Deduïu que f no és exhaustiva.

18 Considerem l'aplicació $f\colon \mathbb{N} \to \mathbb{N}$ definida per:

$$f(n) = \begin{cases} n, & \text{si } n \text{ és múltiple de } 3 \\ 3n, & \text{en cas contrari} \end{cases}$$

1) Proveu que $f \circ f = f$.

2) Calculeu $f[\{1, 2, 3, 4\}]$. Deduïu que f no és injectiva.

3) Calculeu $f^{-1}[\{0, 1, 2\}]$. Deduïu que f no és exhaustiva.

19 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{Z}$ definida per:

$$f(n) = \begin{cases} -n^2, & \text{si } n < 0 \\ n^2, & \text{si } n \geq 0 \end{cases}$$

1) Calculeu $f[\{-2, -1, 0, 1, 2\}]$.

2) Proveu que f és injectiva.

3) Calculeu $f^{-1}[\{0, 1, 2\}]$. Deduïu que f no és exhaustiva.

20 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{N}$ definida per:

$$f(n) = \begin{cases} 2n - 1, & \text{si } n > 0 \\ -2n, & \text{si } n \leq 0 \end{cases}$$

1) Calculeu $f[\{-2, -1, 0, 1, 2\}]$ i $f[\{-5, -3, 0, 3, 5\}]$.

2) Calculeu $f^{-1}[\{0, 1, 2\}]$ i $f^{-1}[\{0, 3, 6\}]$

3) Proveu que f és injectiva.

4) Proveu que f és exhaustiva.

21 Considerem l'aplicació $f\colon \mathbb{N} \to \mathbb{Z}$ definida per:

$$f(n) = \begin{cases} -\frac{n}{2}, & \text{si } n \text{ és parell} \\ \frac{n+1}{2}, & \text{si } n \text{ és senar} \end{cases}$$

1) Calculeu $f[\{0,1,2,3,4,5\}]$ i $f[\{0,3,5,6,7,10\}]$.

2) Calculeu $f^{-1}[\{-1,0,1,2\}]$ i $f^{-1}[\{-3,-1,0,1\}]$.

3) Proveu que f és exhaustiva.

4) Proveu que f és injectiva.

22 Considerem l'aplicació $f\colon \mathbb{N} \to \mathbb{N}$ definida per:

$$f(n) = \begin{cases} n+1, & \text{si } n \text{ no és múltiple de } 5 \\ \frac{n}{5}, & \text{si } n \text{ és múltiple de } 5 \end{cases}$$

1) Calculeu $f^{-1}[\{0,1,2,3,4,5\}]$.

2) Proveu que f és exhaustiva.

3) Calculeu $f[\{0,1,2,5,10,15\}]$. Deduïu que f no és injectiva.

23 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{N}$ definida per:

$$f(n) = n^2 + 1.$$

Siguin: $S = \{n \in \mathbb{N} : n \text{ és senar}\}$, $P = \{m \in \mathbb{Z} : m \text{ és parell}\}$.

1) Proveu que $f^{-1}[S] = P$.

2) Proveu que f no és exhaustiva.

3) Proveu que f no és injectiva.

4) És f bijectiva?

24 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{Z}$ definida per:

$$f(n) = \begin{cases} 7n, & \text{si } n \text{ és parell} \\ n+2, & \text{si } n \text{ és senar} \end{cases}$$

1) Calculeu $f^{-1}[\{-1,0,1,2\}]$. Deduïu que f no és exhaustiva.

2) Proveu que f és injectiva.

3) És f bijectiva?

25 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{Z}$ definida per:

$$f(n) = n^2 + n + 1$$

1) Calculeu $f[\{-2,-1,0,1,2\}]$. Deduïu que f no és injectiva.

2) Calculeu $f^{-1}[\{0,1\}]$. Deduïu que f no és exhaustiva.

3) És f bijectiva?

26 Considerem els conjunts:

$$A = \{n \in \mathbb{N} : n \geq 2\}, \quad P = \{p \in \mathbb{N} : p \text{ és un nombre primer}\}$$

i l'aplicació $f\colon A \to P$ definida per:

$$f(n) = \text{nombre primer més petit que divideix } n$$

1) Proveu que $f_{|P} = I_P$. ($f_{|P}$ és la restricció de f a $P \subseteq A$ i I_P és l'aplicació identitat de P.)

2) Calculeu $f[\{2,6,9,11,35\}]$. Deduïu que f no és injectiva.

3) Proveu que f és exhaustiva.

4) És f bijectiva?

27 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{Z}$ definida per:

$$f(n) = \begin{cases} n, & \text{si } n \text{ és múltiple de } 5 \\ 5n, & \text{en cas contrari} \end{cases}$$

1) Proveu que $f \circ f = f$.

2) Calculeu $f[\{0,1,2,3,4,5\}]$. Deduïu que f no és injectiva.

3) Calculeu $f^{-1}[\{0,1,5\}]$. Deduïu que f no és exhaustiva.

4) És f bijectiva?

28 Considerem l'aplicació $f\colon \mathbb{N} \to \mathbb{N}$ definida per:

$$f(n) = \begin{cases} n, & \text{si } n \text{ és múltiple de } 3 \\ n+1, & \text{si el residu de dividir } n \text{ per 3 és 1} \\ n-1, & \text{si el residu de dividir } n \text{ per 3 és 2} \end{cases}$$

1) Calculeu $f[A]$, si $A = \{1,2,3,4,5,6\}$.

2) Deduïu que l'aplicació $g\colon A \to A$ definida per $g(a) = f(a)$, si $a \in A$, és bijectiva.

3) Proveu que f és injectiva.

4) Calculeu $f[B]$, si $B = \{0, 1, 2, 4, 5, 9\}$.

5) Deduïu que l'aplicació $h\colon B \to B$ definida per $h(b) = f(b)$, si $b \in B$, és bijectiva.

6) Proveu que f és exhaustiva.

29 Considerem els conjunts:

$$A = \{n \in \mathbb{N} : n \geq 2\}, \quad P = \{p \in \mathbb{N} : p \text{ és un nombre primer}\}$$

i les aplicacions $f\colon A \to P$, $g\colon P \to A$ definides per:

$$f(n) = \text{nombre primer més petit que divideix } n$$
$$g(p) = p^2$$

1) Calculeu $g[\{2, 3, 5, 7, 11\}]$ i $f^{-1}[\{2\}]$.

2) Proveu que $f \circ g = I_P$. (I_P és l'aplicació identitat de P.)

3) Proveu que f és exhaustiva.

4) Per a quins valors de $n \in A$ se satisfà $(g \circ f)(n) = n$?

5) Proveu que g és injectiva.

30 Considerem l'aplicació $f\colon \mathbb{Z} \to \mathbb{Z}$ definida per:

$$f(n) = \begin{cases} n/2, & \text{si } n \text{ és parell} \\ 2n, & \text{si } n \text{ és senar} \end{cases}$$

1) Calculeu $f[\{0, 1, 2, 4, 8\}]$. Deduïu que f no és injectiva.

2) Proveu que f és exhaustiva.

3) És f bijectiva?

Principi d'inducció

31 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$$

32 Demostreu per inducció que per a tot $n \geq 1$:

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

33 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{j=1}^{n} j(j+1) = \frac{n(n+1)(n+2)}{3}$$

34 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{\ell=1}^{n} \frac{1}{\ell(\ell+1)} = \frac{n}{n+1}$$

35 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{r=1}^{n} (3r-2) = \frac{3n^2-n}{2}$$

36 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{s=1}^{n} (4s+1) = n(2n+3)$$

37 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{v=1}^{n} (v^2+v) = \frac{n(n+1)(n+2)}{3}$$

38 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{m=1}^{n} (5m-3) = \frac{5n^2-n}{2}$$

39 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{u=1}^{n} (u^2-u) = \frac{n(n^2-1)}{3}$$

40 Demostreu per inducció que per a tot $n \geq 1$:

$$\sum_{t=1}^{n} t^3 = \frac{n^2(n+1)^2}{4}$$

41 Demostreu per inducció que per a tot $n \geq 1$:

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

Enters: divisibilitat

42 Siguin $a, b \in \mathbb{Z}$ i $d = \mathrm{mcd}(a, b)$. Proveu que $\mathrm{mcd}(2a, d) = d$.

43 Siguin $a, b \in \mathbb{Z}$ primers entre ells. Proveu que si b és senar, llavors $\mathrm{mcd}(2a, b) = 1$.

44 Siguin $a, b \in \mathbb{Z}$ primers entre ells i p, q nombres primers diferents. Proveu que $\mathrm{mcd}(pa, qb)$ és igual a 1, p, q o pq.

45 Sigui p un nombre primer senar i a un enter parell. Proveu que $\mathrm{mcd}(a, 2p)$ és igual a 2 o igual a $2p$.

46 Siguin p, q i ℓ tres nombres primers diferents i a un enter. Sabem que $\ell | a$ i que $a = p \cdot N = q \cdot M$, on N i M són enters. Proveu que $\mathrm{mcd}(N, M) \neq 1$.

47 Siguin a, b, c, d enters. Proveu que si $a \mid b$ i $c \mid d$, llavors $ac \mid bd$.

48 Siguin a, b, c, d enters. Proveu que si $ac + bd = 1$, llavors $\mathrm{mcd}(a, b) = 1$.

49 Siguin $a, b \in \mathbb{Z}$. Proveu que si $\mathrm{mcd}(a, a + b) = 1$, llavors $\mathrm{mcd}(a, a - b) = 1$.

50 Siguin $a, b \in \mathbb{Z}$. Proveu que $\mathrm{mcd}(a, b)$ és un divisor de $\mathrm{mcm}(a, a + b)$.

51 Siguin a, b, c enters i p un nombre primer. Proveu que si $p \mid ab$, $p \mid ac$ i $\mathrm{mcd}(b, c) = 1$, llavors $p \mid a$.

52 Siguin a, b, c, d enters i $r = \mathrm{mcd}(a, b)$, $s = \mathrm{mcd}(c, d)$. Proveu que si $a \mid c$ i $b \mid d$, llavors $r \mid s$.

53 Calculeu el màxim comú divisor dels nombres que s'indiquen i els coeficients x i y

de la identitat de Bézout corresponent.

a	b	$\text{mcd}(a,b)$	x	y
603	651	3	-95	88
484	460	4	-19	20
792	599	1	-90	119
317	482	1	111	-73
643	524	1	251	-308
430	721	1	166	-99
372	348	12	-14	15
696	467	1	-104	155
431	636	1	-121	82
680	593	1	-259	297
545	433	1	58	-73
384	748	4	-37	19
794	591	1	230	-309
560	502	2	26	-29
391	505	1	31	-24
686	651	7	-37	39
722	667	1	-97	105
310	685	5	42	-19
558	314	2	-9	16
388	657	1	127	-75

1.2 Examen parcial 22/11/2010

54

1) Considerem la proposició p següent:

$$\forall\, a,b,c \in \mathbb{Z}\,(\ c \text{ parell} \wedge c = a\cdot b \quad\rightarrow\quad a \text{ parell} \wedge b \text{ parell}\ )$$

Digueu si p és certa o falsa i justifiqueu la resposta.

2) Siguin A, B conjunts no buits. Proveu que l'aplicació $g\colon A\times B \to A$ definida per $g\big((x,y)\big) = x$ és exhaustiva.

55 Considerem el conjunt $A = (\mathbb{Z}-\{0\})\times(\mathbb{Z}-\{0\})$ i la relació R sobre A definida per:

$$(a,b)\ R\ (c,d) \iff a\cdot d = b\cdot c,$$

on $(a,b),(c,d)\in A$.

1) Demostreu que R és una relació d'equivalència sobre A.

2) Trobeu la classe d'equivalència de l'element $(a,b)\in A$.

3) Doneu una descripció del conjunt quocient A/R.

56 Demostreu per inducció que l'enter $n^3 + 3n^2 + 2n$ és divisible per 6, per a tot enter $n \geq 0$.

57

1) Considerem la proposició p següent:

$$\forall\, a, b, c \in \mathbb{Z}\,(\ a \text{ parell} \wedge a = b + c \quad \rightarrow \quad b \text{ senar} \wedge c \text{ senar}\ )$$

   Digueu si p és certa o falsa i justifiqueu la resposta.

2) Siguin A, B conjunts no buits i $b_0 \in B$ un element fix. Proveu que l'aplicació $h\colon A \rightarrow A \times B$ definida per $h(x) = (x, b_0)$ és injectiva.

58 Considerem el conjunt $A = \mathbb{Z} \times \mathbb{Z}$ i la relació R sobre A definida per:

$$(a, b)\ R\ (c, d) \iff a + d = b + c,$$

on $(a, b), (c, d) \in A$.

1) Demostreu que R és una relació d'equivalència sobre A.

2) Trobeu la classe d'equivalència de l'element $(0, b) \in A$.

3) Doneu una descripció del conjunt quocient A/R.

59 Demostreu per inducció que l'enter $(n+1)^3 - n - 1$ és múltiple de 6, per a tot enter $n \geq 0$.

1.3 Examen final 17/01/2011

60 Digueu si les afirmacions següents són certes o falses i justifiqueu la resposta.

1) $(\forall n \in \mathbb{Z})(\exists a, b \in \mathbb{Z} \quad n = 5a + 7b)$

2) Les proposicions $\neg[((\neg p) \vee q) \rightarrow r]$ i $(\neg p) \wedge q \wedge (\neg r)$ són lògicament equivalents.

3) Si $f\colon X \rightarrow Y$ és una funció, llavors $f(f^{-1}(Y)) = Y$.

61 Proveu que si $a, b, c \in \mathbb{Z}$, llavors $\text{mcd}(a, b) = \text{mcd}(bc - a, b)$.

62 Considerem l'aplicació $f\colon \mathbb{Z}_{29} \rightarrow \mathbb{Z}_{29}$ definida per $f(\overline{x}) = \overline{22} \cdot \overline{x} + \overline{7}$

1) Proveu que f és bijectiva i trobeu la seva inversa.

2) Considerem l'alfabet de 29 símbols indicat a continuació i assignem a cada símbol el nombre que té a la dreta:

A	0	F	5	K	10	P	15	U	20	Z	25	
B	1	G	6	L	11	Q	16	V	21		26	(espai)
C	2	H	7	M	12	R	17	W	22	.	27	
D	3	I	8	N	13	S	18	X	23	,	28	
E	4	J	9	O	14	T	19	Y	24			

Codifiquem cada frase escrita en l'alfabet anterior aplicant la regla de codificació $x \mapsto 22x + 7 \pmod{29}$ al valor numèric corresponent a cadascun dels símbols. Per exemple 'AVUI' és '0 21 20 8' i es codificaria en '7 5 12 9', o sigui 'HFMJ', ja que $0 \mapsto 7$, $21 \mapsto 5$, $20 \mapsto 12$, $8 \mapsto 9$.

Si el resultat d'una codificació ha estat el missatge 'KZRT,AI' (el que hi ha entre les cometes), quin era el missatge original?

63 Proveu que per a tot $n \geq 0$ es compleix que $2^{n+2} + 3^{2n+1} \equiv 0 \pmod{7}$. (*Indicació*: pot fer-se per inducció, però també d'altres maneres.)

1.4 Exàmens de taller 2010–2011 Q2

Lògica i raonament

64 Considerem les dues connectives lògiques X i O definides per les taules de veritat que segueixen:

p	q	pXq	pOq
0	0	1	1
0	1	1	0
1	0	1	0
1	1	0	0

a) Expresseu la connectiva $\wedge$ en funció únicament de la connectiva X.

b) Expresseu la connectiva $\vee$ en funció únicament de la connectiva X.

c) Expresseu la connectiva $\rightarrow$ en funció únicament de la connectiva X.

d) Expresseu la connectiva $\wedge$ en funció únicament de la connectiva O.

e) Expresseu la connectiva $\vee$ en funció únicament de la connectiva O.

f) Expresseu la connectiva $\rightarrow$ en funció únicament de la connectiva O.

g) Expresseu la connectiva X en funció únicament de la connectiva O.

h) Expresseu la connectiva O en funció únicament de la connectiva X.

65 Doneu una condició necessària però no suficient perquè el nombre natural n sigui parell. Doneu una condició suficient però no necessària perquè el nombre natural n sigui parell. Justifiqueu les respostes.

66 És necessari que la suma de dos enters sigui parell perquè els dos nombres siguin parells? I suficient? Justifiqueu les respostes.

67 Doneu una condició necessària i suficient, diferent d'ella mateixa, perquè el nombre natural n sigui múltiple de 6. Doneu-ne també una de necessària però no suficient i una de suficient però no necessària. Justifiqueu les respostes.

68 Formalitzeu l'enunciat següent: 'no hi ha més de dos enters diferents que compleixin la propietat P'. Doneu una propietat P per a la qual l'enunciat sigui vertader i una altra propietat P per a la qual l'enunciat sigui fals. Justifiqueu les respostes.

69 Formalitzeu l'enunciat següent: 'hi ha al menys tres enters diferents que compleixen la propietat P'. Doneu una propietat P per a la qual l'enunciat sigui vertader i una altra propietat P per a la qual l'enunciat sigui fals. Justifiqueu les respostes.

70 Siguin A i B dos enunciats. De 'A' i de 'si B, llavors A', és correcte deduir 'B'? Justifiqueu la resposta.

71 En una "demostració" trobem un primer apartat on a partir de p i de $\neg q$ s'arriba a r i un segon apartat on a partir de $\neg p$ i $\neg r$ s'arriba a q. És una demostració de $q \vee r$? És una demostració de $q \wedge r$? Justifiqueu les respostes.

Conjunts i aplicacions

72

1) Siguin A, B i C conjunts arbitraris.
   a) Proveu que si $B \cap C = \emptyset$, llavors $(A - B) \cup C \subseteq (A \cup B \cup C) - (A \cap B)$.
   b) És certa la igualtat $(A - B) \cup C = (A \cup B \cup C) - (A \cap B)$? Justifiqueu la resposta.
2) Doneu un exemple de funció $f\colon \mathbb{Z} \to \mathbb{Z}$ que sigui injectiva però no exhaustiva. Justifiqueu la injectivitat i la no exhaustivitat.

73

1) Siguin A, B i C conjunts arbitraris.

a) Proveu que $A - (B - C) \subseteq (A - B) \cup C$.

b) És certa la igualtat $A - (B - C) = (A - B) \cup C$? Justifiqueu la resposta.

2) Doneu un exemple de funció $f\colon \mathbb{Z} \to \mathbb{Z}$ que sigui exhaustiva però no injectiva. Justifiqueu la exhaustivitat i la no injectivitat.

74

1) Siguin A, B i C conjunts arbitraris.

a) Proveu que $(A - B) \cap (A - C) \subseteq A - (B \cap C)$.

b) És certa la igualtat $(A - B) \cap (A - C) = A - (B \cap C)$? Justifiqueu la resposta.

2) Doneu un exemple de funció $f\colon \mathbb{Z} \to \mathbb{Z}$ que sigui bijectiva i que no sigui l'aplicació identitat. Calculeu f^{-1}.

75

1) Siguin A, B i C conjunts arbitraris.

a) Proveu que $A - (B \cup C) \subseteq (A - B) \cup (A - C)$.

b) És certa la igualtat $A - (B \cup C) = (A - B) \cup (A - C)$? Justifiqueu la resposta.

2) Doneu un exemple de funció $f\colon \mathbb{N} \to \mathbb{N}$ que sigui bijectiva i que no sigui l'aplicació identitat. Calculeu f^{-1}.

76

1) Siguin $f\colon A \to B$ una aplicació i $P, Q \subseteq A$.

a) És certa la implicació: $f[P] = f[Q] \Rightarrow P = Q$? Justifiqueu la resposta.

b) Proveu que si f és injectiva, llavors la implicació anterior és certa.

2) Siguin A, B, C conjunts tals que $A \neq B$ i $C \neq \emptyset$. Es pot donar el cas que $A \times C = B \times C$? Justifiqueu la resposta.

77

1) Siguin $g\colon A \to B$ una aplicació i $S, T \subseteq B$.

a) És certa la implicació: $f^{-1}[S] = f^{-1}[T] \Rightarrow S = T$? Justifiqueu la resposta.

b) Proveu que si f és exhaustiva, llavors la implicació anterior és certa.

2) Siguin A, B, C, D conjunts. Podem assegurar que

$$(A \cup B) \times (C \cup D) = (A \times C) \cup (B \times D)?$$

Justifiqueu la resposta.

78

1) Siguin $f: A \to B$ una aplicació i $C \subseteq A$.
   a) És certa la igualtat: $f[A - C] = f[A] - f[C]$? Justifica la resposta.
   b) Proveu que si f és injectiva, llavors la igualtat anterior és certa.

2) Sigui X un conjunt no buit. Definiu a X una relació d'equivalència R tal que X/R tingui un element. Comproveu que es tracta d'una relació d'equivalència.

Principi d'inducció i divisibilitat

79 Proveu per inducció que si $n \geq 1$, llavors l'enter $6 \cdot 7^n - 2 \cdot 3^n$ és un múltiple de 4.

80 Proveu per inducció que si $n \geq 0$, llavors $\frac{n^5}{5} + \frac{n^3}{3} + \frac{7n}{15}$ és un nombre enter.

81 Proveu per inducció que si $n \geq 0$, llavors $9 \mid [n^3 + (n+1)^3 + (n+2)^3]$.

82 Proveu per inducció que si $n \geq 0$, llavors $73 \mid (8^{n+2} + 9^{2n+1})$.

83 Proveu per inducció que si $n \geq 1$, llavors $\frac{(2n)!}{2^n} \in \mathbb{Z}$.

84 Proveu per inducció que si $n \geq 1$, llavors $\frac{(2n)!}{n!2^n} \in \mathbb{Z}$.

85 Calculeu el màxim comú divisor dels nombres que s'indiquen i els coeficients x i y de la identitat de Bézout corresponent.

a	b	mcd(a, b)	x	y
7658	3853	1	-883	1755
9191	6987	1	-1975	2598
5548	1727	1	80	-257
3614	7752	2	1435	-669
1084	4904	4	-95	21
7084	3563	7	-85	169
9176	7084	4	640	-829
3419	9168	1	4403	-1642
7119	6966	9	-91	93
3643	8590	1	-3353	1422
6312	2659	1	1276	-3209
1628	9613	1	-124	21
8304	1274	2	-83	541

1.5 Examen parcial 28/04/2011

86 Considerem en $\mathbb{R} \times \mathbb{R}$ la relació següent:

$$(x, y)R(z, t) \text{ si, i només si, } |x| + |y| = |z| + |t|.$$

1) Proveu que R és una relació d'equivalència.

2) Assenyaleu, en el pla, quins són els elements de la classe de $(1, 0)$. Raoneu la resposta.

87 Siguin X, Y conjunts.

1) Proveu que $\mathcal{P}(X) \cup \mathcal{P}(Y) \subseteq \mathcal{P}(X \cup Y)$.

2) És certa l'inclusió contrària? Justifiqueu la resposta.

88 Sigui A un conjunt i $f, g\colon A \to A$ dues aplicacions tals que $f \circ g = I_A$.

1) Proveu que g és injectiva.

2) Proveu que f és exhaustiva.

3) Podem afirmar que $g \circ f = I_A$? Justifiqueu la resposta.

1.6 Examen final 06/06/2011

89

1) Comproveu que $\text{mcd}(1876, 365) = 1$ i calculeu enters r i s tals que:

$$1876 \cdot r + 365 \cdot s = 1$$

Expliciteu els càlculs que feu per a arribar a la solució.

2) Trobeu el mínim enter positiu x tal que $365x + 902 \equiv -508 \pmod{1876}$. Expliciteu i justifiqueu els càlculs que feu per a arribar a la solució.

90 Proveu que si $n \geq 0$, llavors:

$$\sum_{k=0}^{n} k2^{n-k} = 2^{n+1} - n - 2$$

91 Siguin m, n enters positius.

1) Proveu que, en general, $\text{mcd}(m, n) \neq \text{mcd}(m - n, m + n)$.

2) Proveu que una condició suficient perquè $\text{mcd}(m, n) = \text{mcd}(m - n, m + n)$ és que m i n tinguin paritat diferent.

3) Proveu que la condició esmentada a l'apartat anterior no és necessària.

92 Trieu **dues** preguntes de les següents.

1) Enunrieu les lleis de De Morgan per a proposicions i demostreu-les.

2) Definiu el concepte de diferència de dos conjunts. Demostreu que si A i B són conjunts, llavors:

$$A \subseteq B \iff A - B = \emptyset$$

3) Siguin $a, a', b, b' \in \mathbb{Z}$ i $n > 1$ tals que $a \equiv a' \pmod{n}$ i $b \equiv b' \pmod{n}$. Demostreu que $a + b \equiv a' + b' \pmod{n}$ i $ab \equiv a'b' \pmod{n}$.

1.7 Exàmens de taller 2011–2012 Q1

Raonament

93

1) Siguin m i n nombres enters. És suficient que m i n siguin múltiples de 3 per a poder afirmar que $m + n$ és múltiple de 3? I necessari? Justifiqueu les respostes.

2) Formalitzeu la proposició següent i negueu-la: "hi ha enters que són quadrats, senars i múltiples de 5".

94

1) Sigui n un nombre enter. És necessari que n sigui múltiple de 4 perquè n^2 sigui múltiple de 8? I suficient? Justifiqueu les respostes.

2) Formalitzeu la proposició següent i negueu-la: "hi ha nombres naturals que no són parells, ni múltiples de 3, però sí múltiples de 5".

95

1) Proveu que una condició necessària i suficient perquè un enter sigui parell és que el seu quadrat sigui parell.

2) Formalitzeu la proposició següent i negueu-la: "per a tot nombre natural n més petit que 100, $n^2 + n + 41$ és un nombre primer".

96

1) Acabar en 55, és una condició necessària per ser senar múltiple de 5? I suficient? Justifiqueu les respostes.

2) Formalitzeu la proposició següent i negueu-la: "tot nombre natural és suma de dos quadrats".

97

1) Siguin m i n nombres enters. És suficient que m i n siguin consecutius per a poder afirmar que $(m+n)^2$ és senar? I necessari? Justifiqueu les respostes.

2) Formalitzeu la proposició següent i negueu-la: "per a tot nombre naturals n, o bé n^2 és parell o bé no acaba en 7".

98

1) Demostreu, per reducció a l'absurd, que tot nombre que acaba en 4 i no és múltiple de 4 té la xifra de les desenes senar.

2) Formalitzeu la proposició següent i negueu-la: "per a tot enter n, n és parell o n^3 no acaba en 9".

99

1) Demostreu que el cub de qualsevol enter és o bé multiple de 8 o bé és senar.

2) Formalitzeu la proposició següent i negueu-la: "hi ha enters n que són cubs, parells i múltiples 8".

100

1) Demostreu, per reducció a l'absurd, que si x és un nombre racional tal que x^2 és un nombre enter, aleshores x és un nombre enter.

2) Formalitzeu la proposició següent i negueu-la: "el producte de dos nombres primers és un nombre primer".

101

1) Proveu si m és un enter qualsevol i n és un enter senar múltiple de 3, aleshores el producte mn és senar o és múltiple de 6.

2) Formalitzeu la proposició següent i negueu-la: "la suma de dos nombres primers és un nombre parell".

102

1) Proveu que si n és un nombre natural, aleshores n^2 dividit per 3 dóna com a residu 0 o 1, però mai no dóna 2. Pista: feu una demostració per casos: considereu el residu de n entre 3.

2) Formalitzeu la proposició següent i negueu-la: “hi ha enters n que són quadrats, parells però no múltiples de 8”.

Conjunts i aplicacions

103

1) Siguin $f : \mathbb{N} \to \mathbb{N}$ una aplicació injectiva. Proveu que l'aplicació $g : \mathbb{N} \to \mathbb{N}$ definida per $g(n) = 2f(n)$ també és injectiva.

2) Descriu per extensió el conjunt $\mathcal{P}(\mathcal{P}(\emptyset))$; és a dir, digueu quins són els seus elements.

104

1) Sigui $f : \mathbb{N} \to \mathbb{N}$ una aplicació injectiva. Proveu que l'aplicació $g : \mathbb{N} \to \mathbb{N}$ definida per $g(n) = 2f(n) + 1$ també és injectiva.

2) Siguin A i B conjunts tals que $A \cup B = B$ i $A \cap B = B$. Què podem dir de A i de B? Justifica la resposta.

105

1) Sigui $f : \mathbb{Z} \to \mathbb{Z}$ una aplicació injectiva. Proveu que l'aplicació $g : \mathbb{Z} \to \mathbb{Z}$ definida per $g(n) = f(n - 1)$ també és injectiva.

2) Siguin A i B conjunts no buits. És vertader o fals que $\mathcal{P}(A - B) = \mathcal{P}(A) - \mathcal{P}(B)$? Justifica la resposta.

106

1) Sigui $f : \mathbb{Z} \to \mathbb{Z}$ una aplicació exhaustiva. Proveu que l'aplicació $g : \mathbb{Z} \to \mathbb{Z}$ definida per $g(n) = f(n + 1)$ també és exhaustiva.

2) Siguin A i B conjunts no buits. És vertader o fals que $\mathcal{P}(A \cap B) = \mathcal{P}(A) \cap \mathcal{P}(B)$? Justifica la resposta.

107

1) Sigui $f : \mathbb{R}^* \to \mathbb{R}^*$ una aplicació injectiva. Proveu que l'aplicació $g : \mathbb{R}^* \to \mathbb{R}^*$ definida per $g(x) = 1/f(x)$ també és injectiva. ($\mathbb{R}^* = \mathbb{R} - \{0\}$.)

2) Siguin Ω un conjunt no buit i $A \subseteq \Omega$. És vertader o fals que $\mathcal{P}(A^c) = \mathcal{P}(A)^c$? Justifica la resposta. ($\mathcal{P}(A)^c$ es calcula a $\mathcal{P}(\Omega)$.)

108

1) Sigui $f : \mathbb{R}^* \to \mathbb{R}^*$ una aplicació exhaustiva. Proveu que l'aplicació $g : \mathbb{R}^* \to \mathbb{R}^*$ definida per $g(x) = 1/f(x)$ també és exhaustiva. ($\mathbb{R}^* = \mathbb{R} - \{0\}$.)

2) Siguin Ω un conjunt no buit i $A \subseteq \Omega$ i $B \subseteq \Omega$ tals que $A \cap B = \emptyset$ i $A \cup B = \Omega$. Què podem dir de A i B? Justifica la resposta.

109

1) Sigui $f : \mathbb{N} \to \mathbb{N}$ una aplicació bijectiva i sigui $a \in \mathbb{N}$. Proveu que l'aplicació $g : \mathbb{N} \to \mathbb{N}$ definida per $g(n) = f(n) + a$ és injectiva, però no exhaustiva.

2) És possible que en un conjunt no buit A hi ha hagi definida una relació R que sigui simètrica i antisimètrica? Justifica la resposta.

110

1) Sigui $f : \mathbb{Z} \to \mathbb{Z}$ una aplicació injectiva. Proveu que l'aplicació $g : \mathbb{Z} \to \mathbb{Z}$ definida per $g(n) = f(n-1) + 1$ és injectiva.

2) És possible que en un conjunt no buit A hi ha hagi definida una relació R que no sigui reflexiva ni antireflexiva? Justifica la resposta

111

1) Sigui $f : \mathbb{Z} \to \mathbb{Z}$ una aplicació exhaustiva. Proveu que l'aplicació $g : \mathbb{Z} \to \mathbb{Z}$ definida per $g(n) = f(n+1) - 1$ és exhaustiva.

2) Siguin A, B i C conjunts no buits tals que $A \times B = A \times C$. Podem afirmar que $B = C$? Justifica la resposta.

112

1) Sigui $f : \mathbb{Z} \to \mathbb{Z}$ una aplicació injectiva. Proveu que l'aplicació $g : \mathbb{Z} \to \mathbb{Z}$ definida per $g(n) = 2f(n-1)$ és injectiva.

2) Siguin A i B conjunts no buits. És vertader o fals que si $Z \subseteq (A \times B)$, llavors hi ha $X \subseteq A$ i $Y \subseteq B$ tals que $Z = X \times Y$? Justifica la resposta.

Principi d'iInducció

113 Proveu per inducció que si $n \geq 2$, llavors:

$$1 \cdot 3 + 2 \cdot 4 + 3 \cdot 5 + \cdots + (n-1)(n+1) = \frac{n(n-1)(2n+5)}{6}$$

114 Proveu per inducció que si $n \geq 1$, llavors:

$$1^2 + 3^2 + 5^2 + \cdots + (2n-1)^2 = \frac{n(2n-1)(2n+1)}{3}$$

115 Proveu per inducció que si $n \geq 1$, llavors:

$$2^2 + 4^2 + 6^2 + \cdots + (2n)^2 = \frac{2n(n+1)(2n+1)}{3}$$

116 Proveu per inducció que si $n \geq 1$, llavors:

$$1 - 4 + 9 - 16 + \cdots + (-1)^{n+1}n^2 = (-1)^{n+1} \cdot \frac{n(n+1)}{2}$$

117 Proveu per inducció que si $n \geq 1$, llavors:

$$\frac{1}{1 \cdot 3} + \frac{1}{3 \cdot 5} + \frac{1}{5 \cdot 7} + \cdots + \frac{1}{(2n-1)(2n+1)} = \frac{n}{2n+1}$$

118 Proveu per inducció que si $n \geq 1$, llavors:

$$\frac{1}{1 \cdot 5} + \frac{1}{5 \cdot 9} + \frac{1}{9 \cdot 13} + \cdots + \frac{1}{(4n-3)(4n+1)} = \frac{n}{4n+1}$$

119 Proveu per inducció que si $n \geq 1$, llavors:

$$\frac{1}{1 \cdot 4} + \frac{1}{4 \cdot 7} + \frac{1}{7 \cdot 10} + \cdots + \frac{1}{(3n-2)(3n+1)} = \frac{n}{3n+1}$$

120 Proveu per inducció que si $n \geq 2$, llavors:

$$\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{4}\right) \cdots \left(1 - \frac{1}{n}\right) = \frac{1}{n}$$

121 Proveu per inducció que si $n \geq 2$, llavors:

$$\left(1-\frac{1}{4}\right)\left(1-\frac{1}{9}\right)\left(1-\frac{1}{16}\right)\cdots\left(1-\frac{1}{n^2}\right)=\frac{n+1}{2n}$$

122 Proveu per inducció que si $n \geq 1$, llavors:

$$\frac{1}{1\cdot 3}+\frac{1}{2\cdot 4}+\frac{1}{3\cdot 5}+\cdots+\frac{1}{n(n+2)}=\frac{n(3n+5)}{4(n+1)(n+2)}$$

1.8 Examen parcial 17/11/2011

123

1) Definiu el concepte de diferència de dos conjunts. Proveu l'equivalència següent:

$$(C \subseteq A - B) \iff (C \subseteq A \wedge C \cap B = \emptyset)$$

on A, B i C són conjunts. Justifiqueu tots els passos.

2) Definiu el concepte d'antiimage d'un subconjunt per una aplicació. Siguin A, B conjunts i $f\colon A \to B$ una aplicació. Proveu, justificant tots els passos, que si $B_1 \subseteq B$, $B_2 \subseteq B$, llavors $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$.

124 Considerem en el conjunt $A = \mathbb{Z} - \{0\}$ la relació R següent:

$$\begin{aligned} m\,R\,n \iff & (\text{signe}(n) = \text{signe}(m) \wedge \text{paritat}(n) = \text{paritat}(m)) \vee \\ & (\text{signe}(n) \neq \text{signe}(m) \wedge \text{paritat}(n) \neq \text{paritat}(m)) \end{aligned}$$

1) Proveu que R és una relació d'equivalència.

2) Trobeu les classes d'equivalència de l'element 1 i de l'element 2. Raoneu la resposta.

3) Expliciteu el conjunt quocient A/R. Raoneu la resposta.

125 Considerem el conjunt $X = \{n \in \mathbb{N} : 1 \leq n \leq 100\}$ i l'aplicació $f\colon X \to X$ definida per:

$$f(n) = \begin{cases} 2n, & \text{si } 1 \leq n \leq 50 \\ 2(n-51)+1, & \text{si } 51 \leq n \leq 100 \end{cases}$$

1) Proveu que f és una aplicació bijectiva.

2) Calculeu $f^{-1}[S]$, si $S = \{n \in X : n \text{ senar}\}$. Justifiqueu la resposta.

1.9 Examen final 20/01/2012

126

1) Expliqueu en què consisteix la tècnica de demostració per reducció a l'absurd? Proveu que $\sqrt{2}$ no és un nombre racional.

2) Sigui $m \geq 1$ un enter. Definiu el concepte de relació de congruència mòdul m i demostreu que és una relació d'equivalència.

127

1) Proveu que la classe $\overline{2957}$ és invertible a $\mathbb{Z}_{4096}$ i trobeu la seva classe inversa. Justifiqueu i expliciteu tots els càlculs que feu per a arribar al resultat.

2) Comproveu que les aplicacions:

$$f\colon \mathbb{Z}_{4096} \to \mathbb{Z}_{4096}, \qquad f(\overline{x}) = \overline{2957} \cdot \overline{x}$$
$$g\colon \mathbb{Z}_{4096} \to \mathbb{Z}_{4096}, \qquad g(\overline{x}) = \overline{3909} \cdot \overline{x}$$

són inverses una de l'altra.

128

1) Justifiqueu que per a ser múltiple de 30 és suficient "ser múltiple de 6 i acabar en 0". És aquesta una condició necessària? Justifiqueu la resposta.

2) Siguin a, m enters tals que $\mathrm{mcd}(a, m) = 2$. Proveu que existeix un enter x tal que $ax \equiv 2 \pmod{m}$.

129

1) Sigui A un conjunt no buit i R una relació reflexiva i transitiva en A. Demostreu que la relació S definida per:

$$x\,S\,y \iff (x\,R\,y \wedge y\,R\,x)$$

és d'equivalència.

2) Sigui $\mathcal{P}$ el conjunt de punts del pla i considerem un punt $O \in \mathcal{P}$. Definim a $\mathcal{P}$ la relació R següent:

$$X\,R\,Y \iff d(X, O) \leq d(Y, O)$$

a) Proveu que R és una relació reflexiva i transitiva.

b) Trobeu les classes d'equivalència per la relació S associada a R segons l'apartat 1).

1.10 Exàmens de taller 2011–2012 Q2

Raonament

130

1) Troba una proposició equivalent a $p \wedge q$ on no hi aparegui cap connectiva diferent de $\neg$ i $\rightarrow$. Justifica l'equivalència (aplicant equivalències conegudes o mitjançant taules de veritat).

2) És suficient ser múltiple de 24 per ser múltiple de 6? I necessari? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

131

1) Troba una proposició equivalent a $p \leftrightarrow q$ on no hi aparegui cap connectiva diferent de $\neg$ i $\rightarrow$. Justifica l'equivalència (aplicant equivalències conegudes o mitjançant taules de veritat).

2) És necessari ser parell per ser múltiple de 3? I suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

132

1) Troba una proposició equivalent a $p \rightarrow (q \vee r)$ on no hi aparegui cap connectiva diferent de $\neg$ i $\rightarrow$. Justifica l'equivalència (aplicant equivalències conegudes o mitjançant taules de veritat).

2) És necessari ser parell per ser múltiple de 6? I suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

133

1) Troba una proposició equivalent a $(p \vee q) \rightarrow r$ on no hi aparegui cap connectiva diferent de $\neg$ i $\rightarrow$. Justifica l'equivalència (aplicant equivalències conegudes o mitjançant taules de veritat).

2) És necessari acabar en 00 per ser múltiple de 50? I suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

134

1) Usant els predicats N per 'ser nombre enter' i P per 'ser enter parell', simbolitza en el llenguatge del càlcul de predicats els enunciats següents:

   a) 'No tots els nombres enters són parells'

   b) 'Tot nombre enter té dues arrels quadrades diferents'

2) Perquè el producte de dos nombres sigui parell, és necessari que algun dels dos nombres sigui parell? I suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

135

1) Usant els predicats P per 'ser enter parell' i S per 'ser enter senar', simbolitza en el llenguatge del càlcul de predicats els enunciats següents:

   a) 'Cap nombre enter és parell i senar alhora'

   b) 'Hi ha dos nombres enters que són parells' (és a dir, al menys dos nombres)

2) Perquè el producte de dos nombres sigui senar, és necessari que tots dos nombres siguin senars? I suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

136

1) Usant els predicats P per 'ser enter parell' i S per 'ser enter senar', simbolitza en el llenguatge del càlcul de predicats els enunciats següents:

   a) 'No hi ha nombres enters parells amb quadrat senar'

   b) 'Hi ha més d'un nombre enter senar'

2) És necessari que dos nombres siguin iguals perquè l'un més el quadrat de l'altre coincideixi amb l'altre més el quadrat de l'un? I suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

Conjunts i aplicacions

137

1) Si A, B i C són conjunts tals que $A - B \subseteq A - C$, es compleix que $C \subseteq B$? Justifica la resposta (la resposta no pot ser un diagrama de Venn).

2) Siguin A i B subconjunts dŠun conjunt no buit Ω? Si $A^c \times B = A \times B^c$, es pot afirmar que $A = \Omega$? Justifica la resposta (la resposta no pot ser un diagrama de Venn). X^c és el complementari de X en Ω.

138

1) Si A, B i C són conjunts, es compleix que $A - (B \cup C) \subseteq (A - B) - C$? Justifica la resposta (la resposta no pot ser un diagrama de Venn).

2) Siguin A, B i C conjunts, A no buit. Si $C \subseteq A \cap (A \times B)$, es pot afirmar que $C = \emptyset$? Justifica la resposta.

139

1) Siguin A i B subconjunts d'un conjunt no buit Ω. Si $A \subseteq B^c$ i $A \cup B = \Omega$, es pot afirmar que $A = B^c$? Justifica la resposta (la resposta no pot ser un diagrama de Venn). X^c és el complementari de X en Ω.

2) Siguin A i B conjunts. Es pot afirmar que $\mathcal{P}(A \times B) = \mathcal{P}(A) \times \mathcal{P}(B)$? Justifica la resposta. $\mathcal{P}(X)$ representa el conjunt de les parts de X.

140

1) Siguin A, B i C subconjunts d'un conjunt no buit Ω. Si $A \supseteq (B \cap C)^c$, es pot afirmar que $A - B = \emptyset$? Justifica la resposta (la resposta no pot ser un diagrama de Venn). X^c és el complementari de X en Ω.

2) És transitiva la relació $\not\subseteq$? Justifica la resposta.

141

1) Siguin A, B i C subconjunts d'un conjunt no buit Ω. Es pot afirmar que $(A \cup B)^c \cap C = B^c \cap (C - A)$? Justifica la resposta (la resposta no pot ser un diagrama de Venn). X^c és el complementari de X en Ω.

2) En el conjunt $\mathbb{N}$ dels nombres naturals definim la relació R de la manera següent: $m \, R \, n$ si, i només si, $|m - n| \leq 4$. És R transitiva? Justifica la resposta.

142

1) Si A, B i C són conjunts, és veritat que $A - (B - C) = (A - B) - C$? Justifica la resposta (la resposta no pot ser un diagrama de Venn).

2) Si A i B són conjunts, es pot afirmar que $\mathcal{P}(\mathcal{P}(A) \times B) = \mathcal{P}(A \times \mathcal{P}(B))$? Justifica la resposta. $\mathcal{P}(X)$ representa el conjunt de les parts de X.

143 Siguin A i B subconjunts d'un conjunt no buit Ω. Si $(A \cap B^c) \cup (A^c \cap B) = A \cup B$, es pot afirmar que $A \cap B = \emptyset$? Justifica la resposta (la resposta no pot ser un diagrama de Venn). X^c és el complementari de X en Ω.

Inducció

144 Sigui $f : \mathbb{N} \to \mathbb{N}$ l'aplicació $f(x) = 2x + 1$. Demostreu que per a tot $n \geq 1$ es compleix $f^{(n)}(x) = 2^n x + 2^n - 1$, on $f^{(n)} = f \circ \cdots \circ f$ (composició de f amb ella mateixa n vegades; $f^{(1)} = f$).

145 Proveu que per a tot $n \geq 3$ es compleix:

$$\frac{1}{n+1} + \frac{1}{n+2} + \frac{1}{n+3} + \cdots + \frac{1}{2n} > \frac{3}{5}$$

146 Sigui $f : \mathbb{Q} \to \mathbb{Q}$ l'aplicació $f(x) = \frac{x}{2} + 1$. Demostreu que per a tot $n \geq 1$ es compleix $f^{(n)}(x) = \frac{x}{2^n} - \frac{1}{2^{n-1}} + 2$, on $f^{(n)} = f \circ \cdots \circ f$ (composició de f amb ella mateixa n vegades; $f^{(1)} = f$).

147 Proveu que per a tot $n \geq 2$ es compleix:

$$\sum_{k=1}^{n} \frac{1}{\sqrt{k}} > \sqrt{n}$$

148 Proveu que per a tot $n \geq 2$ es compleix:

$$\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$$

149 Proveu que per a tot $n \geq 3$ es compleix:

$$\sum_{k=1}^{n} \frac{1}{2^k - 1} < \frac{n}{2}$$

150 Proveu que per a tot $n \geq 2$ es compleix:

$$\frac{1}{2!} + \frac{2}{3!} + \frac{3}{4!} + \cdots + \frac{n-1}{n!} = 1 - \frac{1}{n!}$$

Aritmètica

151 Calculeu el màxim comú divisor i els enters de la identitat de Bézout.

$d = \text{mcd}(a, b) = ax + by$

a	b	d	x	y
2453	2932	1	1365	−1142
4889	2544	1	473	−909
4014	4155	3	442	−427
4097	4315	1	−1247	1184
4861	3169	1	−339	520
3920	4361	49	−10	9
2991	3136	1	1103	−1052

1.11 Examen parcial 26/04/2012

152

1) Definiu el concepte de complementari d'un conjunt respecte d'un conjunt Ω. Proveu l'equivalència següent:

$$A \subseteq B \iff B^c \subseteq A^c$$

on A i B són subconjunts de Ω i X^c denota el complementari de X respecte de Ω. Justifiqueu tots els passos.

2) Definiu el concepte d'imatge d'un subconjunt per una aplicació. Siguin A, B conjunts i $f\colon A \to B$ una aplicació. Proveu, justificant tots els passos, que si $A_1 \subseteq A$, $A_2 \subseteq A$, llavors $f[A_1 \cap A_2] \subseteq f[A_1] \cap f[A_2]$.

153 Siguin x, y dos nombres reals positius. La mitjana aritmètica de x i y es defineix com $(x + y)/2$ i la mitjana geomètrica de x i y com $\sqrt{xy}$.

1) Demostreu que si $x < y$, llavors $x < \frac{x+y}{2} < y$ i $x < \sqrt{xy} < y$.

2) Suposem que m representa la mitjana aritmètica o geomètrica dels nombres reals positius x, y. Proveu que si $m = x$ o $m = y$, llavors $x = y$.

3) Proveu que si $x \neq y$, llavors la mitjana geomètrica és menor que la mitjana aritmètica.

154 Siguin A i B conjunts no buits i $f : A \to B$ una aplicació de A en B. Definim, en A, la relació següent: $xRx' \iff f(x) = f(x')$.

1) Demostreu que R és una relació d'equivalència.

2) Considerem l'aplicació $f : \mathbb{R} \to \mathbb{R}$ definida per $f(x) = \lfloor x \rfloor$ (part entera). Descriviu les classes d'equivalència i el conjunt quocient $\mathbb{R}/R$ en aquest cas. Establiu una aplicació bijectiva entre $\mathbb{R}/R$ i $\mathbb{Z}$.

1.12 Examen final 07/06/2012

155

1) Enunicieu el lema de Gauss i demostreu-lo justificant tots els passos.

2) Definiu el concepte de composició d'aplicacions. Proveu que si $f : A \to B$ i $g : B \to C$ són aplicacions injectives, llavors la composició de f i g és una aplicació injectiva.

156

1) Demostra que en $\mathbb{Z}_m$ no és cert, en general, que de l'afirmació $\overline{a}^2 = \overline{b}^2$ se segueixi que a $\overline{a} = \overline{b}$ o $\overline{a} = -\overline{b}$.

2) Demostreu que si m és un nombre primer i $\overline{a}^2 = \overline{b}^2$ a $\mathbb{Z}_m$, llavors $\overline{a} = \overline{b}$ o $\overline{a} = -\overline{b}$. Justifiqueu tots els passos.

157 Sigui A un conjunt no buit i $f, g : A \to A$ dues aplicacions de A en A tals que $g \circ f = f \circ g$.

1) Demostreu que per a tot $n \geq 1$ es compleix que $f^n \circ g = g \circ f^n$. Justifiqueu tots els passos.

2) Demostreu que per a tot $n \geq 1$ es compleix que $(g \circ f)^n = g^n \circ f^n$. Justifiqueu tots els passos.

   Nota: si h és una aplicació de A en A, es defineix $h^1 = h$, i $h^{n+1} = h \circ h^n$, si $n \geq 1$.
   Indicació: en els dos apartats podeu usar inducció. A l'apartat 2 es fa servir l'apartat 1.

158

1) Sigui X un conjunt no buit i siguin R i S relacions d'equivalència definides sobre X. Demostreu que la relació T definida per:

$$xTy \iff xRy \wedge xSy$$

   és una relació d'equivalència sobre X.

2) Sigui $X = \{n \in \mathbb{N} : 1 \leq n \leq 10\}$. Construïu dues relacions d'equivalència R i S sobre X diferents. És la següent relació U definida sobre X:

$$xUy \iff xRy \vee xSy$$

   una relació d'equivalència?

1.13 Exàmens de taller 2012–2013 Q1

Raonament

159

1) Demostra que una condició suficient perquè la suma de dos nombres sigui parell és que els dos nombres siguin parells. És aquesta una condició necessària? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

2) Formalitza 'x és múltiple de 17' mitjançant una fórmula del càlcul de predicats amb una única variable lliure: x. Els únics predicats atòmics vàlids són les predicacions d'igualtat (una cosa igual a una altra). Formalitza: 'hi ha dos i només dos nombres enters que són múltiples de 17: el 17 i el 34'.

160

1) Demostra que una condició necessària perquè la suma de dos nombres sigui senar és que els nombres en qüestió tinguin paritats diferents. És aquesta una condició suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

2) Formalitza 'el nombre enter x és un quadrat perfecte' mitjançant una fórmula del càlcul de predicats amb una única variable lliure: x. Els únics predicats atòmics vàlids són les predicacions d'igualtat (una cosa igual a una altra). Formalitza: 'hi ha exactament un nombre enter que és un quadrat perfecte'.

161

1) Dona una condició necessària però no suficient perquè un nombre sigui parell. Justifica la resposta. Cal deixar clar, en cada cas, què és el s'intenta provar o refutar.

2) Formalitza: 'les equacions del tipus $x^3 + y^3 = z^3$ no admeten cap solució amb x, y, z enters' mitjançant una fórmula del càlcul de predicats sense variables lliures. Els únics predicats atòmics vàlids són les predicacions d'igualtat (una cosa igual a una altra).

162

1) Dona una condició suficient però no necessària perquè un nombre sigui senar. Justifica la resposta. Cal deixar clar, en cada cas, què és el sŠintenta provar o refutar.

2) Formalitza Şel nombre enter x és producte de dos nombres senars consecutiusŤ mitjançant una fórmula del càlcul de predicats amb una única variable lliure: x. Els únics predicats atòmics vàlids són les predicacions dŠigualtat (una cosa igual a una altra).

163

1) És necessari que un nombre acabi en 7 per ser múltiple de 7? I suficient? Justifica la resposta. Cal deixar clar, en cada cas, què és el sŠintenta provar o refutar.

2) Formalitza 'el nombre enter x és un quadrat perfecte' mitjançant una fórmula del càlcul de predicats amb una única variable lliure: x. Els únics predicats atòmics vàlids són les predicacions d'igualtat (una cosa igual a una altra). Formalitza: 'hi ha nombres enters que són suma de dos quadrats perfectes'.

164

1) Demostra que una condició necessària perquè un nombre sigui múltiple de 20 és que acabi en zero. És aquesta una condició suficient? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

2) Formalitza 'el nombre x és irracional' mitjançant una fórmula del càlcul de predicats amb una única variable lliure: x. Els únics predicats atòmics vàlids són les predicacions dŠigualtat (una cosa igual a una altra). Formalitza: 'no hi ha nombres irracionals'.

165

1) Demostra que una condició suficient perquè un nombre sigui múltiple de 5 és que aquest nombre estigui escrit exclusivament amb els dígits '0' i '5' (les vegades que calgui cada un d'ells). És aquesta una condició necessària? Explica clarament què has de demostrar/refutar per veure la suficiència i la necessitat de les condicions (que quedi clar què vol dir, en aquest context, necessari i què vol dir suficient) i justifica les respostes.

2) Formalitza: 'el producte de dos nombres que són potència de 2 és, també, potència de 2' mitjançant una fórmula del càlcul de predicats sense variables lliures. Els únics predicats atòmics vàlids són les predicacions d'igualtat (una cosa igual a una altra).

166

1) Dona una condició necessària però no suficient perquè un nombre sigui múltiple de 10. Justifica la resposta. Cal deixar clar, en cada cas, què és el sŠintenta provar o refutar.

2) Formalitza 'el nombre enter x és un quadrat perfecte' mitjançant una fórmula del càlcul de predicats amb una única variable lliure: x. Els únics predicats atòmics vàlids són les predicacions d'igualtat (una cosa igual a una altra). Formalitza: 'hi ha dos nombres enters tals que cap d'ells és un quadrat perfecte però, en canvi, el seu producte sí que ho és'.

167

1) Dona una condició suficient però no necessària perquè un nombre sigui múltiple de 11. Justifica la resposta. Cal deixar clar, en cada cas, què és el s'intenta provar o refutar.

2) Formalitza 'el producte de dos nombres senars no pot ser múltiple de 4, però sí que pot ser múltiple de 5' mitjançant una fórmula del càlcul de predicats sense variables lliures. Els únics predicats atòmics vàlids són les predicacions d'igualtat (una cosa igual a una altra).

Conjunts i aplicacions

168 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = 2^n, \quad g(n) = n^2$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

169 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = 2n + 1, \quad g(n) = \left\lfloor \frac{n}{2} \right\rfloor$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

170 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = 3n, \quad g(n) = \left\lfloor \frac{n}{3} \right\rfloor$$

Calculeu $g \circ f$ i proveu que la composició és exhaustiva.

171 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = n^2, \quad g(n) = 2^n$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

172 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = 2^{2n+1}, \quad g(n) = \begin{cases} n, & \text{si } n \text{ és senar} \\ n/2, & \text{si } n \text{ és parell} \end{cases}$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

173 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = 3^{2n}, \quad g(n) = \begin{cases} n, & \text{si } n \text{ és senar} \\ n/2, & \text{si } n \text{ és parell} \end{cases}$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

174 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = 2^{2n+1}, \quad g(n) = \left\lfloor \frac{n}{2} \right\rfloor$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

175 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = \begin{cases} 2n, & \text{si } n \text{ és senar} \\ 2n+1, & \text{si } n \text{ és parell} \end{cases}, \quad g(n) = \left\lfloor \frac{n}{2} \right\rfloor$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

176 Considerem les aplicacions $f : \mathbb{N} \to \mathbb{N}$ i $g : \mathbb{N} \to \mathbb{N}$ definides per:

$$f(n) = 2^n, \quad g(n) = \left\lfloor \frac{n}{2} \right\rfloor + 1$$

Calculeu $g \circ f$ i proveu que la composició és injectiva.

Aritmètica

177 Calculeu el màxim comú divisor i els enters de la identitat de Bézout.

$$d = \operatorname{mcd}(a, b) = ax + by$$

a	b	d	x	y
795	238	2	-29	97
958	203	1	-57	269
953	535	1	32	-57
750	454	2	-23	38
527	334	1	45	-71
874	723	1	-158	191
979	454	1	-211	455
987	736	1	-173	232
887	696	1	215	-274

1.14 Examen parcial 15/11/2012

178

1) Definiu el concepte de complementari d'un conjunt respecte d'un conjunt Ω. Enuncieu les lleis de de Morgan per a conjunts i demostreu-ne una d'elles. Justifiqueu tots els passos.

2) Expliqueu en què consisteix la tècnica de demostració per reducció a l'absurd. Demostreu que $\sqrt{2}$ no és un nombre racional.

179

1) Proveu que les proposicions $p \to (q \to r)$ i $(p \wedge q) \to r$ són equivalents.

2) Sigui Ω un conjunt i $A, B, C \subseteq \Omega$. Proveu que $(A^c \cup (B^c \cap C))^c = (A \cap B) \cup (A - C)$.

3) Determineu si les proposicions següents són certes o falses i justifiqueu les respostes:

$$\text{a)} \quad \forall x \in \mathbb{Z}\, \exists y \in \mathbb{Z}\, (xy = 0); \qquad \text{b)} \quad \exists y \in \mathbb{Z}\, \forall x \in \mathbb{Z}\, (xy = x).$$

180 Considerem la relació R definida al conjunt de punts del pla $P = \mathbb{R}^2$ com segueix:

$$(x, y)R(x', y') \iff x = x'$$

1) Demostreu que R és una relació d'equivalència.

2) Calculeu la classe d'equivalència d'un punt $(a, b) \in P$ i descriviu-la geomètricament.

3) Descriviu el conjunt quocient P/R.

1.15 Examen final 14/01/2013

181

1) Siguin A, B conjunts i $f : A \to B$ una aplicació. Definiu el concepte de imatge d'un subconjunt de A per f. Proveu que si $A_1, A_2 \subseteq A$, aleshores $f[A_1 \cup A_2] = f[A_1] \cup f[A_2]$.

2) Sigui $m \geq 2$ un enter. Definiu el concepte de classe invertible de $\mathbb{Z}_m$. Proveu que si $\operatorname{mcd}(a, m) = 1$, llavors la classe $\overline{a} \in \mathbb{Z}_m$ és invertible.

182 Demostreu per inducció que $1 + 2^{3n-1} + 2^{3n+1} \equiv 0 \pmod 7$, per a tot nombre natural $n \geq 1$.

183

1) Siguin $a, b \in \mathbb{Z}$. Proveu que si $15 \mid ab$, llavors $5 \mid a$ o $5 \mid b$.

2) Siguin p, q, r lletres proposicionals. Proveu que la proposició:

$$((p \to q) \wedge (\neg p \to q)) \to (r \to q)$$

és una tautologia.

184 Considerem l'aplicació $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida per $f(x, y) = 52x + 21y$.

1) Comproveu que $\mathrm{mcd}(52, 21) = 1$ i escriviu la corresponent identitat de Bézout. Justifiqueu tots els passos.

2) Proveu que f és exhaustiva. (Pista: podeu feu servir l'apartat anterior.)

1.16 Examen final de reavaluació 04/02/2013

185

1) Siguin A, B conjunts i $f : A \to B$ una aplicació. Definiu el concepte de anti-imatge d'un subconjunt de B per f. Proveu que si $B_1, B_2 \subseteq B$, aleshores $f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$.

2) Siguin $a, b \in \mathbb{Z}$. Proveu que $\mathrm{mcd}(a, b) = \mathrm{mcd}(a, a - b)$ (teorema d'Euclides).

186 Demostreu per inducció que $3 \cdot 5^{2n+1} + 2^{3n+1} \equiv 0 \pmod{17}$, per a tot nombre enter $n \geq 0$.

187 Donat un punt $(x, y) \in \mathbb{R}^2$, definim:

$$\mathrm{signe}(x, y) = \begin{cases} -1, & \text{si } xy < 0 \\ 0, & \text{si } xy = 0 \\ +1, & \text{si } xy > 0 \end{cases}$$

Definim a $\mathbb{R}^2$ la relació R següent:

$$(x, y)\, R\, (u, v) \iff \mathrm{signe}(x, y) = \mathrm{signe}(u, v)$$

1) Proveu que R és una relació d'equivalència.

2) Trobeu totes les classes d'equivalència.

3) Trobeu el conjunt quocient.

188 Si $n \in \mathbb{Z}$, definim el conjunt $A_n = \{x \in \mathbb{Z} | n \nmid x\}$.

1) Siguin p i q nombres primers diferents. Proveu que $A_p \cup A_q = A_{pq}$.

2) Sigui p un nombre primer. Proveu que $A_p \subset A_{p^2}$.

3) És cert que per a tot enter n i tot enter m, es compleix $A_n \cup A_m = A_{nm}$? Justifiqueu la resposta.

1.17 Exàmens de taller 2012–2013 Q2

Raonament

189 Formalitzeu, sense usar la connectiva $\vee$ (i usant els quantificadors necessaris) els enunciats següents. La resposta no pot començar per $\neg$ i no val inventar-se predicats ad-hoc; utilitzeu els que són habituals a matemàtiques.

1) Tot nombre natural és parell o senar.

2) Hi ha nombres que no són múltiples de 4 però el seu quadrat sí que ho és.

3) No tot nombre real té dues arrels quadrades diferents.

4) Si un nombre real coincideix amb el seu quadrat, llavors aquest nombre és 0 ó 1.

5) L'1 és l'únic nombre real no nul que elevat al quadrat coincideix amb ell mateix.

6) Dos nombres naturals no nuls que tenen els mateixos divisors són iguals.

7) Nombres reals amb el mateix quadrat poden ser diferents.

190 Sigui n un nombre natural. És necessari que n^2 acabi en 1 perquè n acabi en 1? És suficient? Justifica les respostes i deixa clar, en cada cas, a què estàs responent.

191 Sigui n un nombre natural. És necessari que n acabi en 3 perquè n^2 acabi en 9? És suficient? Justifica les respostes i deixa clar, en cada cas, a què estàs responent.

192 Sigui n un nombre natural. És necessari que n acabi en 6 perquè n^2 acabi en 6? És suficient? Justifica les respostes i deixa clar, en cada cas, a què estàs responent.

193 Sigui n un nombre natural. És necessari que n acabi en 2 perquè n^2 acabi en 4? És suficient? Justifica les respostes i deixa clar, en cada cas, a què estàs responent.

194 Sigui n un nombre natural. És necessari que n acabi en 3 perquè n^3 acabi en 7? És suficient? Justifica les respostes i deixa clar, en cada cas, a què estàs responent.

195 Sigui n un nombre natural. És necessari que n acabi en 6 perquè n^4 acabi en 6? És suficient? Justifica les respostes i deixa clar, en cada cas, a què estàs responent.

196 Sigui n un nombre natural. És necessari que n acabi en 3 perquè n^4 acabi en 1? És suficient? Justifica les respostes i deixa clar, en cada cas, a què estàs responent.

Aritmètica i inducció

197

1) Trobeu una solució entera (x_0, y_0) de l'equació $51x + 75y = 3$ tal que $y_0 > 0$.

2) Proveu que si $n \geq 1$, llavors $7^n - 1$ és múltiple de 6.

198

1) Trobeu una solució entera (x_0, y_0) de l'equació $79x + 69y = 1$ tal que $y_0 > 0$.

2) Proveu que si $n \geq 1$, llavors $6^n - 1$ és múltiple de 5.

199

1) Trobeu una solució entera (x_0, y_0) de l'equació $61x + 78y = 1$ tal que $x_0 > 0$.

2) Proveu que si $n \geq 1$, llavors $11^n - 1$ és múltiple de 5.

200

1) Trobeu una solució entera (x_0, y_0) de l'equació $77x + 67y = 1$ tal que $x_0 > 0$.

2) Proveu que si $n \geq 1$, llavors $12^n - 1$ és múltiple de 11.

201

1) Trobeu una solució entera (x_0, y_0) de l'equació $63x + 59y = 1$ tal que $y_0 > 0$.

2) Proveu que si $n \geq 1$, llavors $13^n - 1$ és múltiple de 12.

202

1) Trobeu una solució entera (x_0, y_0) de l'equació $81x + 77y = 1$ tal que $y_0 < 0$.

2) Proveu que si $n \geq 1$, llavors $(-5)^n - 1$ és múltiple de 6.

203

1) Trobeu una solució entera (x_0, y_0) de l'equació $70x + 83y = 1$ tal que $y_0 < 0$.

2) Proveu que si $n \geq 1$, llavors $(-10)^n - 1$ és múltiple de 11.

1.18 Examen parcial 2/5/2013

204

1) Definiu el concepte d'unió de conjunts. Siguin A, B i C conjunts. Demostreu:

$$A \cup B \subseteq C \iff (A \subseteq C \wedge B \subseteq C)$$

2) Definiu el concepte de composició d'aplicacions. Siguin A, B i C conjunts i $f : A \to B$ i $g : B \to C$ aplicacions. Demostreu que si f i g són injectives, aleshores $g \circ f$ és injectiva.

205

1) Sigui $f : \mathbb{R} - \{7\} \to \mathbb{R} - \{5\}$ l'aplicació definida per:

$$f(x) = \frac{5x}{x-7}$$

Proveu que és bijectiva i trobeu la seva inversa.

2) Definim a $\mathbb{N} \times \mathbb{N}$ la relació R:

$$(x, y)R(x', y') \iff x + y' = x' + y$$

Proveu que R és transitiva.

206 Sigui R una relació d'equivalència en un conjunt A. Donats a i b elements de A, demostrar l'equivalència de les afirmacions següents:

1) $[a] \cap [b] \neq \emptyset$

2) $a \in [b]$

3) $[a] \subseteq [b]$

1.19 Examen final 6/6/2013

207

a) Proveu que hi ha infinits nombres primers (teorema d'Euclides).

b) Sigui $m \geq 2$ un enter. Demostreu que si $a \equiv b \pmod{m}$ i $a' \equiv b' \pmod{m}$, llavors $a + a' \equiv b + b' \pmod{m}$.

208

a) Calculeu els inversos de totes les classes no nul·les de $\mathbb{Z}_7$. Justifiqueu tots els passos.

b) Resoleu el sistema d'equacions següent a $\mathbb{Z}_7$:

$$\begin{aligned} \overline{5}\cdot\overline{x}-\overline{5}\cdot\overline{y}&=\overline{4}\\ \overline{3}\cdot\overline{x}+\overline{2}\cdot\overline{y}&=\overline{5}\end{aligned}$$

Justifiqueu tots els passos.

209 Si $n\in\mathbb{Z}$, definim el conjunt $M_n=\{x\in\mathbb{Z}: n\mid x\}$.

1) Siguin p i q nombres primers diferents. Proveu que $M_p\cap M_q=M_{pq}$.

2) Sigui p un nombre primer. Proveu que $M_{p^2}\subset M_p$.

210 Proveu per inducció que si $n\geq 1$, aleshores:

$$2\cdot 6\cdot 10\cdots(4n-2)=\frac{(2n)!}{n!}$$

1.20 Examen final de reavaluació 10/07/2013

211 Definim $f:\mathbb{Z}_7\to\mathbb{Z}_7$, $f(\overline{x})=\overline{4}\cdot\overline{x}+\overline{2}$. Considereu els conjunts $A=\{\overline{1},\overline{2},\overline{3},\overline{5}\}$ i $B=\{\overline{1},\overline{5},\overline{6}\}$.

1) Obteniu $f[S]$, on $S=A-B$.

2) Estudieu si f és bijectiva, si té inversa i, en cas afirmatiu, obteniu f^{-1}.

3) Obteniu $f^{-1}[A\cap B]$.

212 Demostreu que $6|(7^n+5)$, per a tot n natural:

1) Per inducció.

2) Per congruències.

3) Per classes de residus.

213

1) Sigui $n\in\mathbb{N}$. Calculeu $\mathrm{mcd}(3n+10,2n+7)$.

2) Sigui $n\in\mathbb{Z}$. Proveu que n^2+3n+6 és parell.

3) Sigui $n\in\mathbb{N}$. Calculeu $\displaystyle\sum_{k=0}^{n}\binom{n}{k}7^k$.

1.21 Examen parcial 17/10/2013

214 Sigui n un nombre enter. Demostreu que les proposicions següents són equivalents:

a) n és senar;

b) n^2 és de la forma $4k+1$, per a algun $k \in \mathbb{Z}$;

c) n^2+1 és parell.

Justifiqueu tots els passos.

215 Demostreu, per inducció sobre n, que si $n \geq 1$, aleshores:

$$-1+3-5+\cdots+(-1)^n(2n-1)=(-1)^n \cdot n$$

Expliciteu, al pas inductiu, la hipòtesi d'inducció i el què voleu demostrar. Justifiqueu tots els passos.

1.22 Examen parcial 14/11/2013

216 Siguin A, B i C conjunts. Proveu que si $A \cap B = A$, llavors $A \cup B \cup C = B \cup C$. Justifiqueu tots els passos.

217 Sigui $n \geq 2$ i considerem el conjunt $X = \{0,1\}^n$ de les paraules binàries de longitud n. Considerem la relació R definida en X de la manera següent:

$$x_1 x_2 \cdots x_n \, R \, y_1 y_2 \cdots y_n \Leftrightarrow x_1 = y_1 \wedge x_2 = y_2$$

a) Comproveu que R és una relació d'equivalència.

b) Trobeu les classes d'equivalència, dient quin són els elements de cada classe.

c) Doneu per extensió el conjunt quocient i digueu quants elements té.

Observació: $\{0,1\}^n = \{0,1\} \times \cdots^n \times \{0,1\}$. Un element $(x_1, x_2, \ldots, x_n) \in \{0,1\}^n$ també l'escrivim com a $x_1 x_2 \ldots x_n$.

1.23 Examen final 09/01/2014

218 Considerem l'equació $a\,x + (3+2a)\,y = 10$, on $a \in \mathbb{Z}$.

1) Determineu tots els enters a tals que l'equació anterior té almenys una solució entera.

2) Trobeu totes les solucions enteres de l'equació anterior quan $a = 31$.

219 Sigui $n \in \mathbb{N}$. Proveu que si $n \equiv 4 \pmod 6$, aleshores $10^n + 3 \equiv 0 \pmod 7$.

220 Considerem l'aplicació $f : \mathbb{Z}_{400} \to \mathbb{Z}_{400}$ definida de la manera següent:

$$f(\overline{x}) = \begin{cases} \overline{7} \cdot \overline{x} + \overline{1}, & \text{si } \overline{x} \in \{\overline{0}, \overline{2}, \cdots, \overline{398}\} \\ \overline{4} \cdot \overline{x} + \overline{3}, & \text{si } \overline{x} \in \{\overline{1}, \overline{3}, \cdots, \overline{399}\} \end{cases}$$

a) És f injectiva?

b) És f exhaustiva?

c) Calculeu $f^{-1}[\{\overline{201}\}]$.

1.24 Examen de recuperació del primer parcial 09/01/2014

221 Proveu per inducció que si $n \geq 1$, llavors $3 \cdot 5^{2n+1} + 2^{3n+1}$ és un múltiple de 17. Expliciteu clarament, en el pas inductiu, quina és la hipòtesi d'inducció i el que s'ha de demostrar.

222 Considerem les proposicions següents referides a nombres naturals:

P1) $\forall x \, \exists y \; (x + y = 0)$

P2) $\exists x \, \forall y \; (x + y = y)$

a) Negueu-les i expresseu el resultat final sense utilitzar el símbol $\neg$. Justifiqueu tots els passos.

b) Digueu si són certes o falses i justifiqueu la resposta en cada cas.

1.25 Examen de recuperació del segon parcial 09/01/2014

223 Siguin A i B conjunts. Demostreu que si $A \subseteq B$, llavors $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. És cert el recíproc? Justifiqueu la resposta.

224 Definim a $\mathbb{R}^2$ la relación R següent:

$$(x_1, y_1)R(x_2, y_2) \Leftrightarrow \frac{y_1}{x_1^2 + 1} = \frac{y_2}{x_2^2 + 1}$$

a) Proveu que R és una relació d'equivalència.

b) Trobeu la classe d'equivalència dels elements $(0, 0)$, $(0, 1)$ i $(0, -2)$.

c) Trobeu la classe d'equivalència de $(a, b) \in \mathbb{R}^2$. Descriviu-la geomètricament.

1.26 Examen final de reavaluació 07/02/2014

225 Siguin $A, B, C \subseteq \Omega$ conjunts tals que $B \cap C^c = \emptyset$.

a) Demostreu que $A \setminus (A \setminus B) \subseteq C$

b) Demostreu que, en general, $C \nsubseteq A \setminus (A \setminus B)$.

226 Considerem l'aplicació $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ definida per:

$$f(x, y) = 333x + 120y$$

a) És injectiva? Justifiqueu la resposta.

b) És exhaustiva? Justifiqueu la resposta.

c) Calculeu $f^{-1}[\{3\}]$.

227 Demostreu que, per a qualsevol enter $n \geq 2$, els dos últims dígits del nombre $11^n - 10n$ són 01.

228 Considerem, al conjunt $\mathbb{Z}$, la relació:

$$xRy \Leftrightarrow \mathrm{mcd}(x, 4) = \mathrm{mcd}(y, 4)$$

a) Demostreu que R és d'equivalència.

b) Doneu una descripció de cada una de les classes d'equivalència. En la descripció no es pot usar $\mathrm{mcd}(\cdot, 4)$ ni cap relació de congruència. Doneu el conjunt quocient $\mathbb{Z}/R$.

1.27 Examen parcial 20/03/2014

229 Proveu per inducció que si $n \geq 1$, llavors:

$$\sum_{k=1}^{n} k(k+2) = \frac{n(n+1)(2n+7)}{6}$$

Al pas inductiu, indiqueu clarament quina és la hipòtesi d'inducció i el que heu de demostrar. Justifiqueu tots els passos.

230 Siguin $x, y \in \mathbb{Z}$. Proveu que les proposicions següents són equivalents:

a) $x - y$ és senar;

b) $x + y$ és senar;

c) $3x + y$ és senar.

1.28 Examen parcial 30/04/2014

231 Definim a $\mathbb{R}$ la relació S per:

$xSy \Leftrightarrow x - y \in \mathbb{Q}$

a) Proveu que S és una relació d'equivalència a $\mathbb{R}$.

b) Calculeu la classe d'equivalència de 0.

Justifiqueu les respostes.

232 Definim les aplicacions $f, g : \mathbb{Z} \to \mathbb{Z}$ de la manera següent:

$$f(n) = \begin{cases} n^2, & \text{si } n \text{ és parell} \\ (n-1)^2, & \text{si } n \text{ és senar} \end{cases} \qquad g(n) = \begin{cases} 3n, & \text{si } n \text{ és parell} \\ 3n+1, & \text{si } n \text{ és senar} \end{cases}$$

a) Proveu que per a tot $n \in \mathbb{Z}$ es compleix $(g \circ f)(n) = 3f(n)$.

b) És f una aplicació injectiva? Justifiqueu la resposta.

c) És g una aplicació exhaustiva? Justifiqueu la resposta.

d) Sigui $T = \{3k : k \in \mathbb{Z}\}$. Calculeu el conjunt $f[g^{-1}[T]]$.

1.29 Examen final 12/06/2014

233 Volem demostrar que si $n \in \mathbb{Z}$, llavors $5n^2 + 10$ no és el quadrat d'un nombre enter. Ho farem per reducció a l'absurd. Suposem que existeixen $n, m \in \mathbb{Z}$ tals que $5n^2 + 10 = m^2$.

1) Proveu que $5 \mid m$.

2) Proveu que $5 \mid (n^2 + 2)$.

3) Proveu que $\overline{n}^2 = \overline{3}$, a $\mathbb{Z}_5$.

Deduïu que si $n \in \mathbb{Z}$, llavors $5n^2 + 10$ no pot ser el quadrat d'un nombre enter.

234 Una banda de 13 pirates s'apodera d'una caixa de monedes d'or. Després de repartir-les equitativament queda un residu de 8 monedes. Moren 2 pirates, es torna a repartir i es té un residu de 3 monedes. Desapareixen 3 pirates més, es torna a repartir i es té un residu de 5 monedes. Quin és, com a mínim, el botí dels pirates?

235

a) Calculeu totes les solucions enteres de l'equació $13x - 47y = 10$.

b) Trobeu la solució (x, y) de l'equació anterior tal que y té el valor negatiu més gran possible.

1.30 Examen de recuperació del primer parcial 12/06/2014

236 Demostreu per inducció que per a tot $n \geq 0$:

$$\sum_{k=0}^{n} 2^k \cdot (2k+1) \cdot k! = (n+1)! \cdot 2^{n+1} - 1$$

Indiqueu clarament, al pas inductiu, quina és la hipòtesi d'inducció i el que volem demostrar.

237

a) Siguin p, q, r lletres proposicionals. Quina de les fórmules proposicionals següents és una tautologia?

1) $((p \vee q) \to r) \to ((p \to r) \vee (q \to r))$
2) $((p \to r) \vee (q \to r)) \to ((p \vee q) \to r)$

b) Siguin $a, b, c \in \mathbb{Z}$. Proveu que si $a + b = c$, llavors almenys un dels enters a, b o c és parell.

1.31 Examen de recuperació del segon parcial 12/06/2014

238 Definim a $\mathbb{R}^2$ la relació S de la manera següent:

$$(a, b)S(c, d) \Leftrightarrow a + b = c + d$$

a) Proveu que S és una relació d'equivalència.

b) Calculeu la classe d'equivalència de l'element $(3, 1)$ i descriviu-la geomètricament.

c) Sigui $D = \{(x, y) \in \mathbb{R}^2 : y = x\}$. Proveu que per a cada classe d'equivalència $[(a, b)]$, la intersecció $D \cap [(a, b)]$ té només un element i trobeu-lo.

239 Definim l'aplicació $f : \mathbb{R}^2 \to \mathbb{R}^2$ per la fórmula següent:

$$f(x, y) = (x + y, x - y)$$

a) Proveu que f és una aplicació injectiva.

b) Proveu que f és una aplicació exhaustiva.

c) Justifiqueu que f té inversa i trobeu-la.

d) Calculeu $f^{-1}(6, 2)$.

1.32 Examen final de reavaluació 11/07/2014

240

1) Se sap que la proposició $\forall\, x \in X\,(A(x) \longrightarrow B(x))$ és certa. Considerem els conjunts:

$$U = \{x \in X \mid A(x)\}, \qquad V = \{x \in X \mid B(x)\}.$$

Raona quina de les inclusions següents és certa: $U \subseteq V$ o $V \subseteq U$.

2) Sigui $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^3 + x$. Demostreu:

$$\forall a \in \mathbb{R}\,(a \neq 0 \Rightarrow f(a) \neq 0)$$

3) Demostreu que $15 \cdot 2^n \equiv 1 \pmod 7$, per a tot n natural i múltiple de 3.

241 Una relació binària R en un conjunt A és *circular* quan es compleix:

$$\forall a, b, c \in A\,(aRb \wedge bRc \Rightarrow cRa)$$

Proveu:

1) Si R és d'equivalència, llavors és circular.

2) Si R és reflexiva i circular, llavors és simètrica.

3) Si R és reflexiva i circular, llavors és d'equivalència.

242 Es dóna el sistema de congruències següent:

$$\begin{cases} x \equiv a \pmod m \\ x \equiv b \pmod n \end{cases}$$

1) Demostreu que el sistema té solució si, i només si, es compleix $d \mid a - b$, éssent $d = \text{mcd}(m, n)$.

2) Deduïu que el sistema:

$$\begin{cases} x \equiv 1 \pmod{12} \\ x \equiv b \pmod{14} \end{cases}$$

té solució si, i només si, b és senar.

3) Resoleu el sistema anterior quan $b = 17$.

1.33 Examen parcial 16/10/2014

243 Considerem la proposició P següent:

> *Per a tots els enters m i n, si $m-n$ és múltiple de 4, aleshores m^2-n^2 és múltiple de 4.*

a) Formalitzeu la proposició P. (Totes les variables prenen valors enters.)

b) Negueu l'expressió que heu obtingut a l'apartat anterior. (No poden quedar quantificadors negats directament.)

c) Proveu que la proposició P és certa. Indiqueu quin mètode de demostració utilitzeu.

d) Considereu la proposició R següent:

> *Per a tots els enters m i n, si m^2-n^2 és múltiple de 4, aleshores $m-n$ és múltiple de 4.*

Què hem de fer si volem provar que R és falsa? Proveu que R és una proposició falsa.

244 Calculeu el valor de l'enter positiu n sabent que:

$$\sum_{k=-n}^{n}(3k+5)=1005.$$

1.34 Examen parcial 17/11/2014

245 Siguin $X=\{1,2,3,4\}$ i $Y=\{4\}$. Considerem al conjunt $\mathcal{P}(X)$ de las parts de X la relació R definida per:

$$A\ R\ B \Leftrightarrow A\cup Y=B\cup Y$$

a) Proveu que R és una relació d'equivalència.

b) Trobeu totes les classes d'equivalència.

c) Trobeu el conjunt quocient $\mathcal{P}(X)/R$.

246 Proveu per inducció que si $n\geq 2$, aleshores:

$$\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)=\frac{1+n}{2n}$$

Indiqueu clarament, en el pas inductiu, quina és la hipòtesi d'inducció i què hem de demostrar.

1.35 Examen final 14/01/2015

247 Considerem l'aplicació $f : \mathbb{Z}_{80} \to \mathbb{Z}_{80}$ definida per $f(\overline{x}) = \overline{2} \cdot \overline{x} + \overline{1}$. Siguin $A = \{\overline{1}, \overline{3}, \overline{22}, \overline{43}\}$ i $B = \{\overline{3}, \overline{50}\}$.

a) Calculeu els conjunts $f[A]$ i $f^{-1}[B]$.

b) És f injectiva? És f exhaustiva?

c) Comproveu que $f[A \cap f^{-1}[B]] = f[A] \cap B$.

248 Calculeu $21456^{16140} \pmod{101}$.

249

a) Siguin $a, b \in \mathbb{Z}$ i p, q nombres primers diferents. Demostreu que $a \equiv b \pmod{pq}$ si, i només si, $a \equiv b \pmod{p}$ i $a \equiv b \pmod{q}$.

b) Calculeu les solucions de $x^2 \equiv 4 \pmod{p}$, on p és un nombre primer senar.

c) Proveu que la congruència $x^2 \equiv 4 \pmod{35}$ té 4 solucions mòdul 35. Trobeu les solucions de la congruència que siguin diferents de $x \equiv 2 \pmod{35}$ i de $x \equiv -2 \pmod{35}$.

1.36 Examen de recuperació del primer parcial 14/01/2015

250

1) Sigui $n \in \mathbb{N}$. Proveu l'equivalència següent: n és parell $\Leftrightarrow$ n^3 és parell.

2) Proveu que $\sqrt[3]{2}$ és irracional. (Podeu usar l'apartat anterior, si és necessari.)

251 Considerem la proposició següent: "Hi ha un nombre natural que és més petit o igual que tots els nombres naturals".

a) Formalitzeu la proposició anterior, tenint en compte que: l'univers de discurs és el conjunt dels nombres naturals; podeu usar els quantificadors i connectives lògiques, el símbol $\leq$ i les variables que siguin necessàries.

b) Negueu la formalització que heu obtingut a l'apartat anterior (a l'expressió final no hi pot aparèixer el símbol de negació).

1.37 Examen de recuperació del segon parcial 14/01/2015

252 Sigui $n \geq 1$ un nombre enter. Considerem el conjunt $X = \{1, 2, \ldots, n\}$. Considerem a $\mathcal{P}(X)$ la relació R definida per: $A\ R\ B$ si, i només si, $|A| = |B|$. ($|A|$ denota el cardinal del conjunt A.)

a) Proveu que R és una relació d'equivalència.

b) Trobeu la classe d'equivalència de $\{1, 3, 4, 5\}$ quan $n = 5$.

c) Trobeu el conjunt quocient $\mathcal{P}(X)/R$ i digueu quants elements té.

253 Proveu que si $n \geq 1$, llavors $\sum_{k=1}^{n} k5^k = (5 + (4n - 1)5^{n+1})/16$.

1.38 Examen final de reavaluació 6/02/2015

254 Considerem l'aplicació $f : \mathbb{Z}_{15} \to \mathbb{Z}_{15}$ definida per $f(\overline{x}) = \overline{5x}$.

1) Calculeu els conjunts $f[\mathbb{Z}_{15}]$ i $f^{-1}[\{\overline{0}\}]$.

2) Estudieu si f és injectiva o exhaustiva.

3) Demostreu que $f \circ f \circ f = f$.

4) Considerem la relació R en $\mathbb{Z}_{15}$ definida per $\overline{x} R \overline{y}$ si, i només si, $f(\overline{x}) = f(\overline{y})$.

   a) Proveu que R és una relació d'equivalència.
   b) Trobeu totes les classes d'equivalència.

255 Siguin A, B i C conjunts.

1) Demostreu que si $A \cap B = \emptyset$, $A \cap C = \emptyset$ i $B \cap C = \emptyset$, llavors $A \cap B \cap C = \emptyset$. Indiqueu quin mètode de demostració utilitzeu i justifiqueu els passos.

2) Escriviu el recíproc de la implicació anterior. És certa aquesta implicació? Per què? Justifiqueu la resposta.

3) Considerem la propietat: "si $A \neq \emptyset$ i $A \subseteq B \cup C$, aleshores $B \cap C \neq \emptyset$". És certa o falsa? Justifiqueu la resposta.

256 Proveu per inducció que si $n \geq 1$, llavors:

$$2 - 3 + 2^2 - 3^2 + \cdots + 2^n - 3^n = \frac{2^{n+2} - 3^{n+1} - 1}{2}$$

257 Trobeu l'enter positiu x més petit tal que:

$$x \equiv 425 \pmod{23}, \quad x \equiv 145 \pmod{51}, \quad x \equiv 293 \pmod{91}$$

258 Considerem el polinomi $p(x) = x^{1024} + x^{512} + x^{256} + 1$. Calculeu $p(23)$ mòdul 251.

1.39 Examen parcial 23/03/2015

259 Considerem la proposició P següent:

Tot enter és tal que la seva meitat és entera o la seva meitat sumada amb $0,5$ *és entera.*

a) Formalitzeu la proposició P. (Totes les variables prenen valors enters.)

b) Negueu l'expressió que heu obtingut a l'apartat anterior. (No poden quedar quantificadors negats directament.)

c) Indiqueu quina seria la hipòtesi si volem demostrar la proposició P utilitzant el mètode de reducció a l'absurd.

d) Proveu que la proposició P és certa. Indiqueu quin mètode de demostració utilitzeu.

260 Proveu per inducció que si $n \geq 2$, llavors:

$$\sum_{i=2}^{n} \frac{1}{i^2 - 1} = \frac{(n-1)(3n+2)}{4n(n+1)}.$$

1.40 Examen parcial 11/05/2015

261

1) Construïu dos conjunts A i B que compleixin totes les condicions següents: $A \subseteq B$; $A \in B$; $A \cap B = \{1\}$.

2) Siguin A, B i C conjunts tals que $A \subseteq B \subseteq C$. Demostreu que:

$$C \setminus A = (C \setminus B) \cup (B \setminus A).$$

3) Siguin $X = \{1, 2, 3, 4\}$ i $M = \{1, 2\}$.

   a) Escriviu per extensió el conjunt $\mathcal{P}(X)$.

b) Definim l'aplicació:

$$f : \mathcal{P}(X) \to \mathcal{P}(X), \qquad f(A) = A \cap M.$$

Estudieu si f és injectiva i si f és exhaustiva.

262 Definim a $\mathbb{R} - \{0\}$ la relació:

$$a\,R\,b \Leftrightarrow a - \frac{1}{a} = b - \frac{1}{b}$$

1) Demostreu que R és una relació d'equivalència.

2) Proveu que si $a\,R\,b$, llavors $(a-b)(ab+1) = 0$.

3) Calculeu la classe d'equivalència d'un nombre real no nul a.

4) Escriviu el conjunt quocient.

1.41 Examen final 09/06/2015

263 Trobeu l'enter positiu x més petit tal que:

$$x \equiv 5 \pmod 7, \quad x \equiv 12 \pmod 8, \quad x \equiv 13 \pmod 9, \quad x \equiv 16 \pmod{11}$$

264 Sigui p i q nombres primers diferents.

a) Demostreu que $p^{q-1} + q^{p-1} \equiv 1 \pmod p$ i que $p^{q-1} + q^{p-1} \equiv 1 \pmod q$. (Pista: podeu usar el teorema petit de Fermat.)

b) Deduïu de l'apartat a) que $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$.

c) Calculeu $\overline{23}^{28} + \overline{29}^{22}$ a $\mathbb{Z}_{667}$.

265

a) Trobeu totes les solucions de l'equació $2m + 3d = 78$ amb $d, m \in \mathbb{Z}$ i $d \geq 1$ i $m \geq 1$.

b) Demostreu que si $d, m \in \mathbb{Z}$ són enters positius tals que $2m + 3d = 78$ i $d \mid m$, llavors $d = 2$ i $m = 36$ o $d = 6$ i $m = 30$.

c) Trobeu tots els enters positius a, b tals que $a < b$, $\mathrm{mcd}(a, b) = d$, $\mathrm{mcm}(a, b) = m$, $2m + 3d = 78$.

1.42 Examen de recuperació del primer parcial 09/06/2015

266 Proveu que si $n \geq 1$, llavors:

$$\sum_{k=1}^{n} \frac{1}{(4k-3)(4k+1)} = \frac{n}{4n+1}.$$

267 Considerem la proposició següent: "Per a tot nombre racional x existeix un nombre enter n tal que nx és enter".

a) Formalitzeu la proposició anterior.

b) Negueu la formalització que heu obtingut a l'apartat anterior (a l'expressió final no hi pot aparèixer el símbol de negació).

c) Digueu si la proposició donada és certa o falsa i justifiqueu la vostra afirmació.

1.43 Examen de recuperació del segon parcial 09/06/2015

268 Sigui F el conjunt d'alumnes de l'assignatura de FM de la FIB i sigui $X = F \times F$. Suposem que hi ha 8 grups, de l'1 al 8. Si $a \in F$, denotem per $g(a)$ el seu grup. Definim una relació a X:

$$(a, b)R(c, d) \Leftrightarrow g(a) + g(b) = g(c) + g(d).$$

a) Proveu que R és una relació d'equivalència.

b) Trobeu totes les classes d'equivalència.

c) Trobeu el conjunt quocient X/R i digueu quants elements té.

269 Definim l'aplicació $f : \mathbb{N} \to \mathbb{N}$ per:

$$f(n) = \begin{cases} 2n+1, & \text{si } n \text{ parell} \\ n+2, & \text{si } n \text{ senar} \end{cases}$$

a) És f injectiva? És f exhaustiva?

b) Trobeu subconjunts $A, B \subseteq \mathbb{N}$ tals que: $f[A \cap B] = f[A] \cap f[B]$.

c) Trobeu subconjunts $A, B \subseteq \mathbb{N}$ tals que: $f[A \cap B] \subset f[A] \cap f[B]$ (inclusió estricta).

1.44 Examen final de reavaluació 13/07/2015

270

1) Sigui n enter. Proveu per classes de residus que $6|n^3 - n$.
2) Sigui n enter. Proveu per congruències que $2|n^2 + n - 2$.
3) Sigui n nombre natural. Proveu que $2|n^3 + n + 6$ per inducció i utilitzant classes de residus.

271 Considereu la propietat $22|23^n - 1$, per a n nombre natural.

1) Demostreu-la per inducció.
2) Demostreu-la aplicant la fórmula del binomi de Newton.
3) Estudieu si es pot demostrar aplicant la fórmula:

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}).$$

272

1) Demostreu que l'aplicació $f : \mathbb{Z}_{13} \to \mathbb{Z}_{13}$, $f(\overline{x}) = \overline{5} \cdot \overline{x} + \overline{7}$ és bijectiva i obteniu f^{-1}.
2) Calculeu $\operatorname{mcd}(3n+4, 4n+5)$, per a n nombre natural.

1.45 Examen parcial 15/10/2015

273

a) Siguin $P(x)$, $Q(x)$, $R(x)$ predicats definits en un univers de discurs U. Obteniu, justificant cada pas que feu, la negació de la proposició següent i expresseu el resultat final només amb les connectives conjunció i negació:

$$\forall\, x\, (P(x) \to (Q(x) \vee R(x))).$$

Raoneu per què, en el cas $R(x) = \neg Q(x)$, la proposició anterior és certa.

b) Siguin a, b, c enters. Demostreu que si $a + b + c = 0$, llavors a és parell o b és parell o c és parell.

274 Demostreu que:

$$\sum_{k=5}^{n+35} (k+7)^2 - \sum_{k=-30}^{n} (k+28)^2 = \sum_{k=1}^{n+31} (28k + 112)$$

Indicació: expresseu cada sumatori de l'esquerra com a un sumatori des de 1 fins a $n+31$.

1.46 Examen parcial 16/11/2015

275 Siguin A i B conjunts. Demostreu que:

$$(A \cup B) \setminus (A \cap B) = (A \setminus B) \cup (B \setminus A).$$

276 Demostreu per inducció que si $n \geq 1$, llavors:

$$\prod_{i=1}^{n} \left(1 - \frac{1}{(i+1)^2}\right) = \frac{n+2}{2(n+1)}.$$

277 Sigui $\Omega = \{1, 2, 3, 4\}$ i considerem el subconjunt $X = \{1, 2, 3\}$. En el conjunt de les parts $\mathcal{P}(\Omega)$ considerem la relació d'equivalència R definida per $A\ R\ B$ si i només si $A \setminus X = B \setminus X$. Calculeu totes les classes d'equivalència, donant de cada classe tots els seus elements.

1.47 Examen final 12/10/2016

278 Sigui $a \in \mathbb{Z}$. Considerem l'aplicació:

$$f_a : \mathbb{Z}_{100} \to \mathbb{Z}_{100}, \qquad f_a(\overline{x}) = \overline{a} \cdot \overline{x} + \overline{4}$$

a) Proveu que si $\operatorname{mcd}(a, 100) = 1$, llavors f_a és bijectiva.

b) Trobeu l'aplicació inversa de f_{77}. Calculeu $f_{77}^{-1}[\{\overline{30}\}]$.

c) Proveu que f_{55} no és injectiva ni exhaustiva.

279 Calculeu a $\mathbb{Z}_{53}$ la suma:

$$S = \sum_{k=0}^{31} \overline{11}^{\,k}$$

Pista: podeu usar, si us cal, la identitat polinomial $\left(\sum_{k=0}^{n} x^k\right)(x-1) = x^{n+1} - 1$.

280 A un ordinador s'executen simultàniament tres procesos que periòdicament accedeixen al mateix recurs compartit. L'ordinador es bloqueja quan els tres procesos accedeixen al recurs al mateix temps. El procés A accedeix per primer cop al recurs a les 10h i després hi accedeix cada 5 minuts. El procés B accedeix al recurs per primera vegada a les 10:02h i després hi accedeix cada 12 minuts. Finalment, el procés C accedeix al recurs per primer cop a les 10:06h i després ho fa cada 7 minuts.

a) Calculeu cada quants minuts es bloqueja l'ordinador.

b) A quina hora es produeix el primer bloqueig?

1.48 Examen de recuperació del primer parcial 12/01/2016

281 Considerem les proposicions següents sobre nombres naturals:

P1) Existeixen dos nombres naturals diferents compresos entre 1 i 20 que no són múltiples de 4.

P2) Donats dos nombres naturals arbitraris diferents compresos entre 1 i 20, algun dels dos és múltiple de 4.

a) Formalitzeu les dues proposicions anteriors (podeu usar el símbol '|', que es llegeix 'divideix a'; se suposa que l'univers del discurs està restringit als nombres naturals).

b) Negueu la proposició P2 fins a arribar a la proposició P1, justificant cada pas.

282 Sigui $a \in \mathbb{R}$.

a) Proveu: $a^3 - 3a^2 + 8a - 17 = 0 \Rightarrow a \neq 0$.

b) Escriviu la implicació recíproca de l'anterior, digueu si és certa o falsa i demostreu-ho.

1.49 Examen de recuperació del segon parcial 12/01/2016

283 Considerem, en el conjunt dels nombres enters $\mathbb{Z}$, la relació R definida per:

$$x \; R \; y \Leftrightarrow x^2 - x = y^2 - y.$$

Demostreu que R és d'equivalència, calculeu la classe d'un enter a i digueu quin és el conjunt quocient.

284 Demostreu que si $n \geq 2$, llavors:

$$\prod_{i=1}^{n} \frac{2i-1}{2i} > \frac{1}{2n}$$

1.50 Examen final de reavaluació 5/02/2016

285 Considerem l'aplicació $f : \mathbb{Z}_{101} \to \mathbb{Z}_{101}$ definida per:

$$f(\overline{0}) = \overline{0}; \quad \text{i} \quad f(\overline{x}) = \overline{1} + \overline{x}^{\,-1}, \quad \text{si } \overline{x} \neq \overline{0}.$$

1) Proveu que f està ben definida. És a dir, si $\overline{x} \neq \overline{0}$, llavors té sentit calcular $f(\overline{x})$.

2) Calculeu $f[\{\overline{50}, \overline{75}, \overline{100}\}]$.

3) Trobeu *totes* les classes $\overline{n}, \overline{m}$ tals que $\overline{n} \neq \overline{m}$ i $f(\overline{n}) = f(\overline{m})$.

4) Trobeu *totes* les classes que no tenen antiimatge per f.

5) Estudieu si f és injectiva o exhaustiva.

286 Siguin A, B i C conjunts.

1) Demostreu que $A \cap (B \cup C) \subseteq (A \cap B) \cup C$.

2) Demostreu que si $C \subseteq A$, aleshores $A \cap (B \cup C) = (A \cap B) \cup C$.

3) Demostreu que, en general, $A \cap (B \cup C) \neq (A \cap B) \cup C$.

Observació: recordeu que un gràfic no és una demostració.

287 Sigui $a > 1$ un nombre real fix. Proveu que si $n \geq 3$, llavors:

$$(1 + a)^n > 1 + n\, a^2.$$

288 Siguin $b, c \in \mathbb{Z}$ i r, s nombres naturals.

1) Demostreu que si p és un nombre primer tal que $p \mid (b^r \cdot c^s)$ i $\text{mcd}(p, b) = 1$, llavors $p \mid c$.

2) Sigui $a \in \mathbb{Z}$ tal que $a \mid (b^r \cdot c^s)$ i $\text{mcd}(a, b) = 1$. Es pot deduir que $a \mid c$?

Justifiqueu tots els passos.

1.51 Examen parcial 30/04/2016

289 Demostreu les proposicions següents, indicant detalladament en cada cas quin mètode de demostració utilitzeu i tots els passos.

1) Si a, b i c són nombres reals i $c = a + 2b$, aleshores $a \leq c/2$ o $b \leq c/4$.

2) Sigui $x \neq -1$ un nombre real. Demostreu que les propietats següents són equivalents:

   a) x és irracional;
   b) $6x - 1$ és irracional;
   c) $\dfrac{x}{x+1}$ és irracional.

290 Demostreu que si $n \geq 1$, llavors:

$$\sum_{j=1}^{n} \frac{j}{2^j} = 2 - \frac{n+2}{2^n}.$$

291 Sabem que le fórmules proposicionals $E \to F$, $\neg G \to \neg F$, $H \to I$ i $E \vee H$ són certes. Podem deduir que $G \vee I$ és certa?

1.52 Examen parcial 02/05/2016

292 Sigui Ω un conjunt i considerem dos subconjunts $X \subseteq \Omega$ i $Y \subseteq \Omega$.

a) Demostreu amb rigor que si $X \subseteq Y^c$, aleshores $X \cap Y = \emptyset$.

b) És cert el recíproc? Justifiqueu la resposta.

293 Sigui A un conjunt no buit i R i S dues relacions d'equivalència en A. Se sap que la relació T definida per:

$$a\, T\, b \Leftrightarrow a\, R\, b \text{ i } a\, S\, b,$$

per a tot $a, b \in A$, és una relació d'equivalència.

a) Siguin $[a]_R$, $[a]_S$ i $[a]_T$ les classes d'equivalència de l'element $a \in A$ segons R, S, i T, respectivament. Demostreu que $[a]_T = [a]_R \cap [a]_S$.

b) Sigui $A = \{a \in \mathbb{Z} : 1 \leq a \leq 12\}$. Suposem que:

$$A/R = \{\{1,3,7,9\}, \{2,4,5,6,8\}, \{10,11\}, \{12\}\},$$
$$A/S = \{\{1,7,9,10,11,12\}, \{2,3,4,5,6,8\}\}.$$

Escriviu raonadament els elements del conjunt quocient A/T.

294 Considerem les aplicacions:

$$f : \mathbb{R} - \{0\} \to \mathbb{R} - \{1\}, \qquad g : \mathbb{R} - \{1\} \to \mathbb{R} - \{2\}$$

definides per:

$$f(x) = \frac{x+5}{x}, \qquad g(x) = \frac{2x}{x-1}.$$

a) Comproveu que la composició $h = g \circ f$ és l'aplicació $h(x) = \frac{2x+10}{5}$.

b) Demostreu que l'aplicació h és bijectiva.

c) Trobeu l'aplicació inversa h^{-1}.

1.53 Examen final 20/06/2016

295

a) Siguin a, b dos enters positius primers entre ells. Demostreu:

$$\exists k \in \mathbb{Z}\ (a = 2^k) \Longleftrightarrow \exists h \in \mathbb{Z}, \forall n \in \mathbb{Z}\ (n \geq h \to a \,|\, 2^n b).$$

b) És certa l'equivalència anterior en el cas de nombres no primers entre ells? Raoneu la resposta.

296 Volem demostrar la proposició següent.

$$\forall\, a, b \in \mathbb{Z}\,(7 \mid (a^2 + b^2) \Leftrightarrow 7 \mid a \wedge 7 \mid b).$$

a) Demostreu que si $a, b \in \mathbb{Z}$, aleshores: $7 \mid a \wedge 7 \mid b \Rightarrow 7 \mid (a^2 + b^2)$.

b) Calculeu el conjunt $\{\overline{a}^2 \,|\, \overline{a} \in \mathbb{Z}_7\}$.

c) Calculeu el conjunt $\{\overline{a}^2 + \overline{b}^2 \,|\, \overline{a}, \overline{b} \in \mathbb{Z}_7\}$.

d) Deduïu de l'apartat anterior que: $7 \mid (a^2 + b^2) \Rightarrow 7 \mid a \wedge 7 \mid b$.

297 Expresseu de totes les maneres possibles la fracció $\dfrac{1}{34}$ com a diferència de dues fraccions amb denominadors 17 i 4.

1.54 Recuperació del primer parcial 20/06/2016

298 Considerem el predicat sobre els nombres reals, $I(x)$: 'x és un nombre irracional'. Considerem la proposició següent:

Per a tot x i tot y, si $x + y$ és irracional, aleshores x és irracional o y és irracional.

a) Formalitzeu aquesta proposició usant el predicat I i els símbols lògics necessaris.

b) Negueu aquesta formalització obtinguda i escriviu la negació amb paraules.

c) Demostreu la proposició original, indicant quin mètode useu.

299 Demostreu per inducció que si $n \geq 1$, llavors:

$$\frac{n}{3} + \frac{n^2}{2} + \frac{n^3}{6} \in \mathbb{N}.$$

1.55 Recuperació del segon parcial 20/06/2016

300 A l'interval de nombres reals $I = (1, +\infty)$ es defineix la relació: $xSy \iff x+y > 2$.

a) Demostreu que S és una relació d'equivalència.

b) Calculeu les classes d'equivalència i el conjunt quocient I/S.

c) Considerem ara la mateixa relació però definida sobre $\mathbb{R}$. Proveu que S no és d'equivalència.

301 Sigui $A = \{0, 1, 2, 3\}$.

a) Escriviu el conjunt $\mathcal{P}(A)$ de les parts de A.

b) Considerem l'aplicació $f : \mathcal{P}(A) \to \mathcal{P}(A)$ definida per: $f(X) = (X \setminus \{0\}) \cup \{1\}$.

  i) És f injectiva? Justifiqueu la resposta.
  ii) És f exhaustiva? Justifiqueu la resposta.

1.56 Examen final de reavaluació 11/07/2016

302 Considera l'aplicació:

$$f : \mathbb{R} \setminus \{-1, 1\} \to \mathbb{R} \setminus \{0\}, \quad f(x) = \frac{1}{x^2 - 1}.$$

a) Justifica que f està ben definida.

b) Demostra si és injectiva o no.

c) Demostra si és exhaustiva o no.

303 En el conjunt $A = \{-3, -2, -1, 0, 1, 2, 3\}$ considerem la relació R donada per:

$$a\,R\,b \Leftrightarrow a^2 - b^2 = b - a.$$

a) Enuncia formalment quines són les propietats que ha de satisfer una relació d'equivalència i demostra que R les compleix.

b) Calcula les classes d'equivalència.

304 Demostra per inducció que per a tot $n \geq 6$ es satisfà que $2^n > (n+1)^2$.

305

a) Quins nombres tenen invers en $\mathbb{Z}_{12}$?

b) Calcula l'invers de 5 mòdul 12.

c) Resol l'equació $5x \equiv 11 \pmod{12}$.

1.57 Examen parcial 7/11/2016

306 Considerem les dues proposicions següents:

a) Si x, y són nombres reals positius qualssevol, llavors es compleix $x/y + y/x \geq 2$.

b) Si x, y són nombres reals positius qualssevol, llavors es compleix $x/y - y/x \geq 2$.

Es demana:

1) Escriviu en llenguatge de predicats les dues proposicions.

2) Demostreu que la primera proposició és certa.

3) Demostreu que la segona proposició és falsa.

307 Demostreu la fórmula:

$$6 \cdot \sum_{k=0}^{n-1} (k^2 + 1) = 2n^3 - 3n^2 + 7n, \qquad n \geq 1,$$

de dues maneres diferents:

a) per inducció sobre el nombre natural n;

b) directament, tenint en compte la fórmula $\sum_{k=1}^{n} k^2 = n(n+1)(2n+1)/6$.

1.58 Examen parcial 5/12/2016

308

1) Siguin A, B, C subconjunts d'un conjunt X tals que $A \cap B = A \cap C$ i $A^c \cap B = A^c \cap C$. Proveu que $B = C$.

2) Definim a $\mathbb{Z}$ la relació: $a \, R \, b \Leftrightarrow (a+1)^2 = (b+1)^2$.

   a) Proveu que R és una relació d'equivalència.
   b) Donat $a \in \mathbb{Z}$, calculeu $[a]$. Doneu una descripció del conjunt $[a]$ per extensió.
   c) Calculeu el conjunt quocient. Doneu una descripció del conjunt quocient per extensió (podeu usar punts suspensius).

309 Sigui $D = \{x \in \mathbb{R} : x > 1\}$. Definim l'aplicació $g : D \to D$ per:

$$g(x) = \frac{x}{x-1}.$$

1) Comproveu que g està ben definida.
2) Proveu que g és una aplicació bijectiva.
3) Calculeu l'aplicació $g \circ g$.
4) Calculeu l'aplicació inversa g^{-1}.

1.59 Examen final 12/01/2017

310 Siguin a, b i n enters més grans o iguals que 1. Proveu que:

$$a^n \mid b^n \Leftrightarrow a \mid b.$$

311

a) Siguin a, b, c, d enters tals que $a \neq 0$ i $d \neq 0$. Demostreu l'equivalència:

$$ab \equiv ac \pmod{ad} \Leftrightarrow b \equiv c \pmod{d}.$$

b) Demostreu que si $n \geq 1$ és un enter tal que $\mathrm{mcd}(n, 7) = 1$, aleshores $5 \cdot 8^n \equiv 5 \cdot n^{48} \pmod{35}$.

312

a) Proveu que si x és un enter positiu més petit que 10^4 del que sabem els residus de les divisions per 13, 25 i 37, llavors x és únic.

b) Trobeu l'únic enter positiu x més petit que 10^4 que dóna residus 2, 4 i 5 al dividir per 13, 25 i 37, respectivament.

1.60 Recuperació del primer parcial 12/01/2017

313 Siguin a, b nombres reals. Demostreu que o bé $a \geq \frac{a+b}{2}$ o bé $b \geq \frac{a+b}{2}$. Indiqueu clarament quin mètode de demostració utilitzeu.

314 Proveu per inducció que si $n \geq 1$, llavors:

$$\sum_{i=1}^{n} (2i)^2 = \frac{2n(n+1)(2n+1)}{3}.$$

1.61 Recuperació del segon parcial 12/01/2017

315 Siguin A, B, i C conjunts no buits i $f : A \to B$ una aplicació. Construïm l'aplicació següent:

$$g : A \times C \to B \times C, \quad g(x, y) = (f(x), y),$$

per a qualssevol $x \in A$ i $y \in C$.

a) Demostreu que si f és injectiva, també ho és g.

b) Demostreu que si f és exhaustiva, també ho és g.

316 Siguin $n, p \in \mathbb{N}$ i $A = \{1, \dots, n\}$. Definim la relació R a A, de forma que:

$$a\, R\, b \Leftrightarrow \mathrm{mcd}(a, p) = \mathrm{mcd}(b, p).$$

a) Demostreu R que és una relació d'equivalència.

b) Domeu les classes d'equivalència per a $n = 18$ i $p = 5$.

c) Doneu el conjunt quocient A/R, per a $n, p \geq 1$ qualssevol.

1.62 Examen final de reavaluació 6/02/2017

317 Sigui $n \geq 2$ un nombre enter i p un nombre primer. Demostreu que $\sqrt[n]{p}$ és irracional.

318 Demostreu per inducció que $7^{2n} - 48n - 1$ és divisible per 2304, per a tot $n \geq 1$. Heu de posar clarament l'esquema de la prova inductiva i indicar (quan toqui) quina és la hipòtesi d'inducció i què és el que voleu demostrar.

319

a) Siguin A i B subconjunts d'un univers Ω ($A, B \subseteq \Omega$). Dieu si el que segueix és vertader o fals i justifiqueu la resposta: $A \subseteq B \Leftrightarrow A \cap B = \emptyset$.

b) Sigui $f : \mathbb{Z} \to \mathbb{Z}$ una aplicació injectiva. Demostreu que l'aplicació $g : \mathbb{Z} \to \mathbb{Z}$ definida per $g(x) = 4 \cdot f(x) + 1$ és injectiva però no és exhaustiva.

320 Resoleu l'equació diofàntica següent i trobeu la solució amb la x positiva mínima: $902x - 434y = 104$.

1.63 Examen parcial 20/04/2017

321 Demostreu per inducció que si $n \geq 2$, llavors:

$$\sum_{i=0}^{n} \frac{1}{2i+1} < \frac{n}{3} + 1.$$

Expliciteu, al pas inductiu, la hipòtesi d'inducció i el que voleu demostrar. Justifiqueu tots el passos.

322 Sigui n un nombre natural arbitrari. Demostra que són equivalents:

a) $n+3$ és senar.

b) $5n^2+2n+1$ és senar.

c) $n-2$ és parell.

Indiqueu quins mètodes de demostració utilitzeu.

1.64 Examen parcial 15/05/2017

323 Considerem el conjunt $A = \{1,2,3\}$. Definim al conjunt $X = A \times \mathcal{P}(A)$ la relació R:

$$(a,B)\, R\, (a',B') \Leftrightarrow a = a' \wedge |B| = |B'|,$$

on $|B|$ denota el cardinal del conjunt B.

a) Proveu que R és una relació d'equivalència al conjunt X.

b) Trobeu totes les classes d'equivalència. Doneu-les per extensió.

c) Trobeu el conjunt quocient.

d) Quantes classes hi ha si el conjunt A té n elements?

324 Siguin $f : \mathbb{N} \to \mathbb{Z}$ i $g : \mathbb{Z} \to \mathbb{N}$ les aplicacions següents:

$$f(n) = \begin{cases} -\frac{n}{2} & \text{si } n \text{ és parell} \\ \frac{(n+1)}{2} & \text{si } n \text{ és senar} \end{cases} \qquad g(n) = \begin{cases} 2n-1 & \text{si } n > 0 \\ -2n & \text{si } n \leq 0 \end{cases}$$

a) Calculeu $f[\{0,1,2,3,4\}]$ i $g^{-1}[\{0,1,2,3,4\}]$.

b) Calculeu les aplicacions $g \circ f$ i $f \circ g$.

c) Proveu que f i g són bijectives.

d) Calculeu les aplicacions inverses f^{-1} i g^{-1}.

1.65 Examen final 09/06/2017

325

a) Sabem que a $\mathbb{Z}_n$ el sistema d'equacions:

$$\begin{aligned}\overline{3}\overline{x}+\overline{4}\overline{y}&=\overline{5}\\ \overline{6}\overline{x}+\overline{7}\overline{y}&=\overline{8}\end{aligned}$$

té la solució $\overline{x}=\overline{7}$, $\overline{y}=\overline{8}$. Calculeu els possibles valors de n.

b) Siguin a, b i c enters tals que $\operatorname{mcd}(a,b)=5$ i $\operatorname{mcd}(a,c)=4$. Proveu que a acaba en 0 i b acaba en 5 (en base 10).

326

a) Calculeu l'enter positiu més petit que és congruent amb 2235^{1468} mòdul 223. Justifiqueu tots els pasos.

b) Li demaneu a un amic que multipliqui el dia que va néixer per 12 i el numero del mes per 31 i que us digui el resultat de la suma d'aquestes quantitats. El resultat és 492. Esbrineu la data del seu aniversari.

327

a) Proveu que a $\mathbb{Z}_{126}$ es compleix $\{\overline{5}^n : n\geq 0\}=\{-\overline{25},-\overline{5},-\overline{1},\overline{1},\overline{5},\overline{25}\}$.

b) Siguin $n,m\geq 0$ enters. Demostreu que $\overline{5}^n+\overline{5}^m=\overline{0}$ a $\mathbb{Z}_{126}$ si i només si $n-m\equiv 3 \pmod 6$.

1.66 Examen de recuperació del primer parcial 09/06/2017

328 Considerem l'univers de discurs dels nombres reals. Considerem la propietat $P(x)$ que diu "per a tot nombre real a, existeix un nombre real b tal que $a^2-b^2=x$".

a) Formalitzeu el predicat $P(x)$.

b) Negueu l'expressió obtinguda a l'apartat anterior i passeu la negació a l'interior.

c) Digueu si les proposicions $P(1)$ i $P(-1)$ són certes o falses i justifiqueu les respostes.

329 Proveu per inducció que si $n\geq 1$, llavors:

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

Expliciteu al pas inductiu la hipòtesi d'inducció i el que hem de demostrar.

1.67 Examen de recuperació del segon parcial 09/06/2017

330 Siguin A, B i C conjunts. Proveu les propietats següents:

a) $A \times (B \setminus C) = (A \times B) \setminus (A \times C)$.

b) $A \subseteq B \Leftrightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$. [$\mathcal{P}(X)$ denota el conjunt de les parts del conjunt X.]

331 Considerem l'aplicació $f : \mathbb{R} \setminus \{1\} \to \mathbb{R} \setminus \{2\}$ definida per:

$$f(x) = \frac{1}{x-1} + 2$$

a) Comproveu que si $x \in \mathbb{R} \setminus \{1\}$, aleshores $f(x) \in \mathbb{R} \setminus \{2\}$.

b) Proveu que f és injectiva.

c) Proveu que f és exhaustiva.

d) Justifiqueu que f té inversa i calculeu-la.

1.68 Examen de reavaluació 10/07/2017

332 Sigui $n \geq 2$ un enter i p un nombre primer. Demostreu que $\sqrt[n]{p}$ és irracional.

333 Sigui $f : A \to B$ una aplicació.

a) Demostreu que la relació $a_1 \equiv a_2 \Leftrightarrow f(a_1) = f(a_2)$ és d'equivalència en A.

b) Demostreu que l'aplicació $\tilde{f} : A/\equiv \to B$ definida per $\tilde{f}([a]) = f(a)$ està ben definida i és injectiva.

334 Demostreu que per a tot $n \geq 2$ és $(n+2)! \geq \frac{4^{n+1}}{7}$.

335

a) Resoleu l'equació diofàntica següent: $2005x + 1015y = 15$.

b) Trobeu la solució (x, y) de l'anterior equació diofàntica amb la $x \geq 0$ mínima.

2

Solucions

2.1 Exàmens de taller 2010–2011 Q1

5 Tenim en compte les equivalències: $(p \leftrightarrow q) \equiv (p \to q) \wedge (q \to p)$, $(p \to q) \equiv ((\neg p) \vee q)$, $(p \wedge q) \equiv (p \wedge (\neg(\neg q))) \equiv \neg(p \to (\neg q))$ i les lleis de de Morgan.

1)

$$\begin{aligned} p \leftrightarrow q &\equiv (p \to q) \wedge (q \to p) \\ &\equiv ((\neg p) \vee q) \wedge ((\neg q) \vee p) \\ &\equiv \neg((\neg((\neg p) \vee q)) \vee (\neg((\neg q) \vee p))) \end{aligned}$$

2)

$$\begin{aligned} p \leftrightarrow q &\equiv (p \to q) \wedge (q \to p) \\ &\equiv ((\neg p) \vee q) \wedge ((\neg q) \vee p) \\ &\equiv (\neg(p \wedge (\neg q))) \wedge (\neg(q \wedge (\neg p))) \end{aligned}$$

3) $p \leftrightarrow q \equiv (p \to q) \wedge (q \to p) \equiv \neg((p \to q) \wedge (\neg(q \to p)))$

7

1) $\exists x\, (P(x) \wedge \forall y(P(y) \to y = x))$

2) $\exists x, y\, ((P(x) \wedge P(y) \wedge x \neq y) \wedge \forall z(P(z) \to z = x \vee z = x))$

8

$\Rightarrow$) En primer lloc, observem que: $A - (B \cap C) = (A - B) \cup (A - C)$.

Si $x \in A \cap B$, llavors $x \in A$ i $x \in B$. Volem provar que $x \in A$ i $x \in C$.

Que $x \in A$ ja ho sabem, per hipòtesi.

Suposem que $x \notin C$. Llavors tenim d'una banda que $x \in A$ i d'altra $x \notin C$. Per tant, $x \in A - C \subseteq (A - B) \cup (A - C)$. Ara, per hipòtesi, podem afirmar que $x \in A - B$. És a dir, $x \in A$ i $x \notin B$.

Però ara tenim que $x \in B$ i $x \notin B$: contradicció.

Per tant, $x \in C$.

$\Leftarrow$) Tenim:

$$\begin{aligned} x \in A - (B \cap C) &\Rightarrow x \in A \wedge x \notin B \cap C \\ &\Rightarrow x \in A \wedge \neg(x \in B \wedge x \in C) \\ &\Rightarrow x \in A \wedge (x \notin B \vee x \notin C) && (1) \\ &\Rightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) && (2) \\ &\Rightarrow x \in A - B \vee x \in A - C \end{aligned}$$

(1): llei de de Morgan; (2): distributiva.

Ara si $x \in A - C$ llavors $x \in A$ i $x \notin C$. Per tant, per hipòtesi tenim que $x \in A$ i $x \notin B$. Així doncs, en qualsevol cas obtenim que $x \in A - B$, com volíem demostrar.

9 Es tracta d'una equivalència. Per tant, haurem de demostrar dues implicacions.

$\Leftarrow$) Suposem que $B = \emptyset$. Llavors:

$$(A - B) \cup (B - A) = (A - \emptyset) \cup (\emptyset - A) = A \cup \emptyset = A$$

Efectivament: els elements de $A - \emptyset$ són els elements de A que no pertanyen a $\emptyset$; és a dir, tots els elements de A. A més, $\emptyset - A$ està format pels elements de $\emptyset$ que no pertanyen a A; és a dir, és $\emptyset$.

$\Rightarrow$) Suposem ara que $(A - B) \cup (B - A) = A$. Volem demostrar que $B = \emptyset$. Ho fem per reducció al absurd. Suposem que $B \neq \emptyset$. Llavors existeix un element $x \in B$. Ara distingim dos casos: $x \in A$ i $x \notin A$.

Cas 1: $x \in A$**.** Llavors $x \in A$, però $x \notin B - A$ i $x \notin A - B$; és a dir, $x \notin (A - B) \cup (B - A)$. Contradicció, perquè aquest conjunt és igual a A per hipòtesi.

Cas 2: $x \notin A$**.** Llavors $x \in B - A$ i, per tant, $x \in (A - B) \cup (B - A) = A$. Contradicció perquè estem suposant que $x \notin A$.

Per tant, en qualsevol cas arribem a una contradicció. Conseqüentment, $B = \emptyset$.

10 Es tracta d'una equivalència. Per tant, haurem de demostrar dues implicacions.

$\Leftarrow$) Suposem que $A \cap B = \emptyset$. Llavors:

$$\begin{aligned} A - B &= \{x \in A : x \notin B\} = A \\ B - A &= \{x \in B : x \notin A\} = B \end{aligned}$$

Per tant, $(A - B) \cup (B - A) = A \cup B$.

$\Rightarrow$) Suposem ara que $(A-B)\cup(B-A)=A\cup B$. Volem demostrar que $A\cap B=\emptyset$. Ho fem per reducció al absurd. Suposem que $A\cap B\neq\emptyset$. Llavors existeix un element $x\in A\cap B$, és a dir $x\in A$ i $x\in B$. Però aquest element x satisfà: $x\notin A-B$, perquè $x\in B$, i $x\notin B-A$, perquè $x\in A$. Per tant, $x\notin(A-B)\cup(B-A)$ i $x\in A\cup B$. Contradicció, perquè estem suposant que aquests dos conjunts són iguals.

11 En primer lloc observem que la condició $C^c\cap B=\emptyset$ és equivalent a dir que $B\subseteq C$. Efectivament: si $C^c\cap B=\emptyset$ i $x\in B$, llavors $x\notin C^c$ i per tant $x\in C$. Recíprocament, si $B\subseteq C$ i $x\in C^c\cap B$, llavors $x\in B$ i $x\notin C$; és a dir, $x\in C$ i $x\notin C$. Absurd. Per tant, $C^c\cap B=\emptyset$.

Sigui $x\in A$. Distingim dos casos:

Cas 1: $x\in B$**.** Llavors $x\in C$, per l'anterior observació.

Cas 2: $x\notin B$**.** Llavors $x\in A\cap B^c$ i, per hipòtesi, aquest conjunt és un subconjunt de C. Per tant, $x\in C$.

12 En primer lloc observem que la condició $C^c\cap B=\emptyset$ és equivalent a dir que $B\subseteq C$. Efectivament: si $C^c\cap B=\emptyset$ i $x\in B$, llavors $x\notin C^c$ i per tant $x\in C$. Recíprocament, si $B\subseteq C$ i $x\in C^c\cap B$, llavors $x\in B$ i $x\notin C$; és a dir, $x\in C$ i $x\notin C$. Absurd. Per tant, $C^c\cap B=\emptyset$.

En segon lloc, què és $A-(A-B)$?

$$\begin{aligned}x\in A-(A-B)&\Leftrightarrow x\in A\wedge x\notin(A-B)\\&\Leftrightarrow x\in A\wedge(x\notin A\vee x\in B)\\&\Leftrightarrow(x\in A\wedge x\notin A)\vee(x\in A\wedge x\in B)\\&\Leftrightarrow x\in A\cap B\end{aligned}$$

És a dir: $A-(A-B)=A\cap B$.

Per tant, hem de demostrar que $A\cap B\subseteq A\cap C$. Sigui $x\in A\cap B$. Llavors $x\in A$ i $x\in B$. Per hipòtesi, si $x\in B$, llavors $x\in C$. Per tant, $x\in A$ i $x\in C$. És a dir, $x\in A\cap C$.

13 Sigui $x\in D\cap C$. Llavors $x\in D$ i $x\in C$. Volem demostrar que $x\in A^c$. Ho fem per reducció a l'absurd. Suposem doncs que $x\notin A^c$. Llavors $x\in A$. És a dir: $x\in D$ i $x\in A$. Per hipòtesi, $x\in D\cap B$. Però ara tenim que $x\in A\cap B\cap C$, que és el conjunt buit, per hipòtesi. Contradicció.

Per tant, $x\in A^c$.

14 Donem dues demostracions.

Solució 1: Sigui $x\in B$ qualsevol. Llavors $x\in A\cup B$, i, per la primera hipòtesi, $x\in A\cup C$. Ara tenim dos casos.

Cas 1) $x\in A$. Llavors $x\in A\cap B$ i per la segona hipòtesi $x\in A\cap C$ i per tant $x\in C$.

Cas 2) $x \notin A$. Com teníem $x \in A \cup C$, necessàriament llavors $x \in C$.

En ambdós casos resulta $x \in C$, i per tant queda provat que $B \subseteq C$.

Solució 2: Sigui $x \in B$ un element qualsevol. Per la definició d'unió tindrem $x \in A \cup B$. Per la primera part de la hipòtesi resulta llavors que $x \in A \cup C$ i a més recordem que $x \in B$.

Per tant $x \in (A \cup C) \cap B$, que per la propietat distributiva assegura que $x \in (A \cap B) \cup (C \cap B)$. Emprant la segona part de la hipòtesi resulta ara que $x \in (A \cap C) \cup (B \cap C)$. Tornant a aplicar la propietat distributiva resulta $x \in (A \cup B) \cap C$. I per tant, en particular resulta que $x \in C$. Per tant queda provat que $B \subseteq C$.

15 Ho fem per reducció a l'absurd. Suposem que $A \cap C = \emptyset$. Per hipòtesi, $A \cap B \neq \emptyset$; per tant, existeix un element $x \in A \cap B$. Aquest element x no pot ser un element de C, perquè estem suposant que $A \cap C = \emptyset$. Per tant, $x \in C^c$. Però ara tenim que $x \in B$ i $x \in C^c$, i, per hipòtesi, sabem que $B \cap C^c = \emptyset$. Contradicció. Per tant, $A \cap C \neq \emptyset$.

16 Es tracta de demostrar una equivalència. Per tant, hem de provar dues implicacions.

$\Rightarrow$) La hipòtesis ens diu que tot element de C ho és de A i de B. Si $C \cap A^c \neq \emptyset$, aleshores existeix $x \in C \cap A^c$, i llavors $x \in C$ i $x \notin A$. Però si $x \in C$, llavors, per hipòtesi, $x \in A$. Ara tenim que $x \in A$ i $x \notin A$: Contradicció. Per tant, $C \cap A^c = \emptyset$. Anàlogament es demostra que $C \cap B^c = \emptyset$.

$\Leftarrow$) Hem de provar una inclusió: $C \subseteq A \cap B$. Sigui $x \in C$. Volem veure que $x \in A$ i que $x \in B$. Suposem que $x \notin A$. Llavors tenim que $x \in C \cap A^c$, que per hipòtesi és el conjunt buit. Contradicció. Per tant, $x \in A$. Anàlogament demostrem que $x \in B$.

17

1) a) Si n és parell, llavors $f(n) = n$ i $f(f(n)) = f(n) = n$,
   b) Si n és senar, llavors $f(n) = n + 1$ i $f(f(n)) = f(n + 1)$; com ara $n + 1$ és parell, $f(f(n)) = f(n + 1) = n + 1$.

   En tots els casos $f \circ f = f$.

2) $f[\{1, 2, 3, 4\}] = \{2, 4\}$. f no és injectiva ja que $f(2k) = f(2k - 1)$.

3) $f^{-1}[\{0, 1, 2\}] = \{0, 1, 2\}$. f no és exhaustiva ja que el nombres senars no tenen antiimatge.

18

1) a) Si n és múltiple de 3, llavors $f(n) = n$ i $f(f(n)) = f(n) = n$,
   b) Si n no és múltiple de 3, llavors $f(n) = 3n$ i $f(f(n)) = f(3n)$; com ara $3n$ és múltiple de 3, $f(f(n)) = f(3n) = 3n$.

   En tots els casos $f \circ f = f$.

2) $f[\{1,2,3,4\}] = \{3,6,12\}$. f no és injectiva ja que si n no és múltiple de $f(3n) = f(n)$.

3) $f^{-1}[\{0,1,2\}] = \{0\}$. f no és exhaustiva ja que el nombres que no són múltiple de 3 no tenen antiimatge.

19

1) $f[\{-2,-1,0,1,2\}] = \{-4,-1,0,1,4\}$.

2) Hem de veure que si $f(n_1) = f(n_2)$, llavors $n_1 = n_2$.

$$f(n_1) = f(n_2) \Rightarrow n_1^2 = n_2^2 \vee n_1^2 = -n_2^2 \Rightarrow n_1^2 - n_2^2 = 0 \vee n_1^2 + n_2^2 = 0$$

   a) si $n_1^2 + n_2^2 = 0$, llavors $n_1 = n_2 = 0$,
   b) si $n_1^2 - n_2^2 = 0$, llavors $(n_1 - n_2)(n_1 + n_2) = 0$ i $n_1 - n_2 = 0$, ja que o $n_1, n_2 < 0$ o $n_1, n_2 \geq 0$.

   En tots els casos $n_1 = n_2$.

3) $f^{-1}[\{0,1,2\}] = \{0,1\}$. f no és exhaustiva ja que el nombres que no són quadrats perfectes no tenen antiimatge.

20

1) $f[\{-2,-1,0,1,2\}] = \{4,2,0,1,3\}$. $f[\{-5,-3,0,3,5\}] = \{10,6,0,5,9\}$.

2) $f^{-1}[\{0,1,2\}] = \{-1,0,1\}$. $f^{-1}[\{0,3,6\}] = \{-3,0,2\}$.

3) Hem de veure que si $f(n_1) = f(n_2)$, llavors $n_1 = n_2$. Notem que si $f(n_1) = f(n_2)$, llavors $n_1, n_2 > 0$ o $n_1, n_2 \leq 0$, ja que si $n_1 > 0$ i $n_2 \leq 0$, llavors tindríem que un nombre és parell i senar a la vegada.

   a) si $n_1, n_2 > 0$, llavors $2n_1 - 1 = 2n_2 - 1$, i $n_1 = n_2$,
   b) si $n_1, n_2 \leq 0$, llavors $-2n_1 = -2n_2$, i $n_1 = n_2$.

   En tots els casos $n_1 = n_2$.

4) Hem de veure que per a tot $m \in \mathbb{N}$ existeix $n \in \mathbb{Z}$ tal que $f(n) = m$:

   a) si m és parell, $m = 2k$ amb $k \geq 0$, llavors $f(-k) = m$,
   b) si m és senar, $m = 2k - 1$ amb $k \geq 1$, llavors $f(k) = m$.

21

1) $f[\{0,1,2,3,4,5\}] = \{0,1,-1,2,-2,3\}$.
   $f[\{0,3,5,6,7,10\}] = \{0,2,3,-3,4,-5\}$.

2) $f^{-1}[\{-1,0,1,2\}] = \{-2,0,1,3\}$. $f^{-1}[\{-3,-1,0,1\}] = \{0,1,2,6\}$.

3) Hem de veure que per a tot $m \in \mathbb{Z}$ existeix $n \in \mathbb{N}$ tal que $f(n) = m$:

   a) si $m \geq 0$, llavors $f(2m-1) = m$,
   b) si $m < 0$, llavors $f(-2m) = m$.

4) Hem de veure que si $f(n_1) = f(n_2)$, llavors $n_1 = n_2$. Notem que si $f(n_1) = f(n_2)$, llavors n_1 i n_2 són tots parells o tots dos són senars, ja que si un fos parell i l'altre fos senar llavors tindríem un nombre que és a la vegada més gran o igual que 0 i més petit que 0.

   a) Si n_1 i n_2 són parells, llavors $-\frac{n_1}{2} = -\frac{n_2}{2}$, i $n_1 = n_2$,
   b) si n_1 i n_2 són senars, llavors $\frac{n_1+1}{2} = \frac{n_2+1}{2}$, i $n_1 = n_2$.

   En tots els casos $n_1 = n_2$.

22

1) $f^{-1}[\{0,1,2,3,4,5\}] = \{-1,0,1,2,3,4,5,10,15,20,25\}$.

2) Hem de veure que per a tot $m \in \mathbb{N}$ existeix $n \in \mathbb{N}$ tal que $f(n) = m$: si $m \in \mathbb{N}$, llavors $f(5m) = m$.

3) $f[\{0,1,2,5,10,15\}] = \{0,1,2,3\}$. No és injectiva ja que si n no és múltiple de 5 llavors $f(5(n+1)) = f(n)$.

23

1) Hem de veure que $f^{-1}[S] \subseteq P$ i $P \subseteq f^{-1}[S]$:

   a) $f^{-1}[S] \subseteq P$: si $k \in f^{-1}[S]$, llavors existeix $l \in S$ tal que $l = k^2 + 1$. Donat que l és senar, k^2 és parell i, per tant, k és parell; és a dir, $k \in P$.
   b) $P \subseteq f^{-1}[S]$: si $k \in P$, llavors $f(k) = k^2 + 1$ és senar, ja que k és parell. En conseqüència, $f(k) \in S$ i $k \in f^{-1}[S]$.

2) Per exemple, 3 no té antiimatge perquè no hi ha cap natural amb quadrat igual a 2.

3) No és injectiva perquè $f(n) = f(-n)$

4) No, perquè no és exhaustiva ni injectiva.

24

1) $f^{-1}[\{-1,0,1,2\}] = \{-3,-1,0,2\}$. No es exhaustiva perquè 2 no té antiimatge.

2) Hem de veure que si $f(n_1) = f(n_2)$, llavors $n_1 = n_2$. Notem que si $f(n_1) = f(n_2)$, llavors n_1 i n_2 són tots parells o tots dos són senars, ja que si un fos parell i l'altre fos senar llavors tindríem un nombre que és a la vegada parell i senar.

a) Si n_1 i n_2 són parells, llavors $7n_1 = 7n_2$, i $n_1 = n_2$,

b) si n_1 i n_2 són senars, llavors $n_1 + 2 = n_2 + 2$, i $n_1 = n_2$.

3) No, perquè no és exhaustiva.

25

1) $f[\{-2,-1,0,1,2\}] = \{1,3,7\}$. No és injectiva ja que $f(-2) = f(1)$.

2) $f^{-1}[\{0,1\}] = \{-1,0\}$. No es exhaustiva perquè 1 no té antiimatge.

3) No, perquè no és ni exhaustiva ni injectiva.

26

1) Només cal notar que $f(p) = p$ per tot $p \in P$.

2) $f[\{2,6,9,11,35\}] = \{2,3,5,11\}$. No és injectiva ja que $f(2) = f(6)$.

3) Hem de veure que per a tot $m \in P$ existeix $n \in A$ tal que $f(n) = m$: Només cal notar que $f(p) = p$ per tot $p \in P$; una antiimatge de $p \in P$ és el mateix p.

4) No, perquè no és injectiva.

27

1) a) Si n és múltiple de 5, llavors $f(n) = n$ i $f(f(n)) = f(n) = n$,

b) si n no és múltiple de 5, llavors $f(n) = 5n$ i $f(f(n)) = f(5n)$; com ara $5n$ és múltiple de 5, $f(f(n)) = f(5n) = 5n$.

En tots els casos $f \circ f = f$.

2) $f[\{0,1,2,3,4,5\}] = \{0,5,10,15,20\}$. No és injectiva ja que si n no és múltiple de 5, $f(n) = f(5n)$.

3) $f^{-1}[\{0\}] = \{0\}$, $f^{-1}[\{1\}] = \emptyset$, $f^{-1}[\{5\}] = \{1,5\}$, $f^{-1}[\{0,1,5\}] = \{0,1,5\}$. No és exhaustiva ja que el enters que no són múltiple de 5 no tenen antiimatge.

4) No, perquè no és injectiva ni exhaustiva.

28

1) $f[\{1,2,3,4,5,6\}] = \{2,1,3,5,4,6\} = A$.

2) Per inspecció, tenim que:

a) si $a_1 \neq a_2$, llavors $g(a_1) \neq g(a_2)$; és a dir, g és injectiva;

b) $g[A] = A$; és a dir, g és exhaustiva.

Conseqüentment g es bijectiva.

3) Hem de veure que si $f(n_1) = f(n_2)$, llavors $n_1 = n_2$. Notem que:

a) si n és múltiple de 3, $f(n)$ és múltiple de 3,

b) si el residu de dividir n per 3 és 1, el de $f(n)$ és 2,

c) si el residu de dividir n per 3 és 2, el de $f(n)$ és 1.

Si $f(n_1) = f(n_2)$, llavors:

a) o n_1 i n_2 són tots dos múltiple de 3,

b) o n_1 i n_2 són tots dos múltiple de 3 més 1,

c) o n_1 i n_2 són tots dos múltiple de 3 més 2.

En qualsevol cas, la condició $f(n_1) = f(n_2)$ és pot escriure:

$$n_1 + \delta = n_2 + \delta, \qquad \delta \in \{-1, 0, 1\},$$

i, per tant, $n_1 = n_2$.

4)

$$\begin{aligned} f[\{0,1,2,4,5,9\}] &= \{f(0), f(1), f(2), f(4), f(5), f(9)\} \\ &= \{0,2,1,5,4,9\} = B \end{aligned}$$

5) Per inspecció, tenim que:

a) si $b_1 \neq b_2$, llavors $h(b_1) \neq h(b_2)$; és a dir, h és injectiva,

b) $h[B] = B$; és a dir, h és exhaustiva.

Conseqüentment h es bijectiva.

6) Hem de veure que per a tot $m \in \mathbb{N}$ existeix $n \in \mathbb{N}$ tal que $f(n) = m$: notem que qualsevol $m \in \mathbb{N}$ és pot escriure com $m = 3k$ o $m = 3k+1$ o $m = 3k+2$, per a cert $k \in \mathbb{N}$; llavors:

a) si $m = 3k$, $f(m) = m$,

b) si $m = 3k+1$, $f(m+1) = m$,

c) si $m = 3k+2$, $f(m-1) = m$.

En tots el casos hem trobat una antiimatge de m.

29

1) $g[\{2,3,5,7,11\}] = \{4,9,25,49,121\}$; $f^{-1}[\{2\}] = \{2k : k \in \mathbb{N}\}$.

2) Si $p \in P$, $f(g(p)) = f(p^2)$. El primer més petit que divideix p^2 és p; llavors $f(g(p)) = f(p^2) = p$.

3) Hem de veure que per a tot $m \in P$ existeix $n \in A$ tal que $f(n) = m$: només cal notar que $f(p) = p$, per tot $p \in P$; una antiimatge de $p \in P$ és el mateix p.

30

1) $f[\{0,1,2,4,8\}] = \{0,1,2,4\}$. No es injectiva ja que $f(2k+1) = f(4(2k+1))$, $k \in \mathbb{Z}$.

2) Hem de veure que per a to $m \in \mathbb{Z}$ existeix $n \in \mathbb{Z}$ tal que $f(n) = m$: una antiimatge de $m \in \mathbb{Z}$ és $n = 2m$ ja que $f(2m) = m$.

3) No, perquè no és injectiva.

31

Cas inicial: $n = 1$.

$$\sum_{i=1}^{1} i \cdot i! = 1 \cdot 1! = 1 = (1+1)! - 1 = 2 - 1$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n} i \cdot i! = (n+1)! - 1$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1} i \cdot i! = (n+2)! - 1$$

Ara tenim:

$$\begin{aligned}
\sum_{i=1}^{n+1} i \cdot i! &= \sum_{i=1}^{n} i \cdot i! + (n+1)(n+1)! \\
&= (n+1)! - 1 + (n+1)(n+1)! \qquad \text{per H.I.} \\
&= (n+1)!(1+n+1) - 1 \\
&= (n+1)!(n+2) - 1 = (n+2)! - 1
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

32

Cas inicial: $n = 1$.

$$\sum_{k=1}^{1} (-1)^{k-1} k^2 = 1 = (-1)^0 \frac{1(1+1)}{2}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{k=1}^{n}(-1)^{k-1} \cdot k^2 = (-1)^{n-1}\frac{n(n+1)}{2}$ (hipòtesi d'inducció). Volem demostrar:

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

Ara tenim:

$$\begin{aligned}\sum_{k=1}^{n+1}(-1)^{k-1}k^2 &= \sum_{k=1}^{n}(-1)^{k-1}k^2 + (-1)^n(n+1)^2 \\ &= (-1)^{n-1}\frac{n(n+1)}{2} + (-1)^n(n+1)^2 \qquad \text{per H.I.} \\ &= (-1)^{n-1}(n+1)\left(\frac{n}{2} - (n+1)\right) \\ &= (-1)^n\frac{(n+1)(n+2)}{2}\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

33

Cas inicial: $n = 1$.

$$\sum_{j=1}^{1} j(j+1) = 1 \cdot (1+1) = 2 = \frac{1 \cdot (1+1) \cdot (1+2)}{3}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{j=1}^{n} j(j+1) = \frac{n(n+1)(n+2)}{3}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{j=1}^{n+1} j(j+1) = \frac{(n+1)(n+2)(n+3)}{3}$$

Ara tenim:

$$\begin{aligned}\sum_{j=1}^{n+1} j(j+1) &= \sum_{j=1}^{n} j(j+1) + (n+1)(n+2) \\ &= \frac{n(n+1)(n+2)}{3} + (n+1)(n+2) \qquad \text{per H.I.} \\ &= (n+1)(n+2)\left(\frac{n}{3} + 1\right) \\ &= \frac{(n+1)(n+2)(n+3)}{3}\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

34

Cas inicial: $n = 1$.

$$\sum_{\ell=1}^{1} \frac{1}{\ell(\ell+1)} = \frac{1}{1+1} = \frac{1}{2}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{\ell=1}^{n} \frac{1}{\ell(\ell+1)} = \frac{n}{n+1}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{\ell=1}^{n+1} \frac{1}{\ell(\ell+1)} = \frac{n+1}{n+2}$$

Ara tenim:

$$\begin{aligned}
\sum_{\ell=1}^{n+1} \frac{1}{\ell(\ell+1)} &= \sum_{\ell=1}^{n} \frac{1}{\ell(\ell+1)} + \frac{1}{(n+1)(n+2)} \\
&= \frac{n}{(n+1)} + \frac{1}{(n+1)(n+2)} \qquad \text{per H.I.} \\
&= \frac{n^2+2n+1}{(n+1)(n+2)} \\
&= \frac{(n+1)^2}{(n+1)(n+2)} \\
&= \frac{n+1}{n+2}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

35

Cas inicial: $n = 1$.

$$\sum_{r=1}^{1} (3r-2) = 3-2 = 1 = \frac{3-1}{2}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{r=1}^{n}(3r-2) = \frac{3n^2-n}{2}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{r=1}^{n+1} (3r-2) = \frac{3(n+1)^2-(n+1)}{2}$$

Ara tenim:

$$\begin{aligned}
\sum_{r=1}^{n+1} (3r-2) &= \sum_{r=1}^{n} (3r-2) + (3(n+1)-2) \\
&= \frac{3n^2-n}{2} + 3n+1 \qquad \text{per H.I.} \\
&= \frac{3n^2+5n+1}{2)} \\
&= \frac{3(n+1)^2-(n+1)}{2}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

36

Cas inicial: $n = 1$.

$$\sum_{s=1}^{1}(4s+1) = 4+1 = 5 = 1 \cdot (2+3)$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{s=1}^{n}(4s+1) = n(2n+3)$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{s=1}^{n+1}(4s+1) = (n+1)(2(n+1)+3)$$

Ara tenim:

$$\begin{aligned}\sum_{s=1}^{n+1}(4s+1) &= \sum_{s=1}^{n}(4s+1) + 4(n+1)+1 \\ &= n(2n+3)+4n+5 \qquad \text{per H.I.} \\ &= 2n^2+7n+5\end{aligned}$$

D'altra banda: $(n+1)(2(n+1)+3) = (n+1)(2n+5) = 2n^2+7n+5$.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

37

Cas inicial: $n = 1$.

$$\sum_{v=1}^{1}(v^2+v) = 1^2+1 = 2 = \frac{1 \cdot (1+1)(1+2)}{3}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{v=1}^{n}(v^2+v) = \frac{n(n+1)(n+2)}{3}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{v=1}^{n+1}(v^2+v) = \frac{(n+1)(n+2)(n+3)}{3}$$

Ara tenim:

$$\begin{aligned}\sum_{v=1}^{n+1}(v^2+v) &= \sum_{v=1}^{n}(v^2+v) + (n+1)^2 + (n+1) \\ &= \frac{n(n+1)(n+2)}{3} + (n+1)^2 + (n+1) \qquad \text{per H.I.} \\ &= \frac{n(n+1)(n+2)}{3} + \frac{3(n+1)^2+3(n+1)}{3} \\ &= \frac{(n+1)[n(n+2)+3(n+1)+3]}{3} \\ &= \frac{(n+1)(n^2+5n+6)}{3} = \frac{(n+1)(n+2)(n+3)}{3}\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

38

Cas inicial: $n = 1$**.**

$$\sum_{m=1}^{1}(5m-3) = 5-3 = 2 = \frac{5-1}{2}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{m=1}^{n}(5m-3) = \frac{5n^2-n}{2}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{m=1}^{n+1}(5m-3) = \frac{5(n+1)^2-(n+1)}{2}$$

Ara tenim:

$$\begin{aligned}\sum_{m=1}^{n+1}(5m-3) &= \sum_{m=1}^{n}(5m-3) + 5(n+1) - 3 \\ &= \frac{5n^2-n}{2} + 5n + 2 \qquad \text{per H.I.} \\ &= \frac{5n^2-n+2(5n+2)}{2} \\ &= \frac{5n^2+9n+4}{2}\end{aligned}$$

D'altra banda: $\frac{5(n+1)^2-(n+1)}{2} = \frac{5n^2+10n+5-n-1}{2} = \frac{5n^2+9n+4}{2}$.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

39

Cas inicial: $n = 1$**.**

$$\sum_{u=1}^{1}(u^2-u) = 1^2-1 = 0 = \frac{1\cdot(1-1)}{3}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{u=1}^{n}(u^2-u) = \frac{n(n^2-1)}{3}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{u=1}^{n+1}(u^2-u) = \frac{(n+1)((n+1)^2-1)}{3}$$

Ara tenim:

$$
\begin{aligned}
\sum_{u=1}^{n+1}(u^2-u) &= \sum_{u=1}^{n}(u^2-u)+(n+1)^2-(n+1) \\
&= \frac{n(n^2-1)}{3}+(n+1)^2-(n+1) \qquad \text{per H.I.} \\
&= \frac{n(n^2-1)}{3}+\frac{3(n+1)^2-3(n+1)}{3} \qquad (*) \\
&= \frac{(n+1)[n(n-1)+3(n+1)-3]}{3} \\
&= \frac{(n+1)(n^2+2n)}{3} \\
&= \frac{(n+1)((n+1)^2-1)}{3}
\end{aligned}
$$

(*) Hem utilitzat que: $n^2-1=(n+1)(n-1)$.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n\geq 1$.

40

Cas inicial: $n=1$**.**

$$\sum_{t=1}^{1} t^3 = 1 = \frac{1(1+1)^2}{4}$$

Pas d'inducció: Fixem un enter $n\geq 1$ i suposem que $\sum_{t=1}^{n} t^3 = \frac{n^2(n+1)^2}{4}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{t=1}^{n+1} t^3 = \frac{(n+1)^2(n+2)^2}{4}$$

Ara tenim:

$$
\begin{aligned}
\sum_{t=1}^{n+1} t^3 &= \sum_{t=1}^{n} t^3+(n+1)^3 \\
&= \frac{n^2(n+1)^2}{4}+\frac{4(n+1)^3}{4} \qquad \text{per H.I.} \\
&= \frac{(n+1)^2(n^2+4n+4)}{4} \\
&= \frac{(n+1)^2(n+2)^2}{4}
\end{aligned}
$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n\geq 1$.

41

Cas inicial: $n = 1$.

$$\sum_{p=1}^{1} \frac{1}{(p+1)(p+2)} = \frac{1}{(1+1)(1+2)} = \frac{1}{6} = \frac{1}{2(1+2)}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{p=1}^{n} \frac{1}{(p+1)(p+2)} = \frac{n}{2(n+2)}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{p=1}^{n+1} \frac{1}{(p+1)(p+2)} = \frac{n+1}{2(n+3)}$$

Ara tenim:

$$\begin{aligned}
\sum_{p=1}^{n+1} \frac{1}{(p+1)(p+2)} &= \sum_{p=1}^{n} \frac{1}{(p+1)(p+2)} + \frac{1}{(n+2)(n+3)} \\
&= \frac{n}{2(n+2)} + \frac{1}{(n+2)(n+3)} \qquad \text{per H.I.} \\
&= \frac{n(n+3)+2}{2(n+2)(n+3)} \\
&= \frac{n^2+3n+2}{2(n+2)(n+3)} \\
&= \frac{(n+2)(n+3)}{2(n+2)(n+3)} = \frac{n+1}{2(n+3)}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

42 Si $d = \text{mcd}(a, b)$, llavors $d \mid a$ i, per tant, $d \mid 2a$. Conseqüentment, $\text{mcd}(2a, d) = d$.

43 Si d és un divisor positiu comú de $2a$ i b, llavors d ha de ser un divisor comú de 2 i b, perque a i b són primers entre si. Però b és senar, per tant $d = 1$. És a dir, $\text{mcd}(2a, b) = 1$.

44 Si $p \nmid b$ i $q \nmid a$, llavors $\text{mcd}(pa, qb) = 1$, ja que a i b són primers entre si. Suposem doncs que aquest mcd no és 1 i sigui ℓ un primer tal que $\ell \mid pa$ i $\ell \mid qb$. Llavors tenim els casos:

- $\ell = p$ i $\ell \mid b$: llavors $p \mid \text{mcd}(pa, qb)$;
- $\ell = q$ i $\ell \mid a$: llavors $q \mid \text{mcd}(pa, qb)$.

És a dir, els únics primers que poden dividir a $\text{mcd}(pa, qb)$ són p o q. Per tant: el mcd és p, q o pq.

45 Si a és parell, llavors existeix un enter a' tal que $a = 2a'$. És a dir 2 és un divisor comú de a i $2p$. Llavors: si $p \mid a'$, el mcd és $2p$; si $p \nmid a'$, el mcd és 2.

46 Sabem que $\ell \mid a = pN$. Per tant $\ell \mid p$, i d'aqui $\ell = p$ o $\ell \mid N$. Però $\ell \mid p$ implica que $\ell = p$, que no pot ser. Per tant $\ell \mid N$. De la mateixa manera, de $\ell \mid a = qM$ deduïm que $\ell \mid M$. Per tant, $\ell \mid \mathrm{mcd}(N, M)$ d'on $\mathrm{mcd}(N, M) \neq 1$.

47 Si $a \mid b$, existeix $r \in \mathbb{Z}$ tal que $b = ar$. Si $c \mid d$, llavors existeix $s \in \mathbb{Z}$ tal que $d = cs$. Per tant: $bd = ar \cdot cs = ac \cdot rs$. És a dir, $ac \mid bd$.

48 Ho demostrem per reducció a l'absurd. Suposem que $\mathrm{mcd}(a, b) \neq 1$. Llavors existeix un nombre enter $d \neq 1$ tal que $d \mid a$ i $d \mid b$. Per la linealitat de la relació de divisibilitat: $d \mid ac + bd = 1$. Contradicció.

49 Apliquem el teorema d'Euclides:

$$\mathrm{mcd}(a, a + b) = \mathrm{mcd}(a, a + b - a) = \mathrm{mcd}(a, b) = \mathrm{mcd}(a, a - b).$$

Per tant, si $\mathrm{mcd}(a, a + b) = 1$, llavors $\mathrm{mcd}(a, a - b) = 1$.

50 Pel teorema d'Euclides: $\mathrm{mcd}(a, a + b) = \mathrm{mcd}(a, b)$. Per tant, només hem de demostrar que $\mathrm{mcd}(a, b)$ és un divisor de $\mathrm{mcm}(a, b)$. Però:

$$\mathrm{mcd}(a, b) = |ab| \cdot \mathrm{mcd}(a, b).$$

51 Si $p \mid ab$, llavors $p \mid a$ o $p \mid b$, pel lema de Gauss. Anàlogament, $p \mid a$ o $p \mid c$. Tenim quatre casos:

- $p \mid a$;
- $p \mid a$ i $p \mid c$;
- $p \mid b$ i $p \mid a$;
- $p \mid b$ i $p \mid c$: no pot ser perque $\mathrm{mcd}(b, c) = 1$.

En qualsevol cas, veiem que $p \mid a$.

52 Tenim que $r \mid a$ i $r \mid b$. Atès que $a \mid c$ i $b \mid d$, deduïm que $r \mid c$ i $r \mid d$. Per definició de mcd: $r \mid \mathrm{mcd}(c, d) = s$.

2.2 Examen parcial 22/11/2010

54

1) Aquesta proposició diu que si el producte de dos enters és parell, llavors ambdós enters són parells. Clarament això és fals, com mostra el següent contraexemple: $a = 1$, $b = 2$, $c = 1 \cdot 2$.

2) Hem de provar que donat qualsevol $x \in A$, existeix un element $(a, b) \in A \times B$ tal que $g(a, b) = x$. Però $g(a, b) = a$, per tant, podem prendre l'element (x, b), on $b \in B$ és arbitrari. Fixem-nos que aquest b existeix perquè B és un conjunt no buit.

55

1) Hem de provar que és reflexiva, simètrica i transitiva.

   Reflexiva: $ab = ba$. Per tant: $(a, b)\ R\ (a, b)$.
   Simètrica: $(a, b)\ R\ (c, d) \Rightarrow a \cdot d = b \cdot c \Rightarrow c \cdot b = d \cdot a \Rightarrow (c, d)\ R\ (a, b)$.
   Transitiva: si $(a, b)\ R\ (c, d)$ i $(c, d)\ R\ (e, f)$, llavors $ad = bc$ i $cf = de$. Per tant, $adf = bcf = bde$. Simplificant per d, que és diferente de 0, per hipòtesi, obtenim que $af = be$. És a dir, $(a, b)\ R\ (e, f)$.

2) La classe d'equivalència d'un element és el conjunt dels elements que estan relacionats amb ell.

$$[(a, b)] = \{(x, y) : ay = bx\} = \{(x, y) : \frac{y}{x} = \frac{b}{a}\}$$

   Recordem que per hipòtesi, $a \neq 0$ i $x \neq 0$. Per tant, els elements de la classe de (a, b) són els parells que donen el quocient $b/a \in \mathbb{Q}$.

3) El conjunt quocient és el conjunt que té per elements les classes d'equivalència:

$$A/R = \{[(a, b)] : (a, b) \in A\}.$$

   Com hem vist a l'apartat anterior, cada classe d'equivalència ve *donada* per un quocient b/a d'enters no nuls. Per tant, hi ha tantes classes com possibles quocients d'enters no nuls.

56

Pas inicial: $n = 0$. Efectivament, $0^3 + 3 \cdot 0^2 + 2 \cdot 0 = 0 = 6 \cdot 0$.
Pas d'inducció: fixem un enter $m \geq 0$ i suposem (hipòtesi d'inducció) que:

$$m^3 + 3m^2 + 2m = 6k,$$

per a cert enter k. Volem demostrar que $(m + 1)^3 + 3(m + 1)^2 + 2(m + 1)$ és un múltiple de 6. Tenim:

$$\begin{aligned}(m + 1)^3 + 3(m + 1)^2 + 2(m + 1) &= (m^3 + 3m^2 + 3m + 1) \\ &\quad + 3(m^2 + 2m + 1) + 2m + 2 \\ &= (m^3 + 3m^2 + 2m) + (3m^2 + 9m + 6)\end{aligned}$$

apliquem l'hipòtesi d'inducció:

$$= 6k + (3m^2 + 9m + 6)$$

Ara observem que $3m^2 + 9m + 6 = 3m(m + 3) + 6$. Com que m i $m + 3$ tenen paritat diferent, el seu producte sempre és parell. Per tant, $3m(m+3)$ és múltiple de 6. És a dir, $3m^2 + 9m + 6 = 6k'$, per a cert enter k'.

57

1) Aquesta proposició diu que si la suma de dos enters és un nombre parell, llavors ambdós sumands són senars. Clarament això és fals, com mostra el següent contraexemple: $b = 0$, $c = 2$, $a = 0 + 2 = 2$.

2) Siguin $x, y \in A$. Si $h(x) = h(y)$, llavors $(x, b_0) = (y, b_0)$. Per tant, donat que tenim parells ordenats $x = y$ i $b_0 = b_0$. És a dir, h és injectiva.

58

1) Hem de provar que és reflexiva, simètrica i transitiva.

   Reflexiva: $a + b = b + a$. Per tant: $(a, b)\ R\ (a, b)$.
   Simètrica: $(a, b)\ R\ (c, d) \Rightarrow a + d = b + c \Rightarrow c + b = d + a \Rightarrow (c, d)\ R\ (a, b)$.
   Transitiva: si $(a, b)\ R\ (c, d)$ i $(c, d)\ R\ (e, f)$, llavors $a + d = b + c$ i $c + f = d + e$. Per tant, $a + d + f = b + c + f = b + d + e$. Simplificant per d obtenim que $a + f = b + e$. És a dir, $(a, b)\ R\ (e, f)$.

2) La classe d'equivalència d'un element és el conjunt dels elements que estan relacionats amb ell.

$$[(0, b)] = \{(x, y) : y = b + x\}$$

   Per tant, els elements de la classe de $(0, b)$ són els punts (x, y) amb coordenades enteres de la recta d'equació $y = x + b$.

3) El conjunt quocient és el conjunt que té per elements les classes d'equivalència:

$$A/R = \{[(a, b)] : (a, b) \in A\}.$$

   Com hem vist a l'apartat anterior, la classe d'equivalència de $(0, b)$ està formada pels punts amb coordenades enteres de la recta $y = x + b$. Però, $[(a, b)] = [(0, b - a)]$. Per tant, el conjunt quocient és el conjunt de les rectes que tenen equació de la forma $y = x + b$, on $b \in \mathbb{Z}$ (de cada recta només agafem els punts de coordenades enteres).

59

Pas inicial: $n = 0$. Efectivament, $(0 + 1)^3 - 0 - 1 = 0 = 6 \cdot 0$.
Pas d'inducció: fixem un enter $m \geq 0$ i suposem (hipòtesi d'inducció) que:

$$(m + 1)^3 - m - 1 = 6k,$$

per a cert enter k. Volem demostrar que $(m+2)^3-(m+1)-1$ és un múltiple de 6. Tenim:

$$\begin{aligned}(m+2)^3-(m+1)-1 &= (m^3+6m^2+12m+8)-m-1-1\\ &= m^3+6m^2+11m+6\\ &= [(m^3+3m^2+3m+1)-m-1]\\ &\quad\ +m+1+3m^2+8m+5\\ &= [(m+1)^3-m-1]+3m^2+9m+6\end{aligned}$$

apliquem l'hipòtesi d'inducció:

$$= 6k+(3m^2+9m+6)$$

Ara observem que $3m^2+9m+6=3m(m+3)+6$. Com que m i $m+3$ tenen paritat diferent, el seu producte sempre és parell. Per tant, $3m(m+3)$ és múltiple de 6. És a dir, $3m^2+9m+6=6k'$, per a cert enter k'.

2.3 Examen final 17/01/2011

60

1) Aquesta proposició diu que 'tot enter n es pot expressar com a una suma d'un múltiple de 5 i un múltiple de 7' i és certa. Efectivament, 5 i 7 són primers entre ells, és a dir, $\mathrm{mcd}(5,7)=1$. Per la identitat de Bézout, existeixen enters r,s tals que $1=5r+7s$. Donat un enter n qualsevol, escrivim: $n=5rn+7sn$ i prenem $a=rn$ i $b=sn$.

2) La primera proposició és equivalent a $((\neg p)\vee q)\wedge(\neg r)$ i aquesta proposició no és lògicament equivalent a $(\neg p)\wedge q\wedge(\neg r)$. Això es pot veure de dues maneres: fent les taules de veritat (exercici) i observant que no sempre tenen els mateixos valors de veritat o bé trobant un contraexemple; és a dir, tres proposicions p, q i r tals que les proposicions compostes anteriors tinguin valors de veritat diferents. Per exemple, si prenem $p=q=r$ una proposició falsa, obtenim que $((\neg p)\vee q)\wedge(\neg r)$ és certa i $(\neg p)\wedge q\wedge(\neg r)$ és falsa. Per tant, no són lògicament equivalents.

3) Aquesta propietat és falsa. Per veure-ho, és suficient trobar un contraexemple. Prenem $X=\{1,2\}$ i $Y=\{a,b\}$ i $f(1)=f(2)=a$. Llavors $f^{-1}(Y)=X$ i $f(f^{-1}(Y))=f(X)=\{a\}\neq Y$.

61 Posem $d_1=\mathrm{mcd}(a,b)$ i $d_2=\mathrm{mcd}(bc-a,b)$. Anem a provar que $d_1\mid d_2$ i que $d_2\mid d_1$.

- Tenim: $d_1=\mathrm{mcd}(a,b)\Rightarrow d_1\mid a\wedge d_1\mid b$. Per la linealitat: $d_1\mid bc-a$, per a qualsevol $c\in\mathbb{Z}$. És a dir, d_1 és un divisor comú de b i de $bc-a$. Per definició de mcd, $d_1\mid d_2$.
- Tenim: $d_2=\mathrm{mcd}(bc-a,b)\Rightarrow d_2\mid bc-a\wedge d_2\mid b$. Per la linealitat: $d_2\mid(bc-(bc-a))$. És a dir, $d_2\mid a$ i $d_2\mid b$. Per definició de mcd: $d_2\mid d_1$.

Ara bé, d_1 i d_2 són positius, per definició de mcd, i cadascun divideix a l'altre. Per tant: $d_1 = d_2$.

62

1) Provem per separat que és injectiva i exhaustiva.

- Injectiva: suposem que $f(\overline{x}) = f(\overline{y})$. Llavors:

$$\overline{22} \cdot \overline{x} + \overline{7} = \overline{22} \cdot \overline{y} + \overline{7} \Rightarrow \overline{22} \cdot \overline{x} = \overline{22} \cdot \overline{y} \Rightarrow \overline{a} \cdot \overline{22} \cdot \overline{x} = \overline{a} \cdot \overline{22} \cdot \overline{y} \Rightarrow \overline{x} = \overline{y}$$

  on: primer hem restat a tots dos membres $\overline{7}$ i després hem multiplicat per $\overline{a}$, la classe inversa de $\overline{22}$, que existeix perquè $\text{mcd}(22, 29) = 1$.

- Sigui $\overline{y} \in \mathbb{Z}_{29}$ una classe arbitrària. Volem veure que hi ha una classe $\overline{x}$ tal que $\overline{22} \cdot \overline{x} + \overline{7} = \overline{y}$. Un altre cop, considerem la classe inversa $\overline{a}$ de $\overline{22}$. Llavors, podem aïllar la $\overline{x}$ de la igualtat anterior i obtenim: $\overline{x} = \overline{a}(\overline{y} - \overline{7})$. Per tant, és exhaustiva.

Per trobar l'aplicació inversa hem de calcular la classe $\overline{a}$. Calculem la identitat de Bézout de 29 i 22 i obtenim: $29 \cdot (-3) + 22 \cdot 4 = 1$. Per tant, $\overline{a} = \overline{4}$. Així doncs: $f^{-1}(\overline{x}) = \overline{4}(\overline{x} - \overline{7}) = \overline{4} \cdot \overline{x} + \overline{1}$.

2) Per descodificar escrivim el nombre que li correspon a cada símbol i li apliquem f^{-1}:

$$\begin{array}{rll}
K \mapsto 10 & \to f^{-1}(\overline{10}) = \overline{41} = \overline{12} & \mapsto M \\
Z \mapsto 25 & \to f^{-1}(\overline{25}) = \overline{101} = \overline{14} & \mapsto O \\
R \mapsto 17 & \to f^{-1}(\overline{17}) = \overline{69} = \overline{11} & \mapsto L \\
T \mapsto 19 & \to f^{-1}(\overline{19}) = \overline{77} = \overline{19} & \mapsto T \\
, \mapsto 28 & \to f^{-1}(\overline{28}) = \overline{113} = \overline{26} & \mapsto \\
A \mapsto 0 & \to f^{-1}(\overline{0}) = \overline{1} & \mapsto B \\
I \mapsto 8 & \to f^{-1}(\overline{8}) = \overline{33} = \overline{4} & \mapsto E
\end{array}$$

Per tant, el missatge original és: 'MOLT BE'.

63 Solució 1: Observem que, per a tot $n \geq 0$:

$$2^{n+2} + 3^{2n+1} \equiv 4 \cdot 2^n + 3 \cdot 9^n \equiv 4 \cdot 2^n + 3 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \pmod 7.$$

Solució per inducció:
Cas inicial $n = 0$: $2^2 + 3^1 = 7 \equiv 0 \pmod 7$.
Pas inductiu: fixem un enter $n \geq 0$ i suposem que (H.I.) $2^{n+2} + 3^{2n+1} \equiv 0 \pmod 7$. Ara tenim:

$$2^{n+3} + 3^{2n+3} = 2 \cdot 2^{n+2} + 9 \cdot 3^{2n+1} \equiv 2(2^{n+2} + 3^{2n+1}) \equiv 0 \pmod 7$$

on a l'última congruència hem aplicat la hipòtesi d'inducció. (A més, observeu que $9 \equiv 2 \pmod 7$.)

2.4 Exàmens de taller 2010–2011 Q2

64 Primer observem que $\neg p \equiv pXp \equiv pOp$.

a) $p \wedge q \equiv \neg(pXq) \equiv (pXq)X(pXq)$.

b) $p \vee q \equiv (\neg p)X(\neg q) \equiv (pXp)X(qXq)$.

c) $p \to q \equiv pX(\neg q) \equiv pX(qXq)$.

d) $p \wedge q \equiv (\neg p)O(\neg q) \equiv (pOp)O(qOq)$.

e) $p \vee q \equiv \neg(pOq) \equiv (pOq)O(pOq)$.

f) $p \to q \equiv \neg((\neg p)Oq) \equiv \neg((pOp)Oq) \equiv ((pOp)Oq)O((pOp)Oq))$.

g)

$$\begin{aligned} pXq &\equiv \neg((\neg p)O(\neg q)) \\ &\equiv \neg((pOp)O(qOq)) \\ &\equiv ((pOp)O(qOq))O((pOp)O(qOq)) \end{aligned}$$

h)

$$\begin{aligned} pOq &\equiv \neg((\neg p)X(\neg q)) \\ &\equiv \neg((pXp)X(qXq)) \\ &\equiv ((pXp)X(qXq))X((pXp)X(qXq)) \end{aligned}$$

65

a) Condició necessària, però no suficient: que $4n$ sigui múltiple de 4. Si n és parell, llavors $4n$ és múltiple de 4. Però el recíproc no és cert.

b) Condició suficient, però no necessària: que n sigui múltiple de 4. Si n és múltiple de 4, llavors n és parell. Però el recíproc no és cert.

66 És a dir, és certa la implicació: 'si n i m són enters parells, aleshores $n + m$ és parell'? Sí. Però no és suficient, ja que si n i m són senars, llavors la suma també és parell.

67 Per exemple: n és múltiple de 6 si, i només si, n és parell i múltiple de 3. Una condició necessària però no suficient: 'si n és múltiple de 6, llavors n és múltiple de 3'. Una condició suficient, però no necessària: 'si n és múltiple de 12, llavors n és múltiple de 6'.

68

a) És el mateix que negar que 'hi ha tres enters diferents que compleixen P'. És a dir:

$$\neg(\exists x, y, z \in \mathbb{Z}(P(x) \wedge P(y) \wedge P(z) \wedge x \neq y \wedge x \neq z \wedge y \neq z))$$

Si neguem el quantificador existencial, obtenim la proposició equivalent:

$$\forall x, y, z \in \mathbb{Z}(\neg P(x) \vee \neg P(y) \vee \neg P(z) \vee x = y \vee x = z \vee y = z)$$

Equivalentment, si tenim en compte les lleis de De Morgan i que $p \to q$ és equivalent a $(\neg p) \vee q$, obtenim la proposició:

$$\forall x, y, z \in \mathbb{Z}(P(x) \wedge P(y) \wedge P(z) \to x = y \vee y = z \vee x = z))$$

b) Per exemple, si $P(x)$ és el predicat '$x^2 = 1'$, llavors l'enunciat és vertader.

c) Per exemple, si $P(x)$ és el predicat '$x(x^2 - 1) = 0$', llavors l'enunciat és fals.

69

a) $\exists x, y, z \in \mathbb{Z}(P(x) \wedge P(y) \wedge P(z) \wedge x \neq y \wedge x \neq z \wedge y \neq z)$

b) Per exemple, si $m(x)$ és un polinomi amb coeficients enters, i considerem el predicat $P(x)$: '$m(x)(x-1)(x-2)(x-3) = 0$', llavors hi ha al menys tres enters que la compleixen; en efecte, $P(1)$, $P(2)$ i $P(3)$ són vertaderes.

c) Per exemple, si $P(x)$ és el predicat '$(x-1)(x-2) = 0$, llavors només hi ha dos enters que el compleixen.

70 És a dir, és certa la implicació '$A \wedge (B \to A) \Rightarrow B$'? No. Per exemple, si A és una proposició certa i B és una proposició falsa, llavors la proposició $A \wedge (B \to A)$ és certa però B és falsa. Per tant, en aquest cas, la segona proposició no es pot deduir de la primera proposició. La implicació correcta és: '$B \wedge (B \to A) \Rightarrow A$'.

71 Es tracta d'una demostració per casos, on els casos són: cas 1) p és certa; cas 2) $\neg p$ és certa (és a dir, p és falsa). En el primer cas, es demostra que si, a més, $\neg q$ és certa, llavors r és certa. És a dir, es demostra que $q \vee r$ és certa (perquè $\neg q \to r$ és equivalent a $q \vee r$). En el segon cas, es demostra que si, a més, $\neg r$ és certa, llavors q és certa; és a dir, que $r \vee q$ és certa (perquè $\neg r \to q$ és equivalent a $r \vee q$). Per tant, es tracta de la demostració de $q \vee r$. Aquest raonament no és una demostració de la proposició $q \wedge r$. Per exemple, si q és falsa, el raonament anterior és una demostració de la proposició $q \vee r$, però no ho és de $q \wedge r$.

72

1) Siguin A, B i C conjunts arbitraris.

a) Sigui $x \in (A - B) \cup C$. Llavors:

$$\begin{aligned} x \in (A - B) \cup C &\Rightarrow (x \in A \wedge x \notin B) \vee x \in C \\ &\Rightarrow (x \in A \vee x \in C) \wedge (x \notin B \vee x \in C) \end{aligned}$$

És a dir, tenim que $x \in A \cup C$ i, per tant, podem dir que $x \in A \cup B \cup C$, i a més tenim que $x \notin B \vee x \in C$. Si $x \notin B$, llavors $x \notin A \cap B$; i si $x \in C$, com que per hipòtesi $B \cap C = \emptyset$, tenim que $x \notin B$ i, per tant, $x \notin A \cap B$. Resumint, tenim que x és un element del conjunt $(A \cup B \cup C) - (A \cap B)$.

b) No, la igualtat no és certa, com mostra el contraexemple següent: $A = \{1, 2\}$, $B = \{2\}$, $C = \{2, 3\}$.

2) Per exemple, $f(n) = 2n$, per a tot $n \in \mathbb{Z}$. És injectiva: si $f(n_1) = f(n_2)$, llavors $2n_1 = 2n_2$ i, per tant, $n_1 = n_2$. Però no és exhaustiva perquè la imatge d'un enter sempre és parell. Per tant, els senars no tenen antiimatge.

73

1) Tenim:

$$\begin{aligned} x \in A - (B - C) &\Rightarrow x \in A \wedge x \notin B - C \\ &\Rightarrow x \in A \wedge (x \notin B \vee x \in C) \\ &\Rightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \in C) \\ &\Rightarrow x \in (A - B) \cup (A \cap C) \\ &\Rightarrow x \in (A - B) \cup C \end{aligned}$$

La igualtat no és certa, en general, com mostra el contraexemple següent: $A = \{1, 2, 3\}$, $B = \{2, 3\}$, $C = \{3, 4\}$.

2) Per exemple, l'aplicació f definida de la manera següent. $f(2n) = 2(n - 1)$, si $n \geq 1$ i $f(m) = m$ en qualsevol altre cas. És a dir, f envia el zero, els enters negatius i els positius senars a ells mateixos i cada enter parell positiu a l'enter parell anterior. Llavors f no és injectiva perquè $f(0) = f(2) = 0$. Però sí que és exhaustiva: l'antiimatge d'un enter negatiu o un enter positiu senar és ell mateix; el zero té dues antiimatges, com acabem de veure; i l'antiimatge d'un enter parell positiu és l'enter parell positiu següent.

74

1) Tenim:

$$\begin{aligned} x \in (A - B) \cap (A - C) &\Rightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \\ &\Rightarrow x \in A \wedge (x \notin B \wedge x \notin C) \\ &\Rightarrow x \in A \wedge x \notin (B \cup C) \\ &\Rightarrow x \in A \wedge x \notin (B \cap C) \\ &\Rightarrow x \in A - (B \cap C) \end{aligned}$$

La igualtat no és certa, com mostra el contraexemple següent: $A = \{1, 2, 3\}$, $B = \{1, 2\}$, $C = \{1, 3\}$.

2) Per exemple, $f(n) = n + 1$. La seva inversa és $f^{-1}(n) = n - 1$.

75

1) Tenim:

$$\begin{aligned} x \in A - (B \cup C) &\Rightarrow x \in A \wedge x \notin B \cup C \\ &\Rightarrow x \in A \wedge (x \notin B \wedge x \notin C) \\ &\Rightarrow (x \in A \wedge x \notin B) \wedge (x \in A \wedge x \notin C) \\ &\Rightarrow x \in (A - B) \cap (A - C) \subseteq (A - B) \cup (A - C) \end{aligned}$$

La igualtat no és certa en general, com mostra el contraexemple següent: $A = \{1, 2, 3, 4\}$, $B = \{1, 2\}$, $C = \{1, 3\}$.

2) Per exemple, l'aplicació que permuta els nombres 0 i 1 i envia els altres nombres naturals a ells mateixos. És a dir: $f(0) = 1$, $f(1) = 0$ i $f(n) = n$, si $n \geq 2$. La seva inversa és ella mateixa: $f^{-1} = f$.

76

1) La implicació: $f[P] = f[Q] \Rightarrow P = Q$ no és certa, en general, com mostra el contraexemple següent: $A = B = \{1, 2\}$, $f(1) = f(2) = 1$, $P = \{1\}$ $Q = \{2\}$. Tenim que $f[P] = f[Q] = \{1\}$, però $P \neq Q$.

   Suposem que l'aplicació f és injectiva i que $f[P] = f[Q]$. Volem demostrar que $P = Q$. Sigui $x \in P$. Llavors $f(x) \in f[P]$. Però, per hipòtesi $f[P] = f[Q]$; per tant, $f(x) \in f[Q]$. Això vol dir que existeix un element $x' \in Q$ tal que $f(x) = f(x')$. Com que f és injectiva, deduïm que $x = x'$. És a dir, $x = x' \in Q$. Per tant, hem demostrat que $P \subseteq Q$. Per simetria, deduïm que $P = Q$.

2) No, en les condicions del problema. Primer de tot, observem que A no pot set $\emptyset$, perquè si ho fos, llavors $A \times C = \emptyset = B \times C$ i en tal cas $B = \emptyset$ i sabem que $A \neq B$. Ara sigui $a \in A$. Com que $C \neq \emptyset$, sigui $c \in C$ un element arbitrari. Llavors $(a, c) \in A \times C = B \times C$ i, per tant, $(a, c) \in B \times C$; és a dir, $a \in B$. Conseqüentment, $A \subseteq B$. Per simetria, deduïm l'altra inclusió i, per tant, $A = B$. Contradicció.

77

1) La implicació: $f^{-1}[S] = f^{-1}[T] \Rightarrow S = T$ no és certa en general, com mostra el contraexemple següent: $A = B = \{1, 2\}$, $f(1) = f(2) = 1$, $S = \{1\}$, $T = \{1, 2\}$. Llavors $f^{-1}[S] = f^{-1}[T] = \{1, 2\}$, però $S \neq T$.

   Suposem que f és exhaustiva i que $f^{-1}[S] = f^{-1}[T]$. Volem demostrar que $S = T$. Sigui $y \in S$. Com que f és exhaustiva, existeix $x \in A$ tal que $f(x) = y$, i com que $y \in S$, l'element x pertany a $f^{-1}[S] \subseteq A$. Però per hipòtesi, $f^{-1}[S] = f^{-1}[T]$; per tant, $x \in f^{-1}[T]$; és a dir, $f(x) = y \in T$. Hem demostrat doncs que $S \subseteq T$. Per simetria demostrem l'altra inclusió i per tant $S = T$.

2) No. Per exemple considerem els conjunts $A = \{1\}$, $B = \{2\}$, $C = \{a\}$, $D = \{b\}$. Llavors $(A \cup B) \times (C \cup D) = \{1, 2\} \times \{a, b\}$ que té quatre elements i $(A \times C) \cup (B \times D) = \{(1, a), (2, b)\}$ que només en té dos.

78

1) La igualtat: $f[A-C] = f[A]-f[C]$ no és certa en general, com mostra el contraexemple següent: $A = \{1, 2\}$, $B = \{a\}$, $C = \{1\} \subset A$, i l'aplicació $f\colon A \to B$ definida per $f(1) = f(2) = a$. Llavors $f[A - C] = \{a\}$ i $f[A] - f[C] = \emptyset$

   Suposem que f és injectiva. Demostrem primer l'inclusió $f[A - C] \subseteq f[A] - f[C]$. Sigui $y \in f[A - C]$. Llavors existeix $x \in A - C$ tal que $f(x) = y$. Com que $x \in A$, tenim que $f(x) \in f[A]$. Hem de demostrar a més que $y = f(x) \notin f[C]$. Ho fem per reducció a l'absurd. Suposem que $f(x) \in f[C]$. Llavors existeix un element $x' \in C$ tal que $f(x') = f(x)$. Observem que $x' \neq x$, perquè $x \in A - C$. Però ara tenim que $f(x) = f(x')$ i $x \neq x'$. Això és una contradicció amb el fet que f sigui injectiva. Per tant, $y = f(x) \notin f[C]$. És a dir, $y \in f[A] - f[C]$.

   Demostrem ara l'altra inclusió: $f[A]-f[C] \subseteq f[A-C]$. Sigui $y \in f[A]-f[C]$. Llavors existeix $x \in A$ tal que $f(x) = y$. D'altra banda no pot existir cap element de C que tingui per imatge a y, perquè $y \notin f[C]$. Per tant, podem assegurar que $x \in A - C$ i, conseqüentment, $y = f(x) \in f[A - C]$.

2) Si X/R només té un element, llavors qualsevol parell d'elements de X estan relacionats per R. Per tant, una possible relació pot ser: si $x, y \in X$, definim:xRy si, i només si $x, y \in X$ (de fet, funciona quasevol predicat que sempre sigui vertader).

79

Cas inicial: $n = 1$**:** $6 \cdot 7 - 2 \cdot 3 = 36$, que és múltiple de 4.

Pas d'inducció: Fixem un enter $m \geq 1$ i suposem que $6 \cdot 7^m - 2 \cdot 3^m = 4k$, per a cert $k \in \mathbb{Z}$ (hipòtesi d'inducció). Volem demostrar que $6 \cdot 7^{m+1} - 2 \cdot 3^{m+1}$ també és múltiple de 4. Tenim:

$$\begin{aligned} 6 \cdot 7^{m1} - 2 \cdot 3^{m+1} &= 7 \cdot 6 \cdot 7^m - 3 \cdot 2 \cdot 3^m \\ &= 3 \cdot (6 \cdot 7^m - 2 \cdot 3^m) + 4 \cdot 6 \cdot 7^m \\ &= 3 \cdot 4k + 4 \cdot 6 \cdot 7^m \qquad \text{per H.I.} \\ &= 4(3k + 6 \cdot 7^m) \end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

80

Cas inicial: $n = 0$**:** l'expressió dóna 0, que és un nombre enter.

Pas d'inducció: Fixem un enter $m \geq 0$ i suposem que $\frac{m^5}{5} + \frac{m^3}{3} + \frac{7m}{15} = k \in \mathbb{Z}$ (hipòtesi d'inducció). Volem demostrar que:

$$A = \frac{(m+1)^5}{5} + \frac{(m+1)^3}{3} + \frac{7(m+1)}{15}$$

també és un enter. Tenim:

$$\begin{aligned} A &= \frac{(m^5 + 5m^4 + 10m^3 + 10m^2 + 5m + 1)}{5} + \frac{m^3 + 3m^2 + 3m + 1)}{3} + \frac{7m+7}{15} \\ &= \left(\frac{m^5}{5} + \frac{m^3}{3} + \frac{7m}{15}\right) + (m^4 + 3m^3 + 2m^2 + 2 + 1) \\ &= k + (m^4 + 3m^3 + 2m^2 + 2 + 1) \qquad \text{per H.I.} \end{aligned}$$

que és un enter.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 0$.

81

Cas inicial: $n = 0$**:** l'expressió dóna 9, que és múltiple de 9.

Pas d'inducció: Fixem un enter $m \geq 0$ i suposem que $m^3 + (m+1)^3 + (m+2)^3 = 9k$, per a cer $k \in \mathbb{Z}$ (hipòtesi d'inducció). Volem demostrar que:

$$A = (m+1)^3 + (m+2)^3 + (m+3)^3$$

també és un múltiple de 9. Tenim:

$$\begin{aligned} A &= (9k - m^3) + (m+3)^3 \qquad \text{per H.I.} \\ &= 9k - m^3 + m^3 + 9m^2 + 27m + 27 \\ &= 9k + 9m^2 + 27m + 27 \\ &= 9(k + m^2 + 3m + 3) \end{aligned}$$

que és un múltiple de 9.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 0$.

82

Cas inicial: $n = 0$**:** $8^{0+2} + 9^{0+1} = 64 + 9 = 73$, que és múltiple de 73.

Pas d'inducció: Fixem un enter $m \geq 0$ i suposem que $8^{m+2} + 9^{2m+1} = 73k$, per a cer $k \in \mathbb{Z}$ (hipòtesi d'inducció). Volem demostrar que:

$$8^{m+3} + 9^{2m+3}$$

també és un múltiple de 73. Tenim:

$$\begin{aligned} 8^{m+3} + 9^{2m+3} &= 8 \cdot 8^{m+2} + 9^2 \cdot 9^{2m+1} \\ &= 8 \cdot (8^{m+2} + 9^{2m+1}) + 73 \cdot 9^{2m+1} \\ &= 8 \cdot 73k + 73 \cdot 9^{2m+1} \qquad \text{per H.I.} \\ &= 73(8k + 9^{2m+1}) \end{aligned}$$

que és un múltiple de 73.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 0$.

83

Cas inicial: $n = 1$**:** $2!/2 = 1 \in \mathbb{Z}$.

Pas d'inducció: Fixem un enter $m \geq 1$ i suposem que $(2m)!/2^m = k \in \mathbb{Z}$ (hipòtesi d'inducció). Volem demostrar que:

$$\frac{(2(m+1))!}{2^{m+1}} = \frac{(2m+2)!}{2^{m+1}} \in \mathbb{Z}.$$

Tenim:

$$\frac{(2m+2)!}{2^{m+1}} = \frac{(2m+2)(2m+1)(2m)!}{2 \cdot 2^m} = (m+1)(2m+1)k \in \mathbb{Z}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

84

Cas inicial: $n = 1$**:** $2!/1!2 = 1 \in \mathbb{Z}$.

Pas d'inducció: Fixem un enter $m \geq 1$ i suposem que $(2m)!/m!2^m = k \in \mathbb{Z}$ (hipòtesi d'inducció). Volem demostrar que:

$$\frac{(2(m+1))!}{(m+1)!2^{m+1}} = \frac{(2m+2)!}{(m+1)!2^{m+1}} \in \mathbb{Z}.$$

Tenim:

$$\frac{(2m+2)!}{2^{m+1}} = \frac{(2m+2)(2m+1)(2m)!}{(m+1)m!2 \cdot 2^m} = (2m+1)k \in \mathbb{Z}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

2.5 Examen parcial 28/04/2011

86

1)
- R és reflexiva: donat $(x, y) \in \mathbb{R} \times \mathbb{R}$, tenim que $|x| + |y| = |x| + |y|$; és a dir, $(x, y)R(x, y)$;
- R és simètrica: si $(x, y)R(z, t)$, llavors $|x| + |y| = |z| + |t|$, i, per tant, tenim que $|z| + |t| = |x| + |y|$. És a dir, $(z, t)R(x, y)$;
- R és transitiva: si $(x, y)R(z, t)$ i $(z, t)R(u, v)$, llavors $|x|+|y| = |z|+|t|$ i $|z|+|t| = |u| + |v|$. Per tant, $|x| + |y| = |u| + |v|$ i llavors $(x, y)R(u, v)$.

2) Per definició de classe d'equivalència:

$$[(0,1)] = \{(x,y) : (x,y)R(0,1)\} = \{(x,y) : |x| + |y| = 1\}$$

Per tant, hem de dibuixar el conjunt de punts (x,y) del pla tals que $|x| + |y| = 1$. Distingim quatre casos:

a) si $x \geq 0, y \geq 0$, llavors dibuixem el segment determinat per la recta $x + y = 1$ al primer quadrant;

b) si $x \geq 0, y \leq 0$, llavors dibuixem el segment determinat per la recta $x - y = 1$ al quart quadrant;

c) si $x \leq 0, y \geq 0$, llavors dibuixem el segment determinat per la recta $-x + y = 1$ al segon quadrant;

d) si $x \leq 0, y \leq 0$, llavors dibuixem el segment determinat per la recta $-x - y = 1$ al tercer quadrant;

És a dir, la classe d'equivalència de $(0,1)$ és el conjunt de punts que estan sobre el perímetre del quadrat de vèrtexs $(0,1), (-1,0), (0,-1), (1,0)$.

87

1) Sigui $A \in \mathcal{P}(X) \cup \mathcal{P}(Y)$. Llavors $A \in \mathcal{P}(X)$ o $A \in \mathcal{P}(Y)$. És a dir, $A \subseteq X$ o $A \subseteq Y$. Com que $X \subseteq X \cup Y$ i $Y \subseteq X \cup Y$, tenim en qualsevol cas que $A \subseteq X \cup Y$. Per tant, $A \in \mathcal{P}(X \cup Y)$.

2) L'altra inclusió no és certa, perquè un subconjunt de $X \cup Y$ pot tenir elements de X que no són de $X \cap Y$ i elements de Y que tampoc són de $X \cap Y$. Posem un contraexemple. Si prenem $X = \{1\}$, $Y = \{2\}$, i $A = \{1,2\}$, llavors $A \in \mathcal{P}(X \cup Y)$, però $A \notin \mathcal{P}(X)$ i $A \notin \mathcal{P}(Y)$.

88

1) Siguin $x, x' \in A$ i suposem que $g(x) = g(x')$. Llavors: $x = f(g(x)) = f(g(x')) = x'$, ja que $f \circ g = I_A$. És a dir, g és injectiva.

2) Sigui $y \in A$. Hem de veure que existeix un $x \in A$ tal que $f(x) = y$. Però $y = f(g(y))$. Per tant, podem prendre $x = g(y)$. És a dir, f és exhaustiva.

3) No. Per exemple, prenem $A = \mathbb{N}$; $g(n) = n + 1$; i $f(n) = n - 1$, si $n \geq 1$, $f(0) = 0$. Llavors, $f(g(n)) = f(n+1) = n + 1 - 1 = n$; és a dir, $f \circ g = I_{\mathbb{N}}$. Però: $g(f(0)) = g(0) = 1 \neq 0$. Per tant, $g \circ f \neq I_{\mathbb{N}}$.

2.6 Examen final 06/06/2011

89

1) Apliquem l'algorisme d'Euclides estés, és a dir, calculem el màxim comú divisor i els coeficients enters de la identitat de Bézout.

1	0	1	-7	43	-93	136
0	1	-5	36	-221	478	-699
	5	7	6	2	1	2
1876	365	51	8	3	2	1
51	8	3	2	1	0	

És a dir: $1876 \cdot 136 + 365 \cdot (-699) = 1$.

2) Fem aquest apartat de dues maneres (equivalents): treballant amb classes a $\mathbb{Z}_{1876}$ i amb la notació de les congruències.

Amb classes: Hem de resoldre l'equació $\overline{365} \cdot \overline{x} + \overline{902} = -\overline{508}$. Passem restant $\overline{902}$ al segon membre: $\overline{365} \cdot \overline{x} = -\overline{508} - \overline{902} = \overline{466}$. Ara multipliquem per la classe inversa de $\overline{365}$, que existeix perquè $\operatorname{mcd}(365, 1876) = 1$, com hem comprovat abans. També s'ha calculat a l'apartat anterior que $\overline{365}^{-1} = \overline{-699} = \overline{1177}$. Per tant: $\overline{x} = \overline{1177} \cdot \overline{466} = \overline{690}$. Ara, el representant positiu més petit d'aquesta classe és precisament l'enter 690.

Amb congruències: Passem 902 restant al segon membre i obtenim:

$$365x \equiv -1410 \equiv 466 \pmod{1876}.$$

Ara, multipliquem cada membre per l'invers de 365 mòdul 1876 (que existeix, perquè sabem que $\operatorname{mcd}(1876, 365) = 1$). Pel primer apartat, aquest invers és -699 mòdul 1876. Però: $-699 \equiv 1177 \pmod{1876}$. Per tant:

$$x \equiv 466 \cdot (-699) \equiv 466 \cdot 1177 = 548482 \equiv 690 \pmod{1876}$$

La resposta és 690.

90 Demostrem la propietat aplicant el principi d'inducció.

Cas inicial $n = 0$. Tenim: $\sum_{k=0}^{0} k2^{n-k} = 0$ i d'altra banda: $2^{n+1} - n - 2 = 2 - 0 - 2 = 0$.

Pas d'inducció. Fixem un enter $m \geq 0$ i suposem que:

$$\sum_{k=0}^{m} k2^{m-k} = 2^{m+1} - m - 2 \qquad \text{(H.I.)}$$

Volem demostrar que:

$$\sum_{k=0}^{m+1} k2^{m+1-k} = 2^{m+2} - (m+1) - 2 = 2^{m+2} - m - 3$$

Tenim:

$$\begin{aligned}
\sum_{k=0}^{m+1} k2^{m+1-k} &= \sum_{k=0}^{m+1} k2^{m-k} \cdot 2 \\
&= 2\left(\sum_{k=0}^{m} k2^{m-k} + \frac{(m+1)}{2}\right) \\
&= 2\left(2^{m+1} - m - 2 + \frac{m+1}{2}\right) && \text{apliquem la H.I.} \\
&= 2^{m+2} - 2m - 4 + m + 1 \\
&= 2^{m+2} - m - 3
\end{aligned}$$

Per tant, la propietat és certa per a tot $n \geq 0$.

91

1) Per a demostrar que la propietat $\operatorname{mcd}(m, n) = \operatorname{mcd}(m - n, m + n)$ no és certa, en general, hem de trobar un contraexemple. Si prenem $m = 5$ i $n = 3$, llavors tenim $m + n = 8$ i $m - n = 2$. Per tant:

$$\operatorname{mcd}(m, n) = \operatorname{mcd}(5, 3) = 1, \qquad \operatorname{mcd}(m - n, m + n) = \operatorname{mcd}(2, 8) = 2.$$

2) Hem de provar que:

$$\forall m, n \in \mathbb{Z} \ \ (m \text{ i } n \text{ tenen paritat diferent} \Rightarrow \operatorname{mcd}(m, n) = \operatorname{mcd}(m - n, m + n))$$

Denotem per $d_1 = \operatorname{mcd}(m, n)$ i $d_2 = \operatorname{mcd}(m - n, m + n)$. Veiem que $d_1|d_2$ i que $d_2|d_1$ i com que ambdós són positius, han de ser iguals.

- $d_1|m \wedge d_1|n \Rightarrow d_1|(m - n) \wedge d_1|(m + n) \Rightarrow d_1|\operatorname{mcd}(m - n, m + n) = d_2$. A la primera implicació hem aplicat la propietat de la linealitat de la divisibilitat i a la segona la definició de màxim comú divisor.
- Per hipòtesi, m i n tenen paritat diferent. Per tant, $m - n$ i $m + n$ són nombres enters senars. Conseqüentment, $d_2 = \operatorname{mcd}(m-n, m+n)$ ha de ser senar. Com que $d_2|(m-n)$ i $d_2|(m+n)$, es dedueix que $d_2|(m-n)+(m-n) = 2m$, per la propietat de linealitat de la divisibilitat. Però d_2 és senar; és a dir, $\operatorname{mcd}(d_2, 2) = 1$. Per tant, pel lema de Gauss, $d_2|m$. Anàlogament, tenim que $d_2|(m + n) - (m - n) = 2n$ (també per linealitat) i de la mateixa manera veiem que $d_2|n$. Per tant, $d_2|\operatorname{mcd}(m, n) = d_1$.

3) Hem de veure que la proposició:

$$\forall m, n \in \mathbb{Z} \ \ (\operatorname{mcd}(m, n) = \operatorname{mcd}(m - n, m + n) \Rightarrow m \text{ i } n \text{ tenen paritat diferent})$$

és falsa. És a dir, hem de trobar un contraexemple: dos enters m i n tals que $\operatorname{mcd}(m, n) = \operatorname{mcd}(m - n, m + n)$ i que tinguin la mateixa paritat. Per exemple $m = 4$ i $n = 2$ tenen la mateixa paritat. A més, resulta que $\operatorname{mcd}(m, n) = \operatorname{mcd}(4, 2) = 2$ i $\operatorname{mcd}(m - n, m + n) = \operatorname{mcd}(2, 6) = 2$.

2.7 Exàmens de taller 2011–2012 Q1

93

1) Sí, és suficient. Si m i n són múltiples de 3, llavors hi ha enters k, r tals que $m = 3k$ i $n = 3r$. Aleshores $m + n = 3k + 3r = 3(k + r)$. És a dir, $m + n$ és un múltiple de 3. Però no és una condició necessària. Si $m + n$ és múltiple de 3, llavors m i n no tenen per què ser múltiples de 3. Per exemple, $m = 1$ i $n = 2$.

2) Considerem els predicats: $Q(n)$: 'n és un quadrat'; $S(n)$: 'n és senar'. Llavors la proposició es pot formalitzar així:

   $$\exists n \in \mathbb{Z}(Q(n) \wedge S(n) \wedge 5|n)$$

   Ara, $Q(n)$ es formalitza així: '$\exists k \in \mathbb{Z}(n = k^2)$'; i $S(n)$ així: '$\exists m \in \mathbb{Z}(n = 2m + 1)$'.

   La seva negació és: '$\forall n \in \mathbb{Z}(\neg Q(n) \vee \neg S(n) \vee 5 \nmid n)$'.

94

1) És necessari i suficient. Suposem que n^2 és múltiple de 8. Llavors n^2 és parell i, per tant, n també. Però si n és parell, aleshores n^2 és múltiple de 4. Recíprocament, si n és múltiple de 4, llavors n^2 és múltiple de 16 i, en particular, també múltiple de 8.

2) '$\exists n \in \mathbb{N}(2 \nmid n \wedge 3 \nmid n \wedge 5 \mid n)$'. La negació és: '$\forall n \in \mathbb{N}(2 \mid n \vee 3 \mid n \vee 5 \nmid n)$'.

95

1) *Necessitat*: si $n = 2k$, per a cert $k \in \mathbb{Z}$, llavors $n^2 = 4k^2 = 2(2k^2)$ és parell. *Suficiència*: (pel contrarecíproc) si $n = 2r + 1$, per a cert $r \in \mathbb{Z}$, llavors $n^2 = 4r^2 + 4r + 1 = 2(2r^2 + 2r) + 1$ és senar.

2) '$\forall n(n \in \mathbb{N} \wedge n < 100 \to P(n^2 + n + 41))$', on $P(m)$ és el predicat 'm és primer'. La negació és: '$\exists n(n \in \mathbb{N} \wedge n < 100 \wedge \neg P(n))$'.

96

1) No, no és una condició necessària. Per exemple, 15 és un senar múltiple de 5 i no acaba en 55. Però sí és una condició suficient. Si un enter acaba en 55, llavors és un senar múltiple de 5.

2) '$\forall n \in \mathbb{N}\, \exists m, k \in \mathbb{N}(n = m^2 + k^2)$'. La negació és: '$\exists n \in \mathbb{N}\, \forall m, k \in \mathbb{N}(n \neq m^2 + k^2)$'.

97

1) No és necessari: per exemple, $(3+5)^2$ és senar, però 3 i 5 no són consecutius. Però sí és suficient: si n i m són consecutius, llavors, per exemple, $m = n+1$ i $(m+n)^2 = (2n+1)^2$, que és senar.

2) '$\forall n \in \mathbb{N}(2 \mid n^2 \vee S(n))$', on $S(n)$ és el predicat 'n acaba en 7'. La negació és: '$\exists n \in \mathbb{N}(2 \nmid n^2 \wedge \neg S(n))$'.

98

1) Sigui n un enter que acaba en 4, que no és múltiple de 4 i suposem que té la xifra de les desenes parella. Llavors podem escriure:

$$n = \sum_{k=0}^{l} 10^k \cdot x_k$$

on x_k són les xifres de n en base 10. Com que 10^k és múltiple de 4 si $k \geq 2$, per a que n sigui múltiple de 4 ha de ser $10x_1 + x_0$ múltiple de 4. Però per hipòtesi, x_1 és parell i $x_0 = 4$. Per tant, $10x_1 + 4$ és múltiple de 4 i, per tant, n també. Contradicció.

2) '$\forall n \in \mathbb{Z}(2 \mid n \vee A(n))$', on $A(n)$ és el predicat 'n^3 no acaba en 9'. La negació és: '$\exists n \in \mathbb{Z}(2 \nmid n \wedge \neg A(n))$'.

99

1) Sigui n un enter. Distingim dos casos: que n sigui parell o que n sigui senar. Si $n = 2k$, per a cert $k \in \mathbb{Z}$, llavors $n^3 = 8k^3$, que és múltiple de 8. Si $n = 2k + 1$, per a cert $k \in \mathbb{Z}$, llavors $n^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, que és senar.

2) '$\exists n \in \mathbb{Z}(C(n) \wedge 2 \mid n \wedge 8 \mid n)$', on $C(n)$ és el predicat 'n és un cub', que es pot formalitzar així '$\exists k \in \mathbb{Z}(n = k^3)$'. La negació és: '$\forall n \in \mathbb{Z}(\neg C(n) \vee 2 \nmid n \vee 8 \nmid n)$'.

100

1) Sigui $x \in \mathbb{Q}$ tal que $x^2 \in \mathbb{Z}$. Suposem que $x \notin \mathbb{Z}$. Escrivim x com a fracció irreductible $x = \frac{a}{b}$, amb $a, b \in \mathbb{Z}$, $b \neq 0$, $\mathrm{mcd}(a, b) = 1$. Llavors $x^2 = \frac{a^2}{b^2} \in \mathbb{Z}$ implica que $b^2 \mid a^2$. D'aqui deduïm que $b \mid a$. Per tant, $x \in \mathbb{Z}$. Contradicció.

2) '$\forall p, q \in \mathbb{N}(P(p) \wedge P(q) \to P(pq))$', on $P(n)$ és el predicat 'n és un nombre primer', que es pot formalitzar així '$\forall a, b \in \mathbb{N}(n = ab \to a = 1 \vee b = 1)$'. La negació és: '$\exists p, q \in \mathbb{N}(P(p) \wedge P(q) \wedge \neg P(pq))$'.

101

1) Suposem que mn no és senar; és a dir, mn és parell. Atès que n és múltiple de 3, tenim que mn també ho és. Per tant, mn és parell i múltiple de 3. És a dir, mn és múltiple de 6.

2) '$\forall n, m \in \mathbb{N}(P(n) \wedge P(m) \to 2 \mid (n + m))$', on $P(n)$ és el predicat 'n és primer'. La seva negació és: '$\exists n, m \in \mathbb{N}(P(n) \wedge P(m) \wedge 2 \nmid (n + m))$'.

102

1) Fem una demostració per casos segons el residu de la divisió de n entre 3. Aquest residu r por ser 0, 1 o 2. Cas 1: $r = 0$; llavors $n = 3q$, per a cert $q \in \mathbb{Z}$. Per tant, $n^2 = 9q^2 = 3(3q^2)$; és a dir, n^2 té residu 0. Cas 2: $r = 1$; llavors $n = 3q + 1$, per a cert $q \in \mathbb{Z}$. Per tant, $n^2 = 3q^2+6q+1 = 3(q^2+2q)+1$; és a dir, n^2 té residu 1. Cas 3: $r = 2$; llavors $n = 3q+2$, per a cert $q \in \mathbb{Z}$. Per tant, $n^2 = 9q^2 + 12q + 4 = 3(3q^2 + 4q + 1) + 1$; és a dir, n^2 té residu 1. Veiem doncs que el residu de la divisió de n^2 entre 3 és 0 o 1, però mai és 2.

2) '$\exists n \in \mathbb{Z}(Q(n) \wedge 2 \mid n \wedge 8 \not| \, n)$', on $Q(n)$ és el predicat 'n és un quadrat', que es pot formalitzar així: '$\exists k \in \mathbb{Z}(n = k^2)$'. La negació és: '$\forall n \in \mathbb{Z}(\neg Q(n) \vee 2 \not| \, n \vee 8 \mid n)$'.

103

1) Siguin $n, n' \in \mathbb{N}$ tals que $g(n) = g(n')$. És a dir, $2f(n) = 2f(n')$. D'aquí deduïm que $f(n) = f(n')$ i, com que f és injectiva, $n = n'$. Per tant, g és injectiva.

2) $\mathcal{P}(\emptyset) = \{\emptyset\}$; per tant, $\mathcal{P}(\mathcal{P}(\emptyset)) = \{\emptyset, \{\emptyset\}\}$.

104

1) Siguin $n, n' \in \mathbb{N}$ tals que $g(n) = g(n')$. És a dir, $2f(n)+1 = 2f(n')+1$. D'aquí deduïm que $f(n) = f(n')$ i, com que f és injectiva, $n = n'$. Per tant, g és injectiva.

2) Tenim:

$$B = A \cap B \subseteq A \subseteq A \cup B = B$$

(Les igualtats, per hipòtesi. Les inclusions són certes sempre.) Per tant: $B \subseteq A \subseteq B$, d'on $A = B$.

105

1) Siguin $n, n' \in \mathbb{Z}$ tals que $g(n) = g(n')$. És a dir, $f(n-1) = f(n'-1)$. Com que f és injectiva, deduïm que $n - 1 = n' - 1$ i, per tant, $n = n'$. Per tant, g és injectiva.

2) Tenim:

$$\begin{aligned} X \in \mathcal{P}(A - B) &\Leftrightarrow X \subseteq A - B \\ &\Leftrightarrow X \subseteq A \wedge X \cap B = \emptyset \\ &\Rightarrow X \in \mathcal{P}(A) \wedge X \notin \mathcal{P}(B) \\ &\Leftrightarrow X \in \mathcal{P}(A) - \mathcal{P}(B) \end{aligned}$$

És a dir, $\mathcal{P}(A - B) \subseteq \mathcal{P}(A) - \mathcal{P}(B)$. No obstant, l'altra inclusió no és certa, ja que $X \notin \mathcal{P}(B)$ no implica que $X \cap B = \emptyset$. Per exemple, si $A = \{1, 2, 3\}$, $B = \{1, 2, 4, 5\}$, $X = \{2, 3\}$, llavors $X \in \mathcal{P}(A) - \mathcal{P}(B)$, però $X \notin \mathcal{P}(A - B)$.

106

1) Siguin $m \in \mathbb{Z}$. Volem provar que existeix un $n \in \mathbb{Z}$ tal que $g(n) = m$. Però f és exhaustiva, per tant hi ha un $k \in \mathbb{Z}$ tal que $f(k) = m$. Si prenem $n = k - 1$, llavors $g(n) = g(k-1) = f(k) = m$. Per tant, g és exhaustiva.

2) És vertader.

$$\begin{aligned} X \in \mathcal{P}(A \cap B) &\Leftrightarrow X \subseteq A \cap B \\ &\Leftrightarrow X \subseteq A \wedge X \subseteq B \\ &\Leftrightarrow X \in \mathcal{P}(A) \wedge X \in \mathcal{P}(B) \\ &\Leftrightarrow X \in \mathcal{P}(A) \cap \mathcal{P}(B) \end{aligned}$$

107

1) Siguin $x, x' \in \mathbb{R}^*$ tals que $g(x) = g(x')$. Llavors $1/f(x) = 1/f(x')$ i, per tant, $f(x) = f(x')$. Com que f és injectiva, deduïm que $x = x'$. Per tant, g és injectiva.

2) És fals. Tenim:

$$\begin{aligned} &X \in \mathcal{P}(A^c) \Leftrightarrow X \subseteq A^c \Leftrightarrow X \cap A = \emptyset \\ &X \in \mathcal{P}(A)^c \Leftrightarrow X \notin \mathcal{P}(A) \Leftrightarrow X \nsubseteq A \end{aligned}$$

i està clar que la condició '$X \cap A = \emptyset$' no és equivalent a la condició '$X \nsubseteq A$' (però la primera implica la segona).

108

1) Sigui $y \in \mathbb{R}^*$. Volem provar que existeix un $x \in \mathbb{R}^*$ tal que $g(x) = 1/f(x) = y$. Però $1/f(x) = y$ equival a $f(x) = 1/y$. Com que f és exhaustiva, existeix un nombre real no nul x tal que $f(x) = 1/y$; és a dir, tal que $g(x) = y$. Per tant, g és exhaustiva.

2) Podem afirmar que A és el complementari de B o que B és el complementari de A. En efecte, si $A = \emptyset$ està clar. Suposem que $A \neq \emptyset$ i sigui $x \in A$; llavors $x \notin B$; és a dir $x \in B^c$. Això demostra que $A \subseteq B^c$. D'altra banda, si $x \in B^c$, llavors $x \notin B$. Però com que $\Omega = A \cup B$, tenim que $x \in A$. És a dir, $B^c \subseteq A$.

110

1) Siguin $n, n' \in \mathbb{Z}$ tals que $g(n) = g(n')$. Llavors $f(n-1)+1 = f(n'-1)+1$ i, per tant, $f(n-1) = f(n'-1)$. Com que f és injectiva, deduïm que $n - 1 = n' - 1$; és a dir, $n = n'$. Per tant, g és injectiva.

2) Sí. Per exemple, si $A = \{1, 2\}$ i R és una relació tal que $(1, 1) \in R$, però $(2, 2) \notin R$.

111

1) Sigui $m \in \mathbb{Z}$. Volem provar que existeix un $n \in \mathbb{Z}$ tal que $g(n) = m$. És a dir, tal que $f(n+1) - 1 = m$. Com que f és exhaustiva, existeix un enter k tal que $f(k) = m+1$. Llavors $g(k-1) = f(k) - 1 = m + 1 - 1 = m$ i, per tant, g és exhaustiva.

2) Sí. Fixem un element qualsevol $a_0 \in A$. Tenim:

$$x \in B \Leftrightarrow (a_0, x) \in A \times B = A \times C \Leftrightarrow x \in C$$

Per tant, $B = C$.

112

1) Siguin $n, n' \in \mathbb{Z}$ tals que $g(n) = g(n')$. Llavors $2f(n-1) = 2f(n'-1)$ i, per tant, $f(n-1) = f(n'-1)$. Com que f és injectiva, deduïm que $n - 1 = n' - 1$; és a dir, $n = n'$. Per tant, g és injectiva.

2) És fals. Contraexemple: $A = \{a, b\}$, $B = \{1, 2\}$, $Z = \{(a, 1), (b, 2)\}$. Llavors $Z \subseteq A \times B$, però no es pot escriure com un producte cartesià. En efecte, si $Z = X \times Y$, on $X \subseteq A$ i $Y \subseteq B$, llavors tindríem $a, b \in X$ i $1, 2 \in Y$. És a dir, $X = A$ i $Y = B$ i llavors $Z = X \times Y = A \times B$, que no és el cas.

113

Cas inicial: $n = 2$.

$$1 \cdot 3 = 3 = \frac{2(2-1)(4+5)}{6}$$

Pas d'inducció: Fixem un enter $n \geq 2$ i suposem que $\sum_{i=2}^{n} (i-1)(i+1) = \frac{n(n-1)(2n+5)}{6}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=2}^{n+1} (i-1)(i+1) = \frac{(n+1)n(2n+7)}{6}$$

Tenim:

$$\begin{aligned}
\sum_{i=2}^{n+1} (i-1)(i+1) &= \sum_{i=2}^{n} (i-1)(i+1) + n(n+2) \\
&= \frac{n(n-1)(2n+5)}{6} + n(n+2) \qquad \text{per H.I.} \\
&= \frac{n(n-1)(2n+5)}{6} + \frac{6n(n+2)}{6} \\
&= \frac{n(2n^2+9n+7)}{6} \\
&= \frac{n(n+1)(2n+7)}{6}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 2$.

114

Cas inicial: $n = 1$.

$$1^2 = 1 = \frac{1(2-1)(2+1)}{3}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n}(2i-1)^2 = \frac{n(2n-1)(2n+1)}{3}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1}(2i-1)^2 = \frac{(n+1)(2n+1)(2n+3)}{3}$$

Tenim:

$$\begin{aligned}
\sum_{i=1}^{n+1}(2i-1)^2 &= \sum_{i=1}^{n}(2i-1)^2 + (2n+1)^2 \\
&= \frac{n(2n-1)(2n+1)}{3} + (2n+1)^2 \qquad \text{per H.I.} \\
&= \frac{n(2n-1)(2n+1)}{3} + \frac{3(2n+1)^2}{3} \\
&= \frac{(2n+1)[n(2n-1)+3(2n+1)]}{3} \\
&= \frac{(2n+1)(n+1)(2n+3)}{3}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

115

Cas inicial: $n = 1$.

$$2^2 = 4 = \frac{2(1+1)(2+1)}{3}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n}(2i)^2 = \frac{2n(n+1)(2n+1)}{3}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1}(2i)^2 = \frac{2(n+1)(n+2)(2n+3)}{3}$$

Tenim:

$$\begin{aligned}\sum_{i=1}^{n+1}(2i)^2 &= \sum_{i=1}^{n}(2i)^2 + (2(n+1))^2 \\ &= \frac{2n(n+1)(2n+1)}{3} + 4(n+1)^2 \qquad \text{per H.I.} \\ &= \frac{2n(n+1)(2n+1)}{3} + \frac{12(n+1)^2}{3} \\ &= \frac{2(n+1)[n(2n+1)+6(n+1)]}{3} \\ &= \frac{2(n+1)(n+2)(2n+3)}{3}\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

116

Cas inicial: $n = 1$**.**

$$(-1)^2 \cdot 1^2 = 1 = (-1)^2 \cdot \frac{1+1}{2}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n}(-1)^{i+1}i^2 = (-1)^{n+1}\frac{n(n+1)}{2}$ (hipòtesi d'inducció). Volem demostrar:

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

Tenim:

$$\begin{aligned}\sum_{i=1}^{n+1}(-1)^{i+1}i^2 &= \sum_{i=1}^{n}(-1)^{i+1}i^2 + (-1)^{n+2}(n+1)^2 \\ &= (-1)^{n+1}\frac{n(n+1)}{2} + (-1)^{n+2}(n+1)^2 \qquad \text{per H.I.} \\ &= (-1)^{n+2}(n+1)\left(-\frac{n}{2}+n+1\right) \\ &= (-1)^{n+2}\frac{(n+1)(n+2)}{2}\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

117

Cas inicial: $n = 1$**.**

$$\frac{1}{(2-1)(2+1)} = \frac{1}{3} = \frac{1}{2+1}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} = \frac{n}{2n+1}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1} \frac{1}{(2i-1)(2i+1)} = \frac{n+1}{2n+3}$$

Tenim:

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{(2i-1)(2i+1)} &= \sum_{i=1}^{n} \frac{1}{(2i-1)(2i+1)} + \frac{1}{(2n+1)(2n+3)} \\
&= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} \qquad \text{per H.I.} \\
&= \frac{n(2n+3)+1}{(2n+1)(2n+3)} \\
&= \frac{2n^2+3n+1}{(2n+1)(2n+3)} \\
&= \frac{(n+1)(2n+1)}{(2n+1)(2n+3)} \\
&= \frac{n+1}{2n+3}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

118

Cas inicial: $n = 1$.

$$\frac{1}{(4-3)(4+1)} = \frac{1}{5} = \frac{1}{4+1}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n} \frac{1}{(4i-3)(4i+1)} = \frac{n}{4n+1}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1} \frac{1}{(4i-3)(4i+1)} = \frac{n+1}{4n+5}$$

Tenim:

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{(4i-3)(4i+1)} &= \sum_{i=1}^{n} \frac{1}{(4i-3)(4i+1)} + \frac{1}{(4n+1)(4n+5)} \\
&= \frac{n}{4n+1} + \frac{1}{(4n+1)(4n+5)} \qquad \text{per H.I.} \\
&= \frac{n(4n+5)+1}{(4n+1)(4n+5)} \\
&= \frac{4n^2+5n+1}{(4n+1)(4n+5)} \\
&= \frac{(n+1)(4n+1)}{(4n+1)(4n+5)} \\
&= \frac{n+1}{4n+5}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

119

Cas inicial: $n = 1$**.**

$$\frac{1}{(3-2)(3+1)} = \frac{1}{4} = \frac{1}{3+1}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n} \frac{1}{(3i-2)(3i+1)} = \frac{n}{3n+1}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1} \frac{1}{(3i-2)(3i+1)} = \frac{n+1}{3n+4}$$

Tenim:

$$\begin{aligned}
\sum_{i=1}^{n+1} \frac{1}{(3i-2)(3i+1)} &= \sum_{i=1}^{n} \frac{1}{(3i-2)(3i+1)} + \frac{1}{(3n+1)(3n+4)} \\
&= \frac{n}{3n+1} + \frac{1}{(3n+1)(3n+4)} \qquad \text{per H.I.} \\
&= \frac{n(3n+4)+1}{(3n+1)(3n+4)} \\
&= \frac{3n^2+4n+1}{(3n+1)(3n+4)} \\
&= \frac{(n+1)(3n+1)}{(3n+1)(3n+4)} \\
&= \frac{n+1}{3n+4}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

120

Cas inicial: $n = 2$**.**

$$1 - \frac{1}{2} = \frac{1}{2}$$

Pas d'inducció: Fixem un enter $n \geq 2$ i suposem que $\prod_{i=2}^{n} \left(1 - \frac{1}{i}\right) = \frac{1}{n}$ (hipòtesi d'inducció). Volem demostrar:

$$\prod_{i=2}^{n+1} \left(1 - \frac{1}{i}\right) = \frac{1}{n+1}$$

Tenim:

$$\begin{aligned}
\prod_{i=2}^{n+1} \left(1 - \frac{1}{i}\right) &= \prod_{i=2}^{n} \left(1 - \frac{1}{i}\right) \cdot \left(1 - \frac{1}{n+1}\right) \\
&= \frac{1}{n} \cdot \left(1 - \frac{1}{n+1}\right) \qquad \text{per H.I.} \\
&= \frac{1}{n} - \frac{1}{n(n+1)} \\
&= \frac{n+1-1}{n(n+1)} \\
&= \frac{1}{n+1}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

121

Cas inicial: $n = 2$**.**

$$1 - \frac{1}{2^2} = \frac{3}{4}$$

Pas d'inducció: Fixem un enter $n \geq 2$ i suposem que $\prod_{i=2}^{n} \left(1 - \frac{1}{i^2}\right) = \frac{n+1}{2n}$ (hipòtesi d'inducció). Volem demostrar:

$$\prod_{i=2}^{n+1} \left(1 - \frac{1}{i^2}\right) = \frac{n+2}{2(n+1)}$$

Tenim:

$$\begin{aligned}
\prod_{i=2}^{n+1}\left(1-\frac{1}{i^2}\right) &= \prod_{i=2}^{n}\left(1-\frac{1}{i^2}\right)\cdot\left(1-\frac{1}{(n+1)^2}\right)\\
&= \frac{n+1}{2n}\cdot\left(1-\frac{1}{(n+1)^2}\right) \qquad \text{per H.I.}\\
&= \frac{n+1}{2n}-\frac{n+1}{2n(n+1)^2}\\
&= \frac{n^2+2n}{2n(n+1)}\\
&= \frac{n+2}{2(n+1)}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

122

Cas inicial: $n = 1$**.**

$$\frac{1}{1\cdot 3} = \frac{1(3+5)}{4(1+1)(1+2)}$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $\sum_{i=1}^{n}\frac{1}{i(i+2)} = \frac{n(3n+5)}{4(n+1)(n+2)}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{i=1}^{n+1}\frac{1}{i(i+2)} = \frac{(n+1)(3n+8)}{4(n+2)(n+3)}$$

Tenim:

$$\begin{aligned}
\sum_{i=1}^{n+1}\frac{1}{i(i+2)} &= \sum_{i=1}^{n}\frac{1}{i(i+2)}+\frac{1}{(n+1)(n+3)}\\
&= \frac{n(3n+5)}{4(n+1)(n+2)}+\frac{1}{(n+1)(n+3)} \qquad \text{per H.I.}\\
&= \frac{n(3n+5)(n+3)+4(n+2)}{4(n+1)(n+2)(n+3)}\\
&= \frac{3n^3+14n^2+9n+8}{4(n+1)(n+2)(n+3)}\\
&= \frac{(n+1)^2(3n+8)}{4(n+1)(n+2)(n+3)}\\
&= \frac{(n+1)(3n+8)}{4(n+2)(n+3)}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

2.8 Examen parcial 17/11/2011

123

1) Si A, i B són conjunts, es defineix la diferència $A - B$ com el conjunt dels elements de A que no pertanyen a B; és a dir:

$$A - B = \{x : x \in A \wedge x \notin B\}.$$

Provem l'equivalència '$(C \subseteq A - B) \Leftrightarrow (C \subseteq A \wedge C \cap B = \emptyset)$'.

$\Rightarrow$) Suposem que $C \subseteq (A - B)$. a) Sigui $x \in C$. Per hipòtesi, tenim que $x \in A$ i $x \notin B$. Per tant, $x \in A$. És a dir: $C \subseteq A$. b) Ara hem de veure que $C \cap B = \emptyset$. Suposem que existeix $y \in C \cap B$. Llavors $y \in C$, i per tant, per hipòtesi, $y \notin B$. Però també tenim $y \in B$. Contradicció. És a dir, $C \cap B = \emptyset$.

$\Leftarrow$) Suposem que $C \subseteq A$ i que $C \cap B = \emptyset$. Sigui $x \in C$. Per hipòtesi, sabem que $x \in A$. Només cal veure que $x \notin B$. Però si $x \in B$, llavors $x \in C \cap B$. Contradicció, perquè per hipòtesi aquesta intersecció és buida. Per tant, $x \in (A - B)$.

2) Siguin A, B conjunts i $f : A \to B$ una aplicació. Si $B_1 \subseteq B$, llavors es defineix la antiimatge de B_1 per f per:

$$f^{-1}[B_1] = \{x \in A : f(x) \in B_1\}.$$

Provem que '$f^{-1}[B_1 \cap B_2] = f^{-1}[B_1] \cap f^{-1}[B_2]$', si $B_1, B_2 \subseteq B$. Per a tot x, tenim:

$$\begin{aligned}
x \in f^{-1}[B_1 \cap B_2] &\Leftrightarrow f(x) \in B_1 \cap B_2 && (1)\\
&\Leftrightarrow f(x) \in B_1 \wedge f(x) \in B_2 && (2)\\
&\Leftrightarrow x \in f^{-1}[B_1] \wedge x \in f^{-1}[B_2] && (1)\\
&\Leftrightarrow x \in f^{-1}[B_1] \cap f^{-1}[B_2] && (2)
\end{aligned}$$

(1): per definició d'antiimatge; (2): per definició d'intersecció.

124

1) Provem que R és reflexiva, simètrica i transitiva.

Reflexiva: si $n \in A$, llavors signe(n) = signe(n) i paritat(n) = paritat(n). Per tant $n\,R\,n$.

Simètrica: en efecte, ja que la definió de la relació R queda igual si intercanviem n per m.

Transitiva: suposem que $n\,R\,m$ i $m\,R\,t$. Distingim quatre casos:

a) n i m tenen el mateix signe i paritat; m i t tenen el mateix signe i paritat. En aquest cas deduïm que n i t tenen el mateix signe i paritat i, per tant, $n\,R\,t$.

b) n i m tenen el mateix signe i paritat; m i t tenen signe i paritat diferents. En aquest cas deduïm que n i t tenen signe diferent i paritat diferent. Per tant, $n\,R\,t$.

c) n i m tenen signe i paritats diferents; m i t tenen signe i paritats diferents. Llavors n i t tenen el mateix signe i la mateixa paritat. Per tant, $n\,R\,t$.

d) n i m tenen signe i paritat diferents; m i t tenen el mateix signe i la mateixa paritat. Aquest cas és similar al segon cas. Per tant, $n\,R\,t$.

2) Trobem la classe d'equivalència de l'element $1 \in A$. Un element n està relacionat amb 1 si o bé és positiu i senar o bé és negatiu i parell:

$$[1] = \{n \in A : n\,R\,1\} = \{1, 3, 5, \dots\} \cup \{-2, -4, -6, \dots\}$$

Anàlogament, els elements que estan relacionats amb el 2 són els positius i parells o bé els negatius i senars:

$$[2] = \{n \in A : n\,R\,2\} = \{2, 4, 6, \dots\} \cup \{-1, -3, -5, \dots\}$$

3) A l'apartat anterior observem que qualsevol elements de A (és a dir, qualsevol enter no nul) o bé pertany a la classe de 1 o bé pertany a la classe de 2. Per tant, no hi ha més classes. Això vol dir que el conjunt quocient és:

$$A/R = \{[1], [2]\}.$$

125

1) Comprovem primer que f és una aplicació de X en X. Si $1 \leq n \leq 50$, llavors $2 \leq f(n) = 2n \leq 100$ i si $51 \leq n \leq 100$, llavors $1 \leq f(n) = 2(n-51)+1 \leq 99$. És a dir, si $n \in X$, llavors hi ha un únic $m \in X$ tal que $f(n) = m$. En segon lloc, observem que donat $n \in A$, si $1 \leq n \leq 50$, llavors $f(n)$ és parell i si $51 \leq n \leq 100$, llavors $f(n)$ és senar. És a dir, pel contrarecíproc, si $f(n)$ és senar, llavors n està entre 51 i 100 i si $f(n)$ és parell, llavors n està entre 1 i 50.

Per a demostrar que f és bijectiva, hem de provar que f és injectiva i exhaustiva.

Injectivitat: suposem que $n, m \in A$ i que $f(n) = f(m)$. Si $f(n)$ és parell, llavors $f(m)$ també és parell, n i m estan entre 1 i 50 i, per tant, $f(n) = 2n = 2m = f(m)$, d'on $n = m$. Si $f(n)$ és senar, llavors $f(m)$ també és senar, n i m estan entre 51 i 100 i, per tant $f(n) = 2(n-51)+1 = 2(m-51)+1 = f(m)$, d'on també deduïm que $n = m$.

Exhaustivitat: sigui $k \in A$. Hem de trobar un $n \in A$ tal que $f(n) = k$. Si k és parell, llavors $k/2 \in A$ i $1 \leq k/2 \leq 50$ i $f(k/2) = 2(k/2) = k$. Si k és senar, llavors $51+(k-1)/2$ és enter i està entre 51 i 100. Per tant, $f(51+(k-1)/2) = k$.

2) De l'observació del principi se segueix que la imatge d'un element de A és senar si, i només si, l'element està entre 51 i 100. És a dir:

$$f^{-1}[S] = \{n \in A : f(n) \in S\} = \{n \in A : 51 \leq n \leq 100\}$$

2.9 Examen final 20/01/2012

126

1) La tècnica de demostració per reducció a l'absurd consisteix en prendre com a hipòtesi la negació de la proposició que volem demostrar i arribar a una contradicció; és a dir, demostrar que una proposició i la seva negació són certes.

   Provem, per reducció a l'absurd, que $\sqrt{2} \notin \mathbb{Q}$. Suposem que $\sqrt{2}$ és un nombre racional. Concretament, suposem que $\sqrt{2} = a/b$, on a, b són enters positius i primers entre ells. Elevant al quadrat tenim: $2b^2 = a^2$ [*]. És a dir, $2 \mid a^2$, d'on deduïm que $2 \mid a$ (ja que si a és senar, llavors a^2 és també senar). Per tant, podem escriure $a = 2a_1$, on $a_1 \in \mathbb{Z}$. Substituint a [*] i simplificant un 2, obtenim que $b^2 = 2a_1^2$. Però això vol dir que $2 \mid b^2$ i, per tant, que $2 \mid b$. Ara tenim que tant a com b són parells. Contradicció, ja que havíem suposat que eren primers entre ells.

2) Sigui $m \geq 1$ un enter. Diem que els enters a i b són congruents mòdul m si, i només si, $m \mid (a - b)$. O, equivalentment, si el residu de dividir a entre m és igual al residu de dividir b entre m. Ho escrivim així:

$$a \equiv b \pmod{m}$$

   És obvi que és una relació d'equivalència. Reflexiva: el residu de dividir a entre m és igual al residu de dividir a entre m. Simètrica: si el residu de dividir a entre m és igual al residu de dividir b entre m, llavors el residu de dividir b entre m és igual al residu de dividir a entre m. Transitiva: si el residu de dividir a entre m és igual al residu de dividir b entre m i el residu de dividir b entre m és igual al residu de dividir c entre m, llavors el residu de dividir a entre m és igual al residu de dividir c entre m.

127

1) En primer lloc, hem de provar que $\mathrm{mcd}(4096, 2957) = 1$ i després hem d'escriure la identitat de Bézout (de fet, només necessitem el coeficient de 2957).

0	1	−1	3	−4	7	−18	169	−187
	1	2	1	1	2	9	1	21
4096	2957	1139	679	460	219	22	21	1
1139	679	460	219	22	21	1	0	

   Per tant, $\mathrm{mcd}(4096, 2957) = 1$ i $\overline{2957}$ té invers a $\mathbb{Z}_{4096}$. A més, sabem que existeix un enter x tal que:

$$4096x + 2957 \cdot (-187) = 1$$

   És a dir $\overline{2957}^{-1} = \overline{-187} = \overline{3909}$.

2) **Solució 1.** Hem de comprovar que $f \circ g = I$ i $g \circ f = I$, on I és l'aplicació identitat de $\mathbb{Z}_{4096}$, és a dir I està definida per $I(\overline{x}) = \overline{x}$.

$$\begin{aligned}(f \circ g)(\overline{x}) &= f(g(\overline{x})) = f(\overline{3909} \cdot \overline{x}) \\ &= \overline{2957} \cdot (\overline{3909} \cdot \overline{x}) = (\overline{2957} \cdot \overline{3909}) \cdot \overline{x} \\ &= \overline{1} \cdot \overline{x} = \overline{x} = I(\overline{x})\end{aligned}$$

perquè a l'apartat anterior hem provat que la classe inversa de $\overline{2957}$ és $\overline{3909}$. Això demostra que $f \circ g = I$. Anàlogament es demostra l'altra propietat:

$$\begin{aligned}(g \circ f)(\overline{x}) &= g(f(\overline{x})) = g(\overline{2957} \cdot \overline{x}) \\ &= \overline{3909} \cdot (\overline{2957} \cdot \overline{x}) = (\overline{3909} \cdot \overline{2957}) \cdot \overline{x} \\ &= \overline{1} \cdot \overline{x} = \overline{x} = I(\overline{x})\end{aligned}$$

Solució 2. Una altra manera de demostrar el que demanen és trobar l'aplicació inversa de f i comprovar que és g. Per trobar l'inversa de f, aïllem la $\overline{x}$ de l'equació $\overline{y} = \overline{2957} \cdot \overline{x}$. És a dir, multipliquem per la classe inversa a ambdós membres. Però, per l'apartat anterior $\overline{2957}^{-1} = \overline{3909}$. És a dir:

$$\overline{y} = \overline{2957} \cdot \overline{x} \Rightarrow \overline{x} = \overline{2957}^{-1} \cdot \overline{y} \Rightarrow \overline{y} = \overline{3909} \cdot \overline{x}$$

Per tant, hem comprovat que l'aplicació inversa de f és g. I com l'aplicació inversa de l'aplicació inversa de f és f, hem provat que les dues aplicacions són mútuament inverses una de l'altra.

128

1) Sigui $A(x)$ el predicat "x és múltiple de 30" i sigui $B(x)$ el predicat "x és múltiple de 6 i acaba en 0". Llavors que $B(x)$ sigui una condició suficient per a $A(x)$ vol dir que $\forall x(B(x) \Rightarrow A(x))$ i que sigui necessària significa que $\forall x(A(x) \Rightarrow B(x))$.

   Provem que és suficient. Si x és un enter múltiple de 6 i que acaba en 0, llavors és múltiple de 6 i múltiple de 10. Per tant, és múltiple del mínim comú múltiple de 6 i 10, que és 30.

   Provem ara que és una condició necessària. Sigui x un enter múltiple de 30. Llavors x és múltiple de 6 i múltiple de 10 (perquè 30 és múltiple de 6 i de 10). Per tant, x és múltiple de 6 i acaba en 0.

2) Si $\operatorname{mcd}(a, m) = 2$, llavors, per la identitat de Bézout, existeixen enters x i y tals que $ax + my = 2$. Considerant aquesta igualtat mòdul m obtenim que $ax \equiv 2 \pmod{m}$.

129

1) S és reflexiva. Per definició de S, $x\,S\,x \Leftrightarrow x\,R\,x \wedge x\,R\,x$; però $x\,R\,x$ és cert perquè R és reflexiva.

   S és simètrica. Suposem que $x\,S\,y$; és a dir, $x\,R\,y \wedge y\,R\,x$. Com que la conjunció de proposicions és commutativa, deduïm que $y\,R\,x \wedge x\,R\,y$. És a dir, $y\,S\,x$.

   S és transitiva. Suposem que $x\,S\,y$ i $y\,S\,z$. Llavors tenim que $x\,R\,y \wedge y\,R\,x$ i $y\,R\,z \wedge z\,R\,y$. Com que R és transitiva i sabem que $x\,R\,y$ i $y\,R\,z$, deduïm que $x\,R\,z$. D'altra banda, també de la transitivitat de R i de que sabem que $y\,R\,x$ i $z\,R\,y$, deduïm que $z\,R\,x$. Per tant, tenim que $x\,R\,z$ i $z\,R\,x$. És a dir, $x\,S\,z$.

2) R és reflexiva. Per definició de R, $X\,R\,X \Leftrightarrow d(O,X) \leq d(O,X)$, i $d(O,X) \leq d(O,X)$ és cert.

   R és transitiva. Suposem que $X\,R\,Y$ i $Y\,R\,Z$. És a dir, $d(O,X) \leq d(O,Y)$ i $d(O,Y) \leq d(O,Z)$. Per la transitivitat de la relació d'ordre $\leq$ deduïm que $d(O,X) \leq d(O,Z)$, és a dir $X\,R\,Z$.

   Si apliquem l'apartat anterior, tenim que la corresponent relació S és d'equivalència. Però $X\,S\,Y \Leftrightarrow d(O,X) \leq d(O,Y) \wedge d(O,Y) \leq d(O,X) \Leftrightarrow d(O,X) = d(O,Y)$. És a dir, dos punts estan relacionats si, i només si, estan a la mateixa distància del punt O. És a dir, si, i només si, estan sobre la mateixa circumferència de centre O. Per tant, les classes d'equivalència són les circumferències del pla de centre O.

2.10 Exàmens de taller 2011–2012 Q2

130

1) Tenim que:

$$\begin{aligned} (p \wedge q) &\equiv \neg((\neg p) \vee (\neg q)) && (1) \\ &\equiv \neg(p \to (\neg q)) && (2) \end{aligned}$$

   (1): per la llei de la doble negació i les lleis de De Morgan; (2) perquè $(r \to s) \equiv ((\neg r) \vee s)$.

2) Siguin p la proposició 'ser múltiple de 24' i q la proposició 'ser múltiple de 6'. Que p sigui una condició suficient per a q vol dir que la proposició $p \to q$ és certa; que p sigui una condició necessària per a q vol dir que $q \to p$ és certa. Per a demostrar que p és una condició suficient per a q hauríem de provar que un enter múltiple de 24 ho és també de 6, i això és cert; per a demostrar que p és una condició necessària per a q, hauríem de provar que un enter múltiple de 6 també ho és de 24, cosa que no és certa; contraexemple: 12 és múltiple de 6, però no de 24. Per tant, p és una condició suficient per a q, però p no és no necessària per a q.

131

1) Tenim que:

$$\begin{aligned} (p \leftrightarrow q) &\equiv (p \to q) \wedge (q \to p) && (1) \\ &\equiv \neg(\neg(p \to q) \vee \neg(q \to p)) && (2) \\ &\equiv \neg((p \to q) \to (\neg(q \to p))) && (3) \end{aligned}$$

   (1): vist a classe; (2) per la llei de la doble negació i les lleis de De Morgan; (3) perquè $(r \to s) \equiv ((\neg r) \vee s)$.

2) Siguin p la proposició 'ser parell' i q la proposició 'ser múltiple de 3'. Que p sigui una condició suficient per a q vol dir que la proposició $p \to q$ és certa; que p sigui una condició necessària per a q vol dir que $q \to p$ és certa. Per a demostrar que p és una condició suficient per a q hauríem de provar que tot enter parell és un múltiple de 3; per a demostrar que p és una condició necessària per a q, hauríem de provar que tot enter múltiple de 3 és parell. Cap de les dues afirmacions és certa i per a provar-ho hem de trobar en cada cas un contraexemple; és a dir, un enter que sigui parell, però no múltiple de 3 i un enter que sigui múltiple de 3 però no parell: per exemple, el 4 i el 9, respectivament. Per tant, p no és una condició ni suficient ni necessària per a q.

132

1) Tenim que:

$$\begin{aligned}(p \to (q \vee r)) &\equiv (p \to ((\neg(\neg q)) \vee r) && (1)\\ &\equiv (p \to ((\neg q) \to r)) && (2)\end{aligned}$$

(1): per la llei de la doble negació; (2) perquè $(a \to b) \equiv ((\neg a) \vee b)$.

2) Siguin p la proposició 'ser parell' i q la proposició 'ser múltiple de 6'. Que p sigui una condició suficient per a q vol dir que la proposició $p \to q$ és certa; que p sigui una condició necessària per a q vol dir que $q \to p$ és certa. Per a demostrar que p és una condició suficient per a q hauríem de provar que tot enter parell és un múltiple de 6, i això és cert, com es demostra més endavant; per a demostrar que p és una condició necessària per a q, hauríem de provar que tot enter múltiple de 6 és parell, i això és fals; contraexemple: 4. Provem que $q \to p$ és certa; hem de provar que *tot* enter múltiple de 6 és parell. Però si n és un múltiple de 6, llavors n es pot escriure com $n = 6k$, per a algun enter k; és a dir, $n = 2(3k)$, que és parell. Per tant, p no és una condició suficient per a q, però sí és una condició necessària per a q.

133

1) Tenim que:

$$\begin{aligned}((p \vee q) \to r) &\equiv ((\neg(\neg p) \vee q) \to r) && (1)\\ &\equiv (((\neg p) \to q) \to r) && (2)\end{aligned}$$

(1): per la llei de la doble negació; (2) perquè $(a \to b) \equiv ((\neg a) \vee b)$.

2) Siguin p la proposició 'acabar en 00' i q la proposició 'ser múltiple de 50'. Que p sigui una condició suficient per a q vol dir que la proposició $p \to q$ és certa; que p sigui una condició necessària per a q vol dir que $q \to p$ és certa. Per a demostrar que p és una condició suficient per a q hauríem de provar que tot enter que acabi en 00 és un múltiple de 50; per a demostrar que p és una condició necessària per a q, hauríem de provar que tot enter múltiple de 50 acaba en 00. La primera afirmació és certa i la segona és falsa. Per a provar que $p \to q$ és certa, suposem que l'enter n acaba en 00; llavors n és múltiple de 100 i, per tant, també és múltiple de 50, perquè $100 = 2 \cdot 50$. Per a provar que $q \to p$ és falsa, només cal trobar un contraexemple: 50.

134

1) a) $\neg(\forall n(N(n) \to P(n)))$. b) $\forall n(N(n) \to \exists a, b(a^2 = n \wedge b^2 = n \wedge a \neq b))$

2) Siguin n i m nombres enters. Siguin p la proposició 'nm és parell' i α la proposició 'n és parell o m és parell'. Que p sigui una condició suficient per a α vol dir que la proposició $p \to \alpha$ és certa; que p sigui una condició necessària per a α vol dir que $\alpha \to p$ és certa. Per a demostrar que p és una condició suficient per a α, hauríem de provar que si nm és parell, llavors n és parell o m és parell; per a demostrar que p és una condició necessària per a α, hauríem de provar que si n és parell o m és parell, llavors nm és parell. Les dues afirmacions són certes. [Consulteu el problema 1.10.]

135

1) a) $\neg(\exists n(P(n) \wedge S(n)))$. b) $\exists n, m(P(n) \wedge P(m) \wedge n \neq m)$

2) Siguin n i m nombres enters. Siguin p la proposició 'nm és senar' i α la proposició 'n és senar i m és senar'. Que p sigui una condició suficient per a α vol dir que la proposició $p \to \alpha$ és certa; que p sigui una condició necessària per a α vol dir que $\alpha \to p$ és certa. Per a demostrar que p és una condició suficient per a α, hauríem de provar que si nm és senar, llavors n és senar i m és senar; per a demostrar que p és una condició necessària per a α, hauríem de provar que si n és senar i m és senar, llavors nm és senar. Les dues afirmacions són certes. [Consulteu el problema 1.10.]

136

1) a) $\neg(\exists n(P(n) \wedge S(n^2)))$. b) $\exists n, m(S(n) \wedge S(m) \wedge n \neq m)$

2) Siguin n i m nombres enters. Siguin p la proposició '$n = m$' i q la proposició '$n^2 + m = m^2 + n$'. Que p sigui una condició suficient per a q vol dir que la proposició $p \to q$ és certa; que p sigui una condició necessària per a q vol dir que $q \to p$ és certa. Per a demostrar que p és una condició suficient per a q, hauríem de provar que si $n = m$, llavors $n^2 + m = m^2 + n$; per a demostrar que p és una condició necessària per a q, hauríem de provar que si $n^2 + m = m^2 + n$, llavors $n = m$. La primera afirmació és òbviament certa. La segona afirmació és falsa i per a provar-ho, posem un contraexemple: $n = 1$ i $m = 0$.

137

1) No. Posem un contraexemple. $A = \{1, 2, 3\}$, $B = \{2, 4\}$, $C = \{2, 5\}$. Llavors $A - B = \{1, 3\} \subseteq A - C = \{1, 3\}$, però C no és un subconjunt de B.

2) No. Per exemple $A = B = \emptyset$. [No obstant, si suposem que A i B són subconjunts *no buits* de Ω i que $A^c \times B = A \times B^c$, llavors $A = B = \Omega$. Provem, per reducció a l'absurd, que $A = \Omega$. Suposem que $A \neq \Omega$. Llavors $A^c \neq \emptyset$. Per tant, hi ha un element $a' \in A^c$ i també un element $b \in B$ (per hipòtesi). Per tant, $(a', b) \in A^c \times B$. Però per hipòtesi aquest producte cartesià coincideix amb $A \times B^c$. Per tant, $(a', b) \in A \times B^c$. És a dir, $a' \in A^c \cap A$. Contradicció. Per tant $A = \Omega$ (i, per simetria, $B = \Omega$).]

138

1) Sí. Sigui $x \in A - (B \cup C)$. Llavors:

$$\begin{aligned} x \in A - (B \cup C) &\Rightarrow x \in A \wedge x \notin B \cup C \\ &\Rightarrow x \in A \wedge (x \notin B \wedge x \notin C) \\ &\Rightarrow (x \in A \wedge x \notin B) \wedge x \notin C \\ &\Rightarrow x \in A - B \wedge x \notin C \\ &\Rightarrow x \in (A - B) - C \end{aligned}$$

2) No. Posem un exemple: si $B = \{b\}$ i $A = \{(1, b), 1\}$, llavors $A \times B = \{((1, b), b), (1, b)\}$ i, per tant, $A \cap (A \times B) = \{(1, b)\}$. Podem prendre $C = \{(1, b)\}$.

139

1) Sí. Només hem de demostrar que $B^c \subseteq A$. Sigui $x \in B^c$. Llavors $x \notin B$ i com que $\Omega = A \cup B$, deduïm que $x \in A$.

2) No. Posem un exemple: si $A = \{a\}$ i $B = \emptyset$, llavors $A \times B = \emptyset$, $\mathcal{P}(A) = \{\emptyset, A\}$, $\mathcal{P}(B) = \{\emptyset\}$, $\mathcal{P}(A \times B) = \mathcal{P}(\emptyset) = \{\emptyset\}$, $\mathcal{P}(A) \times \mathcal{P}(B) = \{(\emptyset, \emptyset), (A, \emptyset)\}$.

140

1) No. Posem un exemple: si $\Omega = \{1, 2, 3, 4\}$, $A = \{1, 2, 4\}$, $B = \{2, 3\}$, $C = \{3, 4\}$, llavors $B \cap C = \{3\}$, $(B \cap C)^c = \{1, 2, 4\} = A$, $A - B = \{1, 4\}$.

2) No. Per exemple, $A = \{1, 2\}$, $B = \{1, 3\}$. Llavors $A \nsubseteq B$ i $B \nsubseteq A$, però no és cert que $A \nsubseteq A$.

141

1) Sí. Sigui $x \in \Omega$. Tenim:

$$\begin{aligned} x \in (A \cup B)^c \cap C &\Leftrightarrow x \notin A \cup B \wedge x \in C \\ &\Leftrightarrow (x \notin A \wedge x \notin B) \wedge x \in C \\ &\Leftrightarrow x \notin B \wedge x \in C \wedge x \notin A \\ &\Leftrightarrow x \in B^c \wedge (x \in C \wedge x \notin A) \\ &\Leftrightarrow x \in B^c \cap (C - A) \end{aligned}$$

2) No. Per exemple, $1R4$ i $4R8$, però 1 no està relacionat amb 8.

142

1) No. Posem un exemple: $A = \{1, 2, 3, 4\}$, $B = \{1, 2, 3, 5\}$, $C = \{1, 3, 4\}$. Llavors tenim que: $B - C = \{2, 5\}$, $A - (B - C) = \{1, 3, 4\}$, $A - B = \{4\}$, $(A - B) - C = \emptyset$.

2) No. Per exemple, si $A = \emptyset$, $B = \{1\}$, llavors $\mathcal{P}(A) = \{\emptyset\}$, $\mathcal{P}(B) = \{\emptyset, B\}$, $\mathcal{P}(A) \times B = \{(\emptyset, 1)\}$, $A \times \mathcal{P}(B) = \emptyset$ i, com que aquests últims dos conjunts no són iguals, els conjunts de les seves parts tampoc ho són.

143 Sí. Ho demostrem per reducció a l'absurd. Suposem que $A \cap B \neq \emptyset$. Llavors existeix un element $x \in A \cap B$ i, per tant, $x \in A \cup B$. Per hipòtesi, $x \in (A \cap B^c) \cup (A^c \cap B)$. Ara $x \in A \cap B^c$, i per tant $x \notin B$, o $x \in A^c \cap B$, i per tant $x \notin A$. En qualsevol cas arribem a una contradicció. En conseqüència, $A \cap B = \emptyset$.

144

Cas inicial: $n = 1$**.**

$$f^{(1)}(x) = f(x) = 2x + 1 = 2^1 x + 2^1 - 1$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $f^{(n)}(x) = 2^n x + 2^n - 1$ (hipòtesi d'inducció). Volem demostrar:

$$f^{(n+1)}(x) = 2^{n+1} x + 2^{n+1} - 1$$

Tenim:

$$\begin{aligned}
f^{(n+1)}(x) &= f(f^{(n)}(x)) \\
&= f(2^n x + 2^n - 1) && \text{per hipòtesi d'inducció} \\
&= 2(2^n x + 2^n - 1) + 1 \\
&= 2^{n+1} x + 2^{n+1} - 2 + 1 \\
&= 2^{n+1} x + 2^{n+1} - 1
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

145

Cas inicial: $n = 3$**.**

$$\frac{1}{4} + \frac{1}{5} + \frac{1}{6} = \frac{37}{60} > \frac{3}{5}$$

Pas d'inducció: Fixem un enter $n \geq 3$ i suposem que $\sum_{k=n+1}^{2n} \frac{1}{k} > 3/5$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{k=n+2}^{2n+2} \frac{1}{k} > \frac{3}{5}$$

Tenim:

$$\begin{aligned}
\sum_{k=n+2}^{2n+2} \frac{1}{k} &= \left(\sum_{k=n+1}^{2n} \frac{1}{k}\right) + \frac{1}{2n+1} + \frac{1}{2n+2} - \frac{1}{n+1} \\
&> \frac{3}{5} + \left(\frac{1}{2n+1} - \frac{1}{2n+2}\right) \qquad \text{per hipòtesi d'inducció} \\
&> \frac{3}{5}
\end{aligned}$$

Aquesta última desigualtat és certa perquè l'expressió entre parèntesi és positiva.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 3$.

146

Cas inicial: $n = 1$.

$$f^{(1)}(x) = f(x) = \frac{x}{2} + 1 = \frac{x}{2^1} - \frac{1}{2^0} + 2$$

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que $f^{(n)}(x) = \frac{x}{2^n} - \frac{1}{2^{n-1}} + 2$ (hipòtesi d'inducció). Volem demostrar:

$$f^{(n+1)}(x) = \frac{x}{2^{n+1}} - \frac{1}{2^n} + 2$$

Tenim:

$$\begin{aligned}
f^{(n+1)}(x) &= f(f^{(n)}(x)) \\
&= f\left(\frac{x}{2^n} - \frac{1}{2^{n-1}} + 2\right) \qquad \text{per hipòtesi d'inducció} \\
&= \frac{1}{2}\left(\frac{x}{2^n} - \frac{1}{2^{n-1}} + 2\right) + 1 \\
&= \frac{x}{2^{n+1}} - \frac{1}{2^n} + 2
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

147

Cas inicial: $n = 2$.

$$\frac{1}{\sqrt{1}} + \frac{1}{\sqrt{2}} = 1.7\ldots > \sqrt{2} = 1.4\ldots$$

Pas d'inducció: Fixem un enter $n \geq 2$ i suposem que $\sum_{k=1}^{n} 1/\sqrt{k} > \sqrt{n}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{k=1}^{n+1} \frac{1}{\sqrt{k}} > \sqrt{n+1}$$

Tenim:

$$\begin{aligned}\sum_{k=1}^{n+1}\frac{1}{\sqrt{k}} &= \sum_{k=1}^{n}\frac{1}{\sqrt{k}}+\frac{1}{\sqrt{n+1}}\\ &> \sqrt{n}+\frac{1}{\sqrt{n+1}} \qquad \text{per hipòtesi d'inducció}\end{aligned}$$

Ara hem de demostrar que $\sqrt{n}+\frac{1}{\sqrt{n+1}} > \sqrt{n+1}$. Però aquesta desigualtat és equivalent a $\sqrt{n}\sqrt{n+1} > n$ (multiplicant els dos termes per $\sqrt{n+1}$, que és positiu, i després restant 1). Ara $\sqrt{n}\sqrt{n+1} = \sqrt{n^2+n} > \sqrt{n^2} = n$.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 2$.

148

Cas inicial: $n = 2$**.**

$$\frac{4^2}{2+1} = \frac{16}{3} < \frac{4!}{(2!)^2} = \frac{24}{4}$$

Pas d'inducció: Fixem un enter $n \geq 2$ i suposem que $\frac{4^n}{n+1} < \frac{(2n)!}{(n!)^2}$ (hipòtesi d'inducció). Volem demostrar:

$$\frac{4^{n+1}}{n+2} < \frac{(2n+2)!}{((n+1)!)^2}$$

D'una banda tenim:

$$\frac{4^{n+1}}{n+2} = \frac{4^n}{n+1}\cdot\frac{4(n+1)}{(n+2)} < \frac{(2n)!}{(n!)^2}\cdot\frac{4(n+1)}{(n+2)}$$

per hipòtesi d'inducció. D'altra banda tenim:

$$\frac{(2n+2)!}{((n+1)!)^2} = \frac{(2n)!}{(n!)^2}\cdot\frac{(2n+2)(2n+1)}{(n+1)(n+1)} = \frac{(2n)!}{(n!)^2}\cdot\frac{2(2n+1)}{n+1}$$

Per tant, és suficient demostrar que:

$$\frac{(2n)!}{(n!)^2}\cdot\frac{4(n+1)}{(n+2)} < \frac{(2n)!}{(n!)^2}\cdot\frac{2(2n+1)}{n+1}$$

Aquesta desigualtat és equivalent a $2n^2+4n+2 < 2n^2+5n+2$, que és certa (primer simplifiquem el quocient de factorials als dos membres i després multipliquem els dos membres per $(n+1)(n+2)$).

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 2$.

149

Cas inicial: $n = 3$.

$$1 + \frac{1}{3} + \frac{1}{7} = \frac{31}{21} < \frac{3}{2}$$

Pas d'inducció: Fixem un enter $n \geq 3$ i suposem que $\sum_{k=1}^{n} \frac{1}{2^k-1} < \frac{n}{2}$ (hipòtesi d'inducció). Volem demostrar:

$$\sum_{k=1}^{n+1} \frac{1}{2^k - 1} < \frac{n+1}{2}$$

Tenim:

$$\sum_{k=1}^{n+1} \frac{1}{2^k - 1} = \sum_{k=1}^{n} \frac{1}{2^k - 1} + \frac{1}{2^{n+1} - 1} < \frac{n}{2} + \frac{1}{2^{n+1} - 1} < \frac{n}{2} + \frac{1}{2} = \frac{n+1}{2}$$

Hem aplicat la hipòtesi d'inducció a la primera desigualtat; i si $n \geq 3$, llavors $1/(2^{n+1} - 1) \leq 1/15 < 1/2$.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 3$.

150

Cas inicial: $n = 2$.

$$\frac{1}{2!} = 1 - \frac{1}{2!}$$

Pas d'inducció: Fixem un enter $n \geq 2$ i suposem que $\sum_{k=2}^{n} \frac{k-1}{k!} = 1 - \frac{1}{n!}$ (hipòtesi d'inducció). Volem demostrar:

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

Tenim:

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

la segona igualtat, per hipòtesi d'inducció. Ara tenim:

$$1 - \frac{1}{n!} + \frac{n}{(n+1)!} = 1 - \frac{n+1}{(n+1)!} + \frac{n}{(n+1)!} = 1 - \frac{1}{(n+1)!}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 3$.

2.11 Examen parcial 26/04/2012

152

1) Es defineix el complementari de A respecte de Ω com $A^c = \{x \in \Omega : x \notin A\}$. Tenim:

$$\begin{aligned} A \subseteq B &\Leftrightarrow \forall x(x \in A \to x \in B) \\ &\Leftrightarrow \forall x(x \notin B \to x \notin A) \qquad (1) \\ &\Leftrightarrow \forall x(x \in B^c \to A^c) \\ &\Leftrightarrow B^c \subseteq A^c \end{aligned}$$

(1): hem aplicat que les proposicions $p \to q$ i $(\neg q) \to (\neg p)$ són equivalents.

2) Siguin A, B conjunts i $f : A \to B$ una aplicació. Si $A_1 \subseteq A$, llavors es defineix $f[A_1]$ com el subconjunt de B format per totes les imatges dels elements de A_1. És a dir: $f[A_1] = \{f(a) : a \in A_1\} \subseteq B$. Tenim:

$$\begin{aligned} b \in f[A_1 \cap A_2] &\Rightarrow \exists a(a \in A_1 \cap A_2 \wedge f(a) = b) \\ &\Rightarrow \exists a(a \in A_1 \wedge a \in A_2 \wedge b = f(a)) \\ &\Rightarrow \exists a(a \in A_1 \wedge b = f(a)) \wedge \exists a(a \in A_2 \wedge b = f(a)) \\ &\Rightarrow b \in f[A_1] \wedge b \in f[A_2] \\ &\Rightarrow b \in f[A_1] \cap f[A_2] \end{aligned}$$

153

1) Suposem que $0 < x < y$. Llavors tenim:

$$\begin{aligned} x < y \Rightarrow 2x = x + x < x + y < y + y = 2y \Rightarrow x < \frac{x+y}{2} < y \\ 0 < x < y \Rightarrow x^2 = x \cdot x < x \cdot y < y \cdot y = y^2 \Rightarrow x < \sqrt{xy} < y \quad (1) \end{aligned}$$

(1): hem aplicat que tant x com y són positius i que l'arrel quadrada és una funció estrictament creixent.

2) Suposem que $m = (x+y)/2 = x$. Llavors $2x = x + y$, d'on $x = y$. Anàlogament si $m = (x+y)/2 = y$. Suposem ara que $m = \sqrt{xy} = x$. Llavors $x^2 = xy$ i, per tant, $x = y$ (ja que $x > 0$). Anàlogament si $m = \sqrt{xy} = y$.

3) Demostrem la forma contra-recíproca; és a dir, si $\sqrt{xy} \geq (x+y)/2$, llavors $x = y$. Suposem que $\sqrt{xy} \geq (x+y)/2$. Llavors, com que es tracta de nombres positius, elevant al quadrat els dos membres obtenim $xy \geq (x+y)^2/4$. És a dir, $4xy \geq x^2 + 2xy + y^2$. D'aquí se segueix que: $x^2 - 2xy + y^2 = (x-y)^2 \leq 0$ i, com que un quadrant sempre és positiu o zero, deduïm que $(x-y)^2 = 0$; és a dir, $x = y$.

154

1) *Reflexiva*: per a tot $x \in A$, xRx, ja que $f(x) = f(x)$. *Simètrica*: si xRx', llavors $f(x) = f(x')$ i, per tant, $x'Rx$. *Transitiva*: si xRx' i $x'Rx''$, llavors $f(x) = f(x') = f(x'')$, d'on xRx''.

2) A cada classe d'equivalència tots els elements tenen la mateixa imatge per la funció part entera, i aquesta imatge és un nombre enter (comú per a tots els elements de la classe). La funció part entera pren tots els valors enters i només aquests. Per tant, cada nombre enter k determina una única classe d'equivalència; si $x \in \mathbb{R}$ i $\lfloor x \rfloor = k$, llavors:

$$[x]_R = \{x' \in \mathbb{R} : \lfloor x' \rfloor = \lfloor x \rfloor\} = [k, k+1)$$

(interval tancat per l'esquerra, obert per la dreta). És a dir, hi ha una classe per a cada nombre enter k formada pels nombres reals que tenen part entera igual a k.

Podem definir doncs l'aplicació $g : \mathbb{R}/R \to \mathbb{Z}$

$$g([x]_R) = \lfloor x \rfloor$$

Dir d'una altra manera, si la classe $[x]_R$ és l'interval $[k, k+1)$, amb $k \in \mathbb{Z}$, llavors $g([x]_R) = k$. Per les consideracions que hem fet abans, està clar que aquesta aplicació és una bijecció.

2.12 Examen final 07/06/2012

156

1) Només ens cal trobar un contraexemple; és a dir, un nombre enter m i dues classes $\overline{a}, \overline{b} \in \mathbb{Z}_m$ tals que $\overline{a}^2 = \overline{b}^2$, però $\overline{a} \neq \overline{b}$ i $\overline{a} \neq -\overline{b}$. Com que a l'apartat següent es demana demostrar que la propietat és certa si m és un nombre primer, busquem un contraexemple amb m no primer. Per exemple, si prenem $m = 4$, $\overline{a} = \overline{2}$ i $\overline{b} = \overline{0}$, tenim que $\overline{2}^2 = \overline{0}^2 = \overline{0}$. Però $\overline{2} \neq \overline{0} = -\overline{0}$.

2) Sigui m un nombre primer i $a, b \in \mathbb{Z}$ tals que $\overline{a}^2 = \overline{b}^2$. Llavors $\overline{a}^2 - \overline{b}^2 = (\overline{a} - \overline{b})(\overline{a} + \overline{b}) = \overline{0}$; com que $\mathbb{Z}_m$ és un cos (perquè m és primer), deduïm que $\overline{a} = \overline{b}$ o $\overline{a} = -\overline{b}$. També ho podem deduir utilitzant el llenguatge de congruències com segueix: si $(\overline{a} - \overline{b})(\overline{a} + \overline{b}) = \overline{0}$, llavors tenim que $p \mid (a - b)(a + b)$ i pel lema de Gauss deduïm que $p \mid (a - b)$, i per tant $\overline{a} = \overline{b}$, o bé $p \mid (a + b)$, i per tant $\overline{a} = -\overline{b}$.

157

1) Ho demostrem per inducció. Cas inicial: $n = 1$. El que s'ha de demostrar, $f \circ g = g \circ f$, és cert, per hipòtesi. Pas d'inducció: fixem un enter $n \geq 1$ i suposem que $f^n \circ g = g \circ f^n$.

Llavors:

$$\begin{aligned}
f^{n+1}\circ g &= (f\circ f^n)\circ g && (1)\\
&= f\circ(f^n\circ g) && (2)\\
&= f\circ(g\circ f^n) && (3)\\
&= (f\circ g)\circ f^n && (2)\\
&= (g\circ f)\circ f^n && (4)\\
&= g\circ(f\circ f^n) && (2)\\
&= g\circ f^{n+1} && (1)
\end{aligned}$$

(1): per definició de f^{n+1}; (2): per la propietat associativa de la composició; (3): per hipòtesi d'inducció; (4): per hipòtesi del problema.

Per tant, la propietat és certa per a tot $n \geq 1$.

2) Ho demostrem per inducció. Cas inicial: $n = 1$: $(g\circ f)^1 = g\circ f = g^1\circ f^1$. Pas d'inducció: fixem un enter $n \geq 1$ i suposem que $(g\circ f)^n = g^n\circ f^n$. Llavors:

$$\begin{aligned}
(g\circ f)^{n+1} &= (g\circ f)^n\circ(g\circ f) && (1)\\
&= (g^n\circ f^n)\circ(g\circ f) && (2)\\
&= g^n\circ(f^n\circ g)\circ f && (3)\\
&= g^n\circ(g\circ f^n)\circ f && (4)\\
&= (g^n\circ g)\circ(f^n\circ f) && (3)\\
&= g^{n+1}\circ f^{n+1} && (5)
\end{aligned}$$

(1): per definició de $(g\circ f)^{n+1}$; (2): per hipòtesi d'inducció; (3): per la propietat associativa de la composició; (4): per l'apartat 1; (5) per definició de g^{n+1} i de f^{n+1}.

Per tant, la propietat és certa per a tot $n \geq 1$.

158

1)
- T és reflexiva: sigui $x \in A$; com que R i S són reflexives, tenim que xRx i xSx. Per tant, xTx.
- T és simètrica: siguin $x, y \in A$ i suposem que xTy. Llavors, xRy i xSy. Com que R i S són simètriques, tenim que yRx i ySx. Per tant, yTx.
- T és transitiva: siguin $x, y, z \in A$ i suposem que xTy i yTz. Llavors tenim que xRy, xSy, yRz i yTz. Com que R i S són transitives, deduïm que xRz i xSz.

2) Hi ha diverses respostes possibles i per a algunes U serà d'equivalència i per d'altres no.

- Sigui R la relació d'igualtat: $xRy \Leftrightarrow x = y$, que òbviament és una relació d'equivalència. Sigui S la relació total (és a dir, dos elements qualssevol estan relacionats). Llavors la relació U coincideix amb la relació S i, per tant, és d'equivalència.

- Sigui R la relació: $xRy \Leftrightarrow x \equiv y \pmod 2$ (x, y tenen la mateixa paritat). Ja sabem que R és una relació d'equivalència. Sigui S la relació donada per la partició de X: $\{A, B\}$, on $A = \{1, 2, 3, 4, 5\}$, $B = \{6, 7, 8, 9, 10\}$ (dos elements estan relacionats si estan al mateix conjunt d'aquesta partició). Llavors la relació U es descriu així: xUy si, i només si, x i y tenen la mateixa paritat o $x, y \in A$ o $x, y \in B$. Llavors U no és una relació transitiva. Per exemple, $2U6$ i $6U9$, però el 2 i el 9 no estan relacionats per U.

2.13 Exàmens de taller 2012–2013 Q1

2.14 Examen parcial 15/11/2012

178

1) Si $A \subseteq \Omega$, llavors el complementari de A respecte de Ω, denotat per A^c, és el conjunt format pels elements de Ω que no pertanyen a A. És a dir:

$$A^c = \{x \in \Omega : x \notin A\}$$

Les lleis de De Morgan per a conjunts són:

$$(A \cup B)^c = A^c \cap B^c, \qquad (A \cap B)^c = A^c \cup B^c,$$

on $A, B \subseteq \Omega$. Provem la primera: sigui $x \in \Omega$; llavors:

$$\begin{aligned} x \in (A \cup B)^c &\Leftrightarrow x \notin A \cup B \\ &\Leftrightarrow \neg(x \in A \cup B) \\ &\Leftrightarrow \neg(x \in A \vee x \in B) && (1) \\ &\Leftrightarrow x \notin A \wedge x \notin B \\ &\Leftrightarrow x \in A^c \wedge x \in B^c \\ &\Leftrightarrow x \in A^c \cap B^c \end{aligned}$$

(1): per la corresponent llei de De Morgan del càlcul proposicional. Provem la segona: sigui $x \in \Omega$; llavors:

$$\begin{aligned} x \in (A \cap B)^c &\Leftrightarrow x \notin A \cap B \\ &\Leftrightarrow \neg(x \in A \cap B) \\ &\Leftrightarrow \neg(x \in A \wedge x \in B) && (2) \\ &\Leftrightarrow x \notin A \vee x \notin B \\ &\Leftrightarrow x \in A^c \vee x \in B^c \\ &\Leftrightarrow x \in A^c \cup B^c \end{aligned}$$

(2): per la corresponent llei de De Morgan del càlcul proposicional.

2) El mètode de demostració per reducció a l'absurd és un mètode de demostració indirecte que consisteix en demostrar una proposició provant que la seva negació porta a contradicció; és a dir, a partir de la seva negació arribem a provar que una proposició r i la seva negació $\neg r$ són certes a la vegada. Pel principi de la no contradicció, una proposició i la seva negació no poden ser certes al mateix temps.

   Provem que $\sqrt{2} \notin \mathbb{Q}$. Suposem que $\sqrt{2} \in \mathbb{Q}$. Posem $\sqrt{2} = \frac{a}{b}$, amb a i b enters i $b \neq 0$. Suposem, a més, que la fracció és irreductible; és a dir, $\mathrm{mcd}(a, b) = 1$ (a i b no tenen factors en comú). Ara tenim:

$$\sqrt{2} = \frac{a}{b} \Rightarrow \frac{a^2}{b^2} = 2 \Rightarrow a^2 = 2b^2 \Rightarrow a^2 \text{ parell}$$

   Però si a^2 és parell, llavors a és parell (prova: demostrem la forma contrarrecíproca: si a és senar, llavors a^2 és senar. Si $a = 2k + 1$, llavors $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, que és senar.) Per tant, podem escriure $a = 2m$ i per tant $a^2 = 4m^2$. Ara:

$$a^2 = 4m^2 = 2b^2 \Rightarrow b^2 = 2m^2 \Rightarrow b^2 \text{ parell}$$

   Per tant, igual que abans, deduïm que b és parell. Ara tenim per un costat que la fracció a/b és irreductible i per l'altre que a i b són parells. Contradicció.

   Per tant, $\sqrt{2}$ és un nombre irracional.

179

1) Dues proposicions són equivalents si, prenguin el valor de veritat que prenguin les lletres proposicionals de que consten, les dues proposicions sempre tenen el mateix valor de veritat. Per tant, fem la taula de veritat d'aquestes proposicions i comprovem que les columnes corresponents (la 5 i la 7) coincideixen.

p	q	r	$q \to r$	$p \to (q \to r)$	$p \wedge q$	$(p \wedge q) \to r$
0	0	0	1	1	0	1
0	0	1	1	1	0	1
0	1	0	0	1	0	1
0	1	1	1	1	0	1
1	0	0	1	1	0	1
1	0	1	1	1	0	1
1	1	0	0	0	1	0
1	1	1	1	1	1	1

   Una altra solució: tenint en compte l'equivalència $a \to b \equiv (\neg a) \vee b$, la llei de de Morgan $\neg(a \wedge b) \equiv (\neg a) \vee (\neg b)$ i l'associativitat de la disjunció, obtenim:

$$\begin{aligned} p \to (q \to r) &\equiv (\neg p) \vee (q \to r) \equiv (\neg p) \vee ((\neg q) \vee r) \\ &\equiv ((\neg p) \vee (\neg q)) \vee r \\ &\equiv (\neg(p \wedge q)) \vee r \\ &\equiv (p \wedge p) \to r \end{aligned}$$

2) Una solució, sense utilitzar elements:

$$\begin{aligned}
(A^c \cup (B^c \cap C))^c &= A^{cc} \cap (B^c \cap C)^c && (1)\\
&= A \cap (B^{cc} \cup C^c) && (2)\\
&= A \cap (B \cup C^c) && (3)\\
&= (A \cap B) \cup (A \cap C^c) && (4)\\
&= (A \cap B) \cup (A - C)
\end{aligned}$$

(1): llei de de Morgan; (2): llei de de Morgan i la propietat del doble complementari, $A^{cc} = A$; (3): propietat del doble complementari, $B^{cc} = B$; (4): propietat distributiva de l'intersecció respecte de la unió.

Una altra solució: prenem un element arbitrari $x \in \Omega$. Llavors tenim:

$$\begin{aligned}
x \in (A^c \cup (B^c \cap C))^c &\Leftrightarrow x \notin A^c \cup (B^c \cap C) && (1)\\
&\Leftrightarrow \neg(x \in A^c \cup (B^c \cap C))\\
&\Leftrightarrow \neg(x \notin A \vee x \in B^c \cap C) && (1), (2)\\
&\Leftrightarrow x \in A \wedge x \notin B^c \cap C && (3)\\
&\Leftrightarrow x \in A \wedge \neg(x \in B^c \cap C)\\
&\Leftrightarrow x \in A \wedge \neg(x \notin B \wedge x \in C) && (1), (2)\\
&\Leftrightarrow x \in A \wedge (x \in B \vee x \notin C) && (3)\\
&\Leftrightarrow (x \in A \wedge x \in B) \vee (x \in A \wedge x \notin C) && (4)\\
&\Leftrightarrow x \in A \cap B \vee x \in A - C && (2), (5)\\
&\Leftrightarrow x \in (A \cap B) \cup (A - C) && (4)
\end{aligned}$$

(1): per definició de complementari; (2): definició d'intersecció; (3): per la llei de De Morgan del càlcul de proposicions; (4): propietat distributiva de la intersecció respecte de la unió; (5) definició de diferència de conjunts.

Per tant, tenim la propietat que volíem demostrar.

3) Les dues propietats són certes. La primera diu que donat un enter x qualsevol, podem trobar un enter y tal que $xy = 0$. Efectivament, $y = 0$: donat x, llavors $x \cdot 0 = 0$. La segona propietat diu que hi ha un enter y que compleix $xy = x$, per a qualsevol enter x. Efectivament, $y = 1$: $x \cdot 1 = x$, per a qualsevol enter x.

180

1) Hem de provar que R és una relació reflexiva, simètrica i transitiva.

Reflexiva: sigui $(x, y) \in P$. Llavors $x = x$. Per tant, $(x, y)R(x, y)$.

Simètrica: siguin $(x, y), (x', y') \in P$. Llavors tenim:

$$(x, y)R(x', y') \Rightarrow x = x' \Rightarrow x' = x \Rightarrow (x', y')R(x, y)$$

Transitiva: siguin $(x, y), (x', y'), (x'', y'') \in P$. Llavors tenim:

$$(x, y)R(x', y') \wedge (x', y')R(x'', y'') \Rightarrow x = x' \wedge x' = x'' \Rightarrow x = x'' \Rightarrow (x', y')R(x'', y'')$$

2) Sigui $(a, b) \in P$. La seva classe d'equivalència està formada pels punts (x, y) del pla tals que $x = a$:

$$[(a, b)] = \{(x, y) \in P : (x, y)R(a, b)\} = \{(x, y) \in P : x = a\}$$

és a dir, la classe d'equivalència del punt (a, b) és la recta vertical d'equació $x = a$.

3) El conjunt quocient P/R és, per definició, el conjunt de les classes d'equivalència:

$$P/R = \{[(a, b)] : (a, b) \in P\}$$

és adir, el conjunt quocient és el conjunt que té per elements les rectes verticals del pla.

2.15 Examen final 14/01/2013

182

1) Cas inicial: $n = 1$. Tenim: $1 + 2^{3-1} + 2^{3+1} = 1 + 2^2 + 2^4 = 21 \equiv 0 \pmod 7$.

2) Pas d'inducció: fixem un enter $m \geq 1$ i suposem que $1 + 2^{3m-1} + 2^{3m+1} \equiv 0 \pmod 7$ (hipòtesi d'inducció). Hem de provar que $1 + 2^{3(m+1)-1} + 2^{3(m+1)+1} \equiv 0 \pmod 7$. Tenim:

$$\begin{aligned} 1 + 2^{3(m+1)-1} + 2^{3(m+1)+1} &= 1 + 2^{3m+2} + 2^{3m+4} \\ &= 1 + 2^3 \cdot 2^{3m-1} + 2^3 \cdot 2^{3m+1} \\ &\equiv 1 + 2^{3m-1} + 2^{3m+1} \pmod 7, \quad \text{ja que } 2^3 = 8 \equiv 1 \\ &\equiv 0 \pmod 7, \quad \text{per H.I.} \end{aligned}$$

183

1) Siguin $a, b \in \mathbb{Z}$. Sabem que $5 \mid 15$ i, per hipòtesi, $15 \mid ab$; a més, la relació de divisibilitat és transitiva. Per tant, $5 \mid ab$. Com que 5 és un nombre primer, podem aplicar el lema d'Euclides: si $5 \mid ab$, llavors $5 \mid a$ o $5 \mid b$.

2) Siguin p, q, r lletres proposicionals. Que la proposició $t = ((p \to q) \wedge (\neg p \to q)) \to (r \to q)$ sigui una tautologia vol dir que és certa sempre; és a dir, per a qualsevol valor de veritat que prenguin p, q i r. Podem fer, doncs, la taula de veritat i comprovar que la columna corresponent té sempre el valor 1 (cert).

p	q	r	$p \to q$	$\neg p \to q$	$(p \to q) \wedge (\neg p \to q)$	$r \to q$	t
0	0	0	1	0	0	1	1
0	0	1	1	0	0	0	1
0	1	0	1	1	1	1	1
0	1	1	1	1	1	1	1
1	0	0	0	1	0	1	1
1	0	1	0	1	0	0	1
1	1	0	1	1	1	1	1
1	1	1	1	1	1	1	1

Una altra solució: tenim les equivalències següents:

$$\begin{aligned}
(p \to q) \wedge (\neg p \to q) &\equiv (\neg p \vee q) \wedge (p \vee q) && (1)\\
&\equiv (\neg p \wedge p) \vee q && (2)\\
&\equiv 0 \vee q && (3)\\
&\equiv q && (4)
\end{aligned}$$

(1): hem usat que $a \to b \equiv \neg a \vee b$; (2): per la propietat distributiva de la disjunció respecte de la conjunció; (3): pel principi de no contradicció: $\neg p \wedge p$ és una contradicció (és a dir, sempre falsa); (4): 0 denota una proposició falsa.

Finalment, tenim:

$$\begin{aligned}
((p \to q) \wedge (\neg p \to q)) \to (r \to q) &\equiv q \to (r \to q) && (1)\\
&\equiv \neg q \vee (\neg r \vee q) && (2)\\
&\equiv (\neg q \vee q) \vee \neg r && (3)\\
&\equiv 1 \vee \neg r && (4)\\
&\equiv 1
\end{aligned}$$

(1): pel que acabem de veure més a dalt; (2): propietats commutativa i associativa de la disjunció; (3): pel principi del terç exclòs $\neg q \vee q$ és una tautologia; (4): 1 denota una tautologia.

184

1) Apliquem l'algorisme d'Euclides estès:

X	1	0	1	-2
Y	0	1	-2	5
Q		2	2	10
R	52	21	10	1
	10	1	0	

on la fila Q conté els quocients de les divisions; la fila R conté els residus; i les entrades de la fila X es calculen aplicant la recurrència: $x_{k+1} = x_{k-1} - x_k q_k$ (i anàlogament per la fila Y).

Per tant, $\text{mcd}(52, 21) = 1$ i l'identitat de Bézout és:

$$52 \cdot (-2) + 21 \cdot 5 = 1$$

2) Hem de provar que per a tot enter n, existeixen enters x, y tals que $f(x, y) = n$. És a dir, per a tot $n \in \mathbb{Z}$, existeixen $x, y \in \mathbb{Z}$ tals que $52x + 21y = n$.

Però per l'apartat anterior, sabem que $52 \cdot (-2) + 21 \cdot 5 = 1$. Si multipliquem aquesta igualtat per n, obtenim:

$$52 \cdot (-2n) + 21 \cdot (5n) = n$$

Per tant, donat un enter n, tenim que $f(-2n, 5n) = n$. És a dir, f és exhaustiva.

2.16 Examen parcial 2/5/2013

205

1) f és injectiva: siguin $x, x' \in \mathbb{R} - \{7\}$. Llavors:

$$\begin{aligned} f(x) = f(x') &\Rightarrow \frac{5x}{x-7} = \frac{5x'}{x'-7} \\ &\Rightarrow 5x(x'-7) = 5x'(x-7) \\ &\Rightarrow xx' - 7x = x'x - 7x' \\ &\Rightarrow -7x = -7x' \\ &\Rightarrow x = x' \end{aligned}$$

f és exhaustiva: sigui $y \in \mathbb{R} - \{5\}$. Volem veure que existeix una $x \in \mathbb{R} - \{7\}$ tal que $f(x) = y$. Plantegem l'equació $f(x) = y$, considerant la y com a un paràmetre i estudiem si té solució en la x. Aïllant la x trobem que:

$$x = \frac{7y}{y-5} \in \mathbb{R}$$

Aquesta expressió és un nombre real, ja que $y \neq 5$. D'altra banda, aquesta x no pot ser igual a 7, ja que si $7y/(y-5) = 7$, llavors $y = y - 5$, que és absurd.

Així, f és injectiva i exhaustiva. Per tant, f és bijectiva. L'expressió anterior ens dóna la fórmula de la funció inversa:

$$f^{-1}(x) = \frac{7x}{x-5}$$

2) Suposem que $(x, y)R(x', y')$ i $(x', y')R(x'', y'')$. És a dir, $x+y' = x'+y$ i $x'+y'' = x''+y'$. Volem demostrar que $(x, y)R(x'', y'')$. Si sumem les dues igualtats anteriors terme a terme, obtenim:

$$x + y' + x' + y'' = x' + y + x'' + y'$$

i, restant $y' + x'$ a cada terme, obtenim finalment: $x + y'' = x'' + y$. És a dir, $(x, y)R(x'', y'')$.

206 Es tracta de demostrar que tres proposicions són equivalents. Demostrarem que $1 \Rightarrow 2$, $2 \Rightarrow 3$ i $3 \Rightarrow 1$.

$1 \Rightarrow 2$) Hipòtesi: $[a] \cap [b] \neq \emptyset$. Volem demostrar: $a \in [b]$.

Per hipòtesi, existeix un element $x \in [a] \cap [b]$. Per definició de classe d'equivalència, tenim que xRa i xRb. Per la propietat simètrica, si xRa, llavors aRx. Per la propietat transitiva, si aRx i xRb, llavors aRb. Per tant, $a \in [b]$.

$2 \Rightarrow 3$) Hipòtesi: $a \in [b]$. Volem demostrar: $[a] \subseteq [b]$. És a dir, hem de veure que, per a tot x, si $x \in [a]$, llavors $x \in [b]$.

Sigui $x \in [a]$. Per definició de classe d'equivalència, xRa. Però, per hipòtesi, $a \in [b]$; és a dir, aRb. Per la propietat transitiva, si xRa i aRb, llavors xRb. Per tant, $x \in [b]$.

$3 \Rightarrow 1$) Hipòtesi: $a \subseteq [b]$. Volem demostrar: $[a] \cap [b] \neq \emptyset$.

Com que $[a] \subseteq [b]$, resulta que $[a] \cap [b] = [a]$ (propietat de la intersecció de conjunts). Ara bé, una classe sempre té un element, com a mínim: $a \in [a]$ (per la propietat reflexiva). Per tant, $[a] \cap [b] = [a] \neq \emptyset$.

2.17 Examen final 6/6/2013

207

a) Volem demostrar que hi ha infinits nombres primers. Ho fem per reducció a l'absurd. Suposem que hi ha un nombre finit de nombres primers i que aquests són $p_1, p_2, \ldots, p_n$. Considerem el nombre:

$$Q = p_1 p_2 \cdots p_n + 1$$

Observem que $Q \geq 2$. Pel teorema de la divisió entera, el residu de dividir Q entre qualsevol dels primers p_i és 1. Per tant, Q no és divisible per cap nombre primer. Però el teorema de la factorització assegura que un nombre enter més gran o igual que 2 és primer o un producte de primers. Deduïm que Q és un nombre primer diferent de tots els nombres primers que existeixen, segons la hipòtesi. Això és una contradicció. Conclusió: hi ha infinits nombres primers.

b) Suposem que $a \equiv b \pmod m$ i $a' \equiv b' \pmod m$. Volem demostrar que $a + a' \equiv b + b' \pmod m$. Si $a \equiv b \pmod m$, llavors, per difinició de congruència, $m \mid (a - b)$. De la mateixa manera, si $a' \equiv b' \pmod m$, llavors $m \mid (a' - b')$. Per la propietat de la linealitat, m divideix la suma; és a dir:

$$m \mid (a - b) + (a' - b')$$

però, $(a - b) + (a' - b') = (a + a') - (b + b')$. Per tant, $m \mid ((a + a') - (b + b'))$; és a dir, $a + a' \equiv b + b' \pmod m$.

208

a) En primer lloc notem que 7 és un nombre primer i, per tant, $\mathbb{Z}_7$ és un cos. Això vol dir que tota classe diferent de la classe $\overline{0}$ té invers. Com que 7 és prou petit, podem fer els càlculs dels inversos calculant tots els productes possibles (és a dir, no cal aplicar l'algorisme d'Euclides estès). Tenim $\overline{1}^{-1} = \overline{1}$ i $\overline{6}^{-1} = \overline{6}$ (ja que $\overline{6} = -\overline{1}$). A més:

$$\overline{2} \cdot \overline{3} = \overline{6}, \qquad \overline{2} \cdot \overline{4} = \overline{1}$$
$$\overline{3} \cdot \overline{5} = \overline{1}$$

Per tant: $\overline{1}^{-1} = \overline{1}$, $\overline{2}^{-1} = \overline{4}$, $\overline{3}^{-1} = \overline{5}$, $\overline{4}^{-1} = \overline{2}$, $\overline{5}^{-3} = \overline{3}$, $\overline{6}^{-1} = \overline{6}$.

b) Apliquem el mètode de reducció de Gauss. Escrivim les matrius del sistema i ampliada i substituïm la fila 2 per $\overline{3}F_1 - \overline{5}F_2$ (F_i denota la fila i), obtenint d'aquesta manera un sistema d'equacions equivalent (és a dir, amb les mateixes solucions que l'original):

$$\begin{pmatrix} \overline{5} & -\overline{5} & | & \overline{4} \\ \overline{3} & \overline{2} & | & \overline{5} \end{pmatrix} \sim \begin{pmatrix} \overline{5} & -\overline{5} & | & \overline{4} \\ \overline{0} & \overline{3} & | & \overline{1} \end{pmatrix}$$

(Càlculs: $-\overline{3} \cdot \overline{5} - \overline{5} \cdot \overline{2} = \overline{3}$; $\overline{3} \cdot \overline{4} - \overline{5} \cdot \overline{5} = \overline{1}$.)

La segona equació és $\overline{3} \cdot \overline{y} = \overline{1}$. Per tant, $\overline{y} = \overline{3}^{-1} \cdot \overline{1} = \overline{5}$. Substituint a la primera equació, obtenim:

$$\overline{5} \cdot \overline{x} - \overline{5} \cdot \overline{y} = \overline{5} \cdot \overline{x} - \overline{5} \cdot \overline{5} = \overline{5} \cdot \overline{x} + \overline{3} = \overline{4} \Rightarrow \overline{5} \cdot \overline{x} = \overline{4} - \overline{3} = \overline{1}$$

i multiplicant per l'invers de $\overline{5}$, obtenim $\overline{x} = \overline{5}^{-1} = \overline{3}$.

Solució del sistema: $\overline{x} = \overline{3}$, $\overline{y} = \overline{5}$.

209

a) Volem demostrar que $M_p \cap M_q = M_{pq}$. Podríem demostrar que cada conjunt està inclòs a l'altre, però en aquest cas es pot demostrar directament que $x \in M_p \cap M_q$ és equivalent a $x \in M_{pq}$:

$$\begin{aligned} x \in M_p \cap M_q &\Leftrightarrow x \in M_p \wedge x \in M_q && \text{definició d'intersecció} \\ &\Leftrightarrow p \mid x \wedge q \mid x && \text{definició de } M_p \text{ i de } M_q \\ &\Leftrightarrow \operatorname{mcm}(p,q) \mid x && \text{propietat del mcm} \\ &\Leftrightarrow pq \mid x && \operatorname{mcm}(p,q) = pq, \text{ perquè són primers diferents} \\ &\Leftrightarrow x \in M_{pq} && \text{definició de } M_{pq} \end{aligned}$$

Conclusió: $M_{pq} = M_p \cap M_q$.

b) Hem de veure que $M_{p^2} \subset M_p$, on p és un nombre primer. És a dir, hem de provar: 1) que tot element de M_{p^2} és un element de M_p i, a més, 2) que són diferents (és dir, que hi ha un element a M_p que no pertany a M_{p^2}).

Sigui $x \in M_{p^2}$. Llavors per definició d'aquest conjunt: $p^2 \mid x$. Però $p \mid p^2$ i, per la propietat transitiva de la divisibilitat, tenim que $p \mid x$. Per tant, $x \in M_p$.

Considerem el nombre p. Està clar que $p \in M_p$, ja que $p \mid p$. Però $p \notin M_{p^2}$, ja que p^2 no és un divisor de p. Per tant, $M_{p^2} \neq M_p$.

210

Cas inicial: $n = 1$. $2 = \frac{(2 \cdot 1)!}{1!}$ és certa..

Pas d'inducció: Fixem un enter $n \geq 1$ i suposem que:

$$2 \cdot 6 \cdot 10 \cdots (4n-2) = \frac{(2n)!}{n!}, \quad \text{(hipòtesi d'inducció)}$$

Volem demostrar:

$$2 \cdot 6 \cdot 10 \cdots (4n-2) \cdot (4(n+1)-2) = \frac{(2(n+1))!}{(n+1)!}$$

Tenim:

$$\begin{aligned} 2 \cdot 6 \cdot 10 \cdots (4n-2) \cdot (4(n+1)-2) &= 2 \cdot 6 \cdot 10 \cdots (4n-2) \cdot (4n+2) \\ &= \frac{(2n)!}{n!} \cdot (4n+2) && \text{per hip. d'ind.} \\ &= \frac{2(2n+1)(2n)!}{n!} \end{aligned}$$

D'altra banda, tenim:

$$\frac{(2(n+1))!}{(n+1)!} = \frac{(2n+2)!}{(n+1)!} = \frac{(2n+2) \cdot (2n+1) \cdot (2n)!}{(n+1) \cdot n!} = \frac{2(2n+1)(2n)!}{n!}$$

Per tant, són iguals.

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

2.18 Examen final de reavaluació 10/07/2013

211

1) En primer lloc obtenim $A - B$. $A - B = \{t : t \in A \wedge t \notin B\} = \{\overline{2}, \overline{3}\}$. Així,

$$\begin{aligned} f[S] &= f[A - B] \\ &= f[\{\overline{2}, \overline{3}\}] = \{f(\overline{2}), f(\overline{3})\} \\ &= \{\overline{4}\,\overline{2} + \overline{2}, \overline{4}\,\overline{3} + \overline{2}\} \\ &= \{\overline{4 \cdot 2 + 2}, \overline{4 \cdot 3 + 2}\} \\ &= \{\overline{10}, \overline{14}\} \\ &= \{\overline{3}, \overline{0}\}. \end{aligned}$$

2) En ser 7 primer, totes les classes diferents de $\overline{0}$ tenen invers.

Injectiva? Hem de veure si $f(\overline{x}) = f(\overline{y}) \Rightarrow \overline{x} = \overline{y}$.

$$f(\overline{x}) = f(\overline{y}) \Rightarrow \overline{4} \cdot \overline{x} + \overline{2} = \overline{4} \cdot \overline{y} + \overline{2} \Rightarrow \overline{4} \cdot \overline{x} = \overline{4}\,\overline{y}$$

Existeix l'invers de la classe $\overline{4}$ (ja que $\text{mcd}(4, 7) = 1$). Multiplicant els dos membres de la igualtat anterior per $(\overline{4})^{-1}$ resulta $((\overline{4})^{-1}\overline{4})\,\overline{x} = ((\overline{4})^{-1}\overline{4})\,\overline{y}$ resulta $\overline{1}\overline{x} = \overline{1}\overline{y}$, d'on $\overline{x} = \overline{y}$. Per tant, f és injectiva. Observeu que per a aquesta argumentació no ens cal saber quin és l'invers: n'hi ha prou amb saber que existeix.

Exhaustiva? Hem de veure que tot element $\overline{z} \in \mathbb{Z}_7$ té alguna antiimatge. És a dir, que existeix $\overline{t} \in \mathbb{Z}_7$ tal que $f(\overline{t}) = \overline{z}$. Imposem $f(\overline{t}) = \overline{z}$ com si fos una equació a resoldre, amb incògnita $\overline{t}$, que hem d'obtenir en funció de $\overline{z}$. Les solucions seran les antiimatges, si n'hi ha, de $\overline{z}$. Es concreta a:

$$\begin{aligned}&\overline{4}\,\overline{t}+\overline{2}=\overline{z}\\&\overline{4}\,\overline{t}=\overline{z}-\overline{2}\end{aligned}$$

Calculem l'invers de $\overline{4}$. Algorisme d'Euclides estès:

1	0	1	−1
0	1	−1	2
	1	1	3
7	4	3	1
3	1	0	

Identitat de Bézout: $7\cdot(-1)+4\cdot 2=1$. Per tant, $(\overline{4})^{-1}=\overline{2}$.

Ara resulta:

$$\begin{aligned}\overline{4}\,\overline{t}=\overline{z}-\overline{2}&\Rightarrow(\overline{4})^{-1}\overline{4}\,\overline{t}=(\overline{4})^{-1}(\overline{z}-\overline{2})\\&\Rightarrow((\overline{4})^{-1}\overline{4})\,\overline{t}=(\overline{4})^{-1}(\overline{z}-\overline{2})\\&\Rightarrow\overline{1}\,\overline{t}=(\overline{4})^{-1}(\overline{z}-\overline{2})\\&\Rightarrow\overline{t}=(\overline{4})^{-1}(\overline{z}-\overline{2})\\&\Rightarrow\overline{t}=\overline{2}(\overline{z}-\overline{2})\\&\Rightarrow\overline{t}=\overline{2}\overline{z}-\overline{2}\cdot\overline{2}\\&\Rightarrow\overline{t}=\overline{2}\overline{z}-\overline{4}\end{aligned}$$

O també $\overline{t}=\overline{2}\overline{z}-\overline{4}=\overline{2}\overline{z}+\overline{3}$.

Per tant, f és exhaustiva. Juntament amb la injectivitat, f és bijectiva i, per tant, f té inversa f^{-1}.

Noteu que de l'estudi anterior, atès que resulta que tot element $\overline{z}$ té antiimatge única, se'n deriva també la propietat de ser injectiva.

La inversa és $f^{-1}(\overline{z})=\overline{2}\overline{z}+\overline{3}$.

3) $A\cap B=\{\overline{1},\overline{5}\}$. Així:

$$\begin{aligned}f^{-1}[A\cap B]&=f^{-1}[\{\overline{1},\overline{5}\}]\\&=f^{-1}[\{\overline{1}\}]\cup f^{-1}[\{\overline{5}\}]\\&=\{\overline{2}\cdot\overline{1}+\overline{3}\}\cup\{\overline{2}\cdot\overline{5}+\overline{3}\}\\&=\{\overline{5},\overline{13}\}=\{\overline{5},\overline{6}\}\end{aligned}$$

212

1) Per inducció sobre n.

Pas base. Provem la propietat per a $n=0$, és a dir, que $6|(7^0+5)$, cosa que és òbvia, ja que $7^0+5=1+5=6$, que és múltiple de 6.

Pas inductiu. Fixem un enter $n \geq 0$ i suposem que la propietat és certa per a l'enter n. És a dir, suposem que $6|(7^n + 5)$ (hipòtesi d'inducció). Hem de provar que $6|(7^{n+1} + 5)$.

Manipulem l'expressió $7^{n+1} + 5$ amb l'objectiu de fer-hi aparèixer com a subfórmula 7^n+5 i així poder aplicar la hipòtesi d'inducció. Si suposem que $7^n+5 = 6k$, per a algun $k \in \mathbb{Z}$, per hipòtesis, aleshores:

$$\begin{aligned} 7^{n+1} + 5 &= 7^n 7 + 5 = 7^n(6+1) + 5 \\ &= 6 \cdot 7^n + (7^n + 5) \\ &= 6 \cdot 7^n + 6k = 6(7^n + k) \\ &= 6k', \end{aligned}$$

que és múltiple de 6.

Per tant, la propietat és certa per a tot $n \in \mathbb{N}$.

2) Per congruències mòdul $m = 6$. Expressem la propietat de divisibilitat en termes de congruències. Apliquem que $6|7^n + 5$ si, i només si, $7^n + 5 \equiv 0 \pmod 6$. Per tant, resoldre el problema equival a demostrar $7^n + 5 \equiv 0 \pmod 6$. Tenim

$$7 \equiv 1 \pmod 6 \Rightarrow 7^n \equiv 1^n \pmod 6 \Rightarrow 7^n \equiv 1 \pmod 6.$$

Aleshores $7^n + 5 \equiv 1 + 5 = 6 \equiv 0 \pmod 6$. De fet, ja que dos enters iguals són congruents respecte de qualsevol mòdul (trivialment, per la definició), hem vist:

$$7^n + 5 \equiv 1 + 5 \equiv 6 \equiv 0 \pmod 6$$

Per transitivitat de la relació de congruència, $7^n + 5 \equiv 0 \pmod 6$.

3) Per classes de residus mòdul $m = 6$ (és a dir, treballant a $\mathbb{Z}_6$). Expressem la propietat de divisibilitat en termes de classes de residus: $6|7^n + 5$ si, i només si, $\overline{7^n + 5} = \overline{0}$ a $\mathbb{Z}_6$ Hem de demostrar, doncs, $\overline{7^n + 5} = \overline{0}$ a $\mathbb{Z}_6$.

Observem que $\overline{7} = \overline{1}$. Aleshores tenim:

$$\overline{7^n + 5} = \overline{7^n} + \overline{5} = \overline{7}^n + \overline{5} = \overline{1}^n + \overline{5} = \overline{1} + \overline{5} = \overline{6} = \overline{0}$$

com havíem de provar.

213

1) Apliquem el teorema d'Euclides:

$$\begin{aligned} \mathrm{mcd}(3n+10, 2n+7) &= \mathrm{mcd}((3n+10) - (2n+7), 2n+7) \\ &= \mathrm{mcd}(n+3, 2n+7) \\ &= \mathrm{mcd}((2n+7) - (n+3), n+3) \\ &= \mathrm{mcd}(n+4, n+3) \\ &= \mathrm{mcd}((n+4) - (n+3), n+3) \\ &= \mathrm{mcd}(1, n+3) = 1 \end{aligned}$$

2) Per casos segons la paritat de n:

Cas 1. n és parell. Aleshores existeix k enter tal que $n = 2k$. Per tant,

$$\begin{aligned} n^2 + 3n + 6 &= (2k)^2 + 3(2k) + 6 \\ &= 4k^2 + 2(3k) + 2 \cdot 3 \\ &= 2(2k^2 + 3k + 3) \\ &= 2k', \end{aligned}$$

que és parell, amb $k' = 2k^2 + 3k + 3$.

Cas 2. n és senar. Aleshores existeix k enter tal que $n = 2k + 1$. Per tant,

$$\begin{aligned} n^2 + 3n + 6 &= (2k+1)^2 + 3(2k+1) + 6 \\ &= (4k^2 + 4k + 1) + (6k + 3) + 6 \\ &= 4k^2 + 10k + 10 \\ &= 2(2k^2 + 5k + 5) \\ &= 2k \end{aligned}$$

que és parell, amb $k' = 2k^2 + 5k + 5$.

3) Utilitzem la fórmula del binomi de Newton:

$$\sum_{k=0}^{n} \binom{n}{k} 7^k = \sum_{k=0}^{n} \binom{n}{k} 7^k 1^{n-k} = (7+1)^n = 8^n$$

2.19 Examen parcial 17/10/2013

214 Per a demostrar l'equivalència, demostrem que a) implica b), que b) implica c) i, finalment, que c) implica a).

a) $\Rightarrow$ *b*) Fem una prova directa. Suposem que n és senar. Volem demostrar que $n^2 = 4k + 1$, per a algun enter k. Tenim:

$$\begin{aligned} n \text{ senar } &\Rightarrow n = 2t + 1, \text{ per a algun } t \in \mathbb{Z} \\ &\Rightarrow n^2 = (2t+1)^2 = 4t^2 + 4t + 1 \\ &\Rightarrow n^2 = 4(t^2 + t) + 1 \end{aligned}$$

b) $\Rightarrow$ *c*) Fem una prova directa. Suposem que $n^2 = 4k + 1$, per a algun $k \in \mathbb{Z}$. Volem demostrar que $n^2 + 1$ és parell. Tenim:

$$n^2 = 4k + 1 \Rightarrow n^2 + 1 = 4k + 1 + 1 = 4k + 2 = 2(2k + 1)$$

Per tant, $n^2 + 1$ és parell.

$c) \Rightarrow a)$ Fem una prova del contrarrecíproc. Suposem que n és parell. Volem demostrar que n^2+1 és senar.

$$n \text{ parell } \Rightarrow \exists t \in \mathbb{Z}(n = 2t) \Rightarrow n^2+1 = 4t^2+1 = 2(2t^2)+1$$

És a dir, n^2+1 és senar.

215

Cas inicial: $n = 1$**.**

$$(-1)^1 \cdot (2 \cdot 1 - 1) = -1$$

Pas d'inducció: Fixem un enter $m \geq 1$ i suposem que:

$$-1+3-5+\cdots+(-1)^m(2m-1) = (-1)^m \cdot m \qquad \text{(hip. d'inducció)}$$

Volem demostrar:

$$-1+3-5+\cdots+(-1)^{m+1}(2(m+1)-1) = (-1)^{m+1} \cdot (m+1)$$

Tenim:

$$\begin{aligned}\sum_{i=1}^{m+1}(-1)^i(2i-1) &= \left(\sum_{i=1}^{m}(-1)^i(2i-1)\right) + (-1)^{m+1}(2m+1) \\ &= (-1)^m \cdot m + (-1)^{m+1}(2m+1) && \text{per hip. d'ind.} \\ &= (-1)^{m+1}(-m+2m+1) \\ &= (-1)^{m+1}(m+1)\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

2.20 Examen parcial 14/11/2013

216 Presentem dues solucions. *Solució 1.* Sabem que $A \cap B \subseteq B$. Per tant, si $A \cap B = A$, llavors $A \subseteq B$, que implica que $A \cup B = B$. Per tant, $A \cup B \cup C = B \cup C$.

Solució 2. Hem de provar una igualtat de conjunts; és a dir, hem de provar que cada conjunt és un subconjunt de l'altre. La inclusió $B \cup C \subseteq A \cup B \cup C$ és vàlida sempre. Demostrem l'altra.

Per la propietat associativa de la unió de conjunts, podem escriure $A \cup B \cup C = (A \cup B) \cup C$. Sigui $x \in (A \cup B) \cup C$. Tenim:

$$\begin{aligned}x \in (A \cup B) \cup C &\Rightarrow (x \in A \vee x \in B) \vee x \in C \\ &\Rightarrow (x \in B \vee x \in B) \vee x \in C && (1) \\ &\Rightarrow x \in B \vee x \in C \\ &\Rightarrow x \in B \cup C\end{aligned}$$

(1): per hipòtesi, $A = A \cap B \subseteq B$ i, per tant, si $x \in A$, llavors $x \in B$.

217

a) Una relació R és d'equivalència si, i només si, R és reflexiva, simètrica i transitiva.

- R és reflexiva: $x_1x_2\cdots x_n \, R \, x_1x_2\cdots x_n$, perquè $x_1 = x_1$ i $x_2 = x_2$.
- R és simètrica: si $x_1x_2\cdots x_n \; R \; y_1y_2\cdots y_n$, llavors $x_1 = y_1$ i $x_2 = y_2$. D'aqui deduïm que $y_1 = x_1$ i $y_2 = x_2$ i, per tant, $y_1y_2\cdots y_n \, R \, x_1x_2\cdots x_n$.
- R és transitiva: si $x_1x_2\cdots x_n R y_1y_2\cdots y_n$ i $y_1y_2\cdots y_n R z_1z_2\cdots z_n$, llavors $x_1 = y_1$, $x_2 = y_2$ i $y_1 = z_1$, $y_2 = z_2$. Per tant, $x_1 = z_1$ i $x_2 = z_2$. Deduïm doncs que $x_1x_2\cdots x_n \, R \, z_1z_2\cdots z_n$.

b) Per definició de R, dues paraules binàries estan relacionades si, i només si, tenen els mateixos dos primers bits. Per tant:

$$\begin{aligned}[x_1x_2\cdots x_n]_R &= \{y_1y_2\cdots y_n \in X : y_1y_2\cdots y_n \, R \, x_1x_2\cdots x_n\} \\ &= \{y_1y_2\cdots y_n \in X : y_1 = x_1, y_2 = x_2\}\end{aligned}$$

Per tant, tenim les classes d'equivalència següents:

$$\begin{aligned}[000\cdots 0]_R &= \{y_1y_2\cdots y_n \in X : y_1 = 0, y_2 = 0\} \\ [010\cdots 0]_R &= \{y_1y_2\cdots y_n \in X : y_1 = 0, y_2 = 1\} \\ [100\cdots 0]_R &= \{y_1y_2\cdots y_n \in X : y_1 = 1, y_2 = 0\} \\ [110\cdots 0]_R &= \{y_1y_2\cdots y_n \in X : y_1 = 1, y_2 = 1\}\end{aligned}$$

(paraules que comencen per 00, per 01, per 10 i per 11, respectivament).

c) El conjunt quocient és, per definicó, el conjunt els elements del qual són les classes d'equivalència:

$$\begin{aligned}X/R &= \{[x_1x_2\cdots x_n]_R : x_1x_2\cdots x_n \in X\} \\ &= \{[000\cdots 0]_R, [010\cdots 0]_R, [100\cdots 0]_R, [110\cdots 0]_R\}\end{aligned}$$

El conjunt quocient té doncs 4 elements.

2.21 Examen final 09/01/2014

218

1) L'equació diofàntica $ax+(3+2a)y = 10$ té solució entera si, i només si, $\text{mcd}(a, 3+2a)|10$. Ara bé, pel teorema d'Euclides, tenim:

$$\text{mcd}(a, 3 + 2a) = \text{mcd}(a, 3 + 2a - 2a) = \text{mcd}(a, 3)$$

A més, donat que 3 és un nombre primer, tenim:

$$\text{mcd}(a, 3) = \begin{cases} 3, & \text{si } 3|a \\ 1, & \text{si } 3 \not| \, a \end{cases}$$

Com que $3 \not| \, 10$, deduïm que l'equació diofàntica $ax + (3 + 2a)y = 10$ té solució entera si, i només si, $3 \not| \, a$.

2) Quan $a = 31$, l'equació és: $31x + 65y = 10$. Per l'apartat anterior sabem que té solució ja que $3 \not| 31$. Escrivim primer la identitat de Bézout de 31 i 65:

1	0	1	−10
0	1	−2	21
	2	10	3
65	31	3	1
3	1	1	

És a dir: $31 \cdot 21 + 65 \cdot (-10) = 1$. Multiplicant per 10 els dos membres d'aquesta identitat, obtenim una solució particular de l'equació: $31 \cdot 210 + 65 \cdot (-100) = 10$. Per tant, la solució general ve donada por:

$$x = 210 + 65 \cdot t, \qquad y = -100 - 31 \cdot t$$

on $t \in \mathbb{Z}$ és arbitrari.

219 Suposem que $n \equiv 4 \pmod 6$. Llavors existeix un enter k tal que $n = 6k + 4$. A més, $k \geq 0$, ja que $n \in \mathbb{N}$. D'altra banda, $10 \equiv 3 \pmod 7$. Per tant:

$$\begin{aligned} 10^n + 3 &\equiv 3^n + 3 \\ &\equiv 3^{6k+4} + 3 \\ &\equiv (3^6)^k \cdot 3^4 + 3 \qquad\qquad (*) \end{aligned}$$

Ara bé: $3^6 = (3^2)^2 \cdot 3^2$ i tenim:

$$3^2 = 9 \equiv 2, \qquad (3^2)^2 \equiv 2^2 \equiv 4, \qquad 3^6 = (3^2)^2 \cdot 3^2 \equiv 4 \cdot 2 \equiv 1$$

Finalment:

$$(3^6)^k \cdot 3^4 + 3 \equiv 1^k \cdot 3^4 + 3 \equiv 4 + 3 \equiv 0 \pmod 7$$

Observació: si coneixem el teorema de Fermat, llavors en (*) podem dir que com que $7 \not| 3$, llavors $3^{7-1} = 3^6 \equiv 1 \pmod 7$.

220 Notem, per a simplificar, $P = \{\overline{0}, \overline{2}, \cdots, \overline{398}\}$ i $S = \{\overline{1}, \overline{3}, \cdots, \overline{399}\}$. Observem que si $\overline{x} \in P$, llavors tots els enters de la classe de x són parells i si $\overline{x} \in S$, llavors tots els enters de la classe de x són senars. Això és perquè:

$$x' \equiv x \pmod{400} \Leftrightarrow x = x' + 400k$$

per a un cert enter k. Per tant, les paritats de x i x' són la mateixa.

a) Siguin $\overline{x}, \overline{y} \in \mathbb{Z}_{400}$ tals que $f(\overline{x}) = f(\overline{y})$. Volem veure si podem deduir *sempre* que $\overline{x} = \overline{y}$. Tenim els casos següents:

- $\overline{x}, \overline{y} \in P$. Llavors $\overline{7} \cdot \overline{x} + \overline{1} = \overline{7} \cdot \overline{y} + \overline{1}$, d'on deduïm que $\overline{7} \cdot \overline{x} = \overline{7} \cdot \overline{y}$. Ara bé, com que $\text{mcd}(7, 400) = 1$, la classe $\overline{7}$ té invers a $\mathbb{Z}_{400}$. Multiplicant els dos costats de la igualtat per la classe inversa de $\overline{7}$, deduïm que $\overline{x} = \overline{y}$. (El càlcul de la classe inversa de $\overline{7}$ a $\mathbb{Z}_{400}$ el fem separadament al final de l'exercici.)

- $\overline{x}, \overline{y} \in S$. Llavors $\overline{4}\cdot\overline{x}+\overline{3}=\overline{4}\cdot\overline{y}+\overline{3}$, d'on deduïm que $\overline{4}\cdot\overline{x}=\overline{4}\cdot\overline{y}$. En aquest cas, no podem simplificar la igualtat, ja que $\overline{4}$ no té invers a $\mathbb{Z}_{400}$ (perquè $\mathrm{mcd}(4,400)=4\neq 1$). Però tenim:

$$\begin{aligned}\overline{4}\cdot\overline{x}=\overline{4}\cdot\overline{y} &\Leftrightarrow 4x\equiv 4y \pmod{400}\\ &\Leftrightarrow 400 \mid 4\cdot(x-y)\\ &\Leftrightarrow 100 \mid (x-y)\\ &\Leftrightarrow x\equiv y \pmod{100}\end{aligned}$$

  Per tant, si trobem dos enters x, y no congruents entre ells mòdul 400 i tals que la diferència sigui un múltiple de 100, haurem trobat un contraexemple. Per exemple: $x=101$, $y=1$. Tenim: $\overline{101}\neq\overline{1}$, però $f(\overline{101})=f(\overline{1})=\overline{7}$.

Per tant, f no és injectiva.

Observació: encara quedarien dos casos més per discutir: $\overline{x}\in P$ i $\overline{y}\in S$; i $\overline{x}\in S$ i $\overline{y}\in P$. No obstant, no cal estudiar-los, donat que ja hem demostrat que f no és injectiva.

b) Observem el següent. Si $\overline{x}\in P$, llavors $f(\overline{x})=\overline{7}\cdot\overline{x}+\overline{1}\in S$ i si $\overline{x}\in P$, llavors també $f(\overline{x})=\overline{4}\cdot\overline{x}+\overline{3}\in S$. Per tant, la imatge d'un element de $\mathbb{Z}_{400}$ per f mai pertany a P. Per tant, f no és exhaustiva.

c) Plantegem les equacions: $\overline{7}\cdot\overline{x}+\overline{1}=\overline{201}$ i $\overline{4}\cdot\overline{x}+\overline{3}=\overline{201}$. Per la primera tenim:

$$\overline{7}\cdot\overline{x}+\overline{1}=\overline{201}\Rightarrow\overline{7}\cdot\overline{x}=\overline{200}\Rightarrow\overline{x}=\overline{7}^{-1}\cdot\overline{200}=\overline{343}\cdot\overline{200}=\overline{200}$$

Com que $\overline{200}\in\mathcal{P}$, tenim que $\overline{200}\in f^{-1}[\{\overline{201}\}]$.

Estudiem ara la segona equació:

$$\overline{4}\cdot\overline{x}+\overline{3}=\overline{201}\Rightarrow\overline{4}\cdot\overline{x}=\overline{198}$$

Com que la classe $\overline{4}$ no té invers a $\mathbb{Z}_{400}$, escrivim aquesta igualtat de classes com una congruència mòdul 400 i intentem simplificar-la:

$$\overline{4}\cdot\overline{x}=\overline{198}\Rightarrow 4x\equiv 198 \pmod{400}$$

Ara bé, aquesta congruència no té solució perquè $\mathrm{mcd}(4,400)$ no divideix a 198.

Conclusió: $f^{-1}[\{\overline{201}\}]=\{\overline{200}\}$.

Càlcul de l'invers de 7 *mòdul* 400: apliquem l'algorisme d'Euclides estès i escrivim la identitat de Bézout:

X	1	0	1
Y	0	1	-57
Q		57	7
R	400	7	1
	1	0	

Per tant, comprovem que $\mathrm{mcd}(7,400)=1$ i, a més: $400\cdot 1+7\cdot(-57)=1$. Per tant: $\overline{7}^{-1}=\overline{-57}=\overline{343}$.

2.22 Examen de recuperació del primer parcial 09/01/2014

221

Cas inicial. Si $n = 1$, llavors $3 \cdot 5^{2+1} + 2^{3+1} = 391 = 17 \cdot 23$, que és múltiple de 17.

Pas inductiu. Fixem $m \geq 1$ i suposem que:

$$3 \cdot 5^{2m+1} + 2^{3m+1} = 17 \cdot k \qquad \text{(Hipòtesi d'inducció)}$$

per a cert $k \in \mathbb{Z}$. Volem demostrar que $3 \cdot 5^{2(m+1)+1} + 2^{3(m+1)+1}$ també és un múltiple de 17. Tenim:

$$\begin{aligned} 3 \cdot 5^{2(m+1)+1} + 2^{3(m+1)+1} &= 3 \cdot 5^{2m+3} + 2^{3m+4} = \\ &= 3 \cdot 5^{2m+1} \cdot 5^2 + 2^{3m+1} \cdot 2^3 = \\ &= 8 \cdot (3 \cdot 5^{2m+1} + 2^{3m+1}) + 17 \cdot 3 \cdot 5^{2m+1} = \\ &= 8 \cdot 17 \cdot k + 17 \cdot 3 \cdot 5^{2m+1} = && \text{(H.I.)} \\ &= 17 \cdot (8k + 3 \cdot 5^{2m+1}) \end{aligned}$$

Pel principi d'inducció, la propietat és certa per a tot enter $n \geq 1$.

222

a) P1) $\neg \forall x\, \exists y\ (x+y = 0) \equiv \exists x\, \neg \exists y\ (x+y = 0) \equiv \exists x\, \forall y\, \neg (x+y = 0) \equiv \exists x\, \forall y\, (x+y \neq 0)$.

P2) $\neg \exists x\, \forall y\ (x+y = y) \equiv \forall x\, \neg \forall y\ (x+y = y) \equiv \forall x\, \exists y\ \neg (x+y = y) \equiv \forall x\, \exists y\ (x+y \neq y)$.

Hem aplicat les següents equivalències:

$$\neg \forall x\, (A(x)) \equiv \exists x\, (\neg A(x))$$
$$\neg \exists x\, (A(x)) \equiv \forall x\, (\neg A(x))$$

b) P1) Aquesta proposició és falsa. Per a demostrar-ho, és suficient amb trobar un contraexemple. Per exemple, si $x = 1$, no existeix cap nombre natural y tal que $1 + y = 0$.

P2) Aquesta proposició és certa. Si prenem $x = 0$, llavors per a tot nombre natural y, tenim $0 + y = y$. (Si considerem que 0 no és un nombre natural, llavors la propietat és falsa. Per a demostrar-ho, hem de veure que la seva negació és certa. És a dir, donat un $x \in \mathbb{N}$ qualsevol, hem de veure que existeix un $y \in \mathbb{N}$ tal que $x + y \neq y$. Podem prendre $y = x$, de manera que $x + x = 2x \neq x$.)

2.23 Examen de recuperació del segon parcial 09/01/2014

223 Suposem que $A \subseteq B$. Volem veure que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. És a dir, volem demostrar que si $X \in \mathcal{P}(A)$, aleshores $X \in \mathcal{P}(B)$. Tenim:

$$X \in \mathcal{P}(A) \Leftrightarrow X \subseteq A \Rightarrow X \subseteq B \Leftrightarrow X \in \mathcal{P}(B)$$

La primera i la última equivalència, per definició del conjunt de les parts d'un conjunt; la implicació és per hipòtesi, ja que si $X \subseteq A$ i, per hipòtesi $A \subseteq B$, llavors $X \subseteq B$, per la transitivitat de la relació d'inclusió.

El recíproc també és cert. Suposem que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Volem demostrar que $A \subseteq B$; és a dir, que si $x \in A$, llavors $x \in B$. Tenim:

$$x \in A \Leftrightarrow \{x\} \subseteq A \Leftrightarrow \{x\} \in \mathcal{P}(A) \Rightarrow \{x\} \in \mathcal{P}(B) \Leftrightarrow \{x\} \subseteq B \Leftrightarrow x \in B$$

Les equivalències són per definició i a la implicació hem aplicat la hipòtesi.

224

a) *R és reflexiva*: si $(x, y) \in \mathbb{R}^2$, llavors $\frac{y}{x^2+1} = \frac{y}{x^2+1}$. Per tant, és reflexiva.

R és simètrica: suposem que $(x_1, y_1)R(x_2, y_2)$. Llavors $\frac{y_1}{x_1^2+1} = \frac{y_2}{x_2^2+1}$ i, com es tracta d'una igualtat, deduïm que $(x_2, y_2)R(x_1, y_1)$. Per tant, és simètrica.

R és transitiva: suposem que $(x_1, y_1)R(x_2, y_2)$ i $(x_2, y_2)R(x_3, y_3)$. Llavors tenim que $\frac{y_1}{x_1^2+1} = \frac{y_2}{x_2^2+1}$ i $\frac{y_2}{x_2^2+1} = \frac{y_3}{x_3^2+1}$. Deduïm que $\frac{y_1}{x_1^2+1} = \frac{y_3}{x_3^2+1}$. Per tant, $(x_1, y_1)R(x_3, y_3)$. És a dir, R és transitiva.

b) Per definició de classe d'equivalència, tenim:

$$[(a, b)] = \{(x, y) \in \mathbb{R}^2 : (x, y)R(a, b)\} = \left\{(x, y) \in \mathbb{R}^2 : \frac{y}{x^2+1} = \frac{b}{a^2+1}\right\}$$

En particular, trobem que:

$$[(0, 0)] = \left\{(x, y) \in \mathbb{R}^2 : \frac{y}{x^2+1} = 0\right\} = \{(x, y) \in \mathbb{R}^2 : y = 0\}$$

És a dir, la classe $[(0, 0)]$ està formada pels punts de l'eix x. Anàlogament, tenim:

$$[(0, 1)] = \left\{(x, y) \in \mathbb{R}^2 : \frac{y}{x^2+1} = 1\right\} = \{(x, y) \in \mathbb{R}^2 : y = x^2 + 1\}$$

És a dir, la classe d'equivalència del punt $(0, 0)$ està forma de pels punts de la paràbola d'equació $y = x^2 + 1$. Finalment:

$$[(0, -2)] = \left\{(x, y) \in \mathbb{R}^2 : \frac{y}{x^2+1} = -2\right\} = \{(x, y) \in \mathbb{R}^2 : y = -2(x^2 + 1)\}$$

És a dir, els elements de la classe $[(0, -2)]$ són els punts de la paràbola d'equació $y = -2(x^2 + 1)$.

c) En general, donat el punt $(a, b) \in \mathbb{R}^2$, si escrivim $c = \frac{b}{a^2+1}$, tenim:

$$[(a, b)] = \left\{(x, y) \in \mathbb{R}^2 : \frac{y}{x^2+1} = c\right\} = \{(x, y) \in \mathbb{R}^2 : y = c(x^2 + 1)\}$$

És a dir, els elements de la classe $[(a, b)]$ són els punts de la paràbola d'equació $y = c(x^2 + 1)$ (la recta $y = 0$, en el cas de $[(a, 0)] = [(0, 0)]$).

2.24 Examen final de reavaluació 07/02/2014

225

1) Recordem que: $x \in X \setminus Y \Leftrightarrow x \in X \wedge x \notin Y$. Per tant, aplicant la llei de De Morgan corresponent, obtenim:

$$x \notin X \setminus Y \Leftrightarrow x \notin X \vee x \in Y$$

Per a demostrar que $A \setminus (A \setminus B) \subseteq C$ considerem un element $x \in A \setminus (A \setminus B)$ arbitrari i provem que $x \in C$:

$$\begin{aligned} x \in A \setminus (A \setminus B) &\Rightarrow x \in A \wedge x \notin A \setminus B \\ &\Rightarrow x \in A \wedge (x \notin A \vee x \in B) \\ &\Rightarrow x \in B \end{aligned}$$

D'altra banda, com que $B \cap C^c = \emptyset$, si $x \in B$, llavors $x \notin C^c$; és a dir, $x \in C$. Hem vist, doncs, que $x \in C$, que és el que volíem demostrar.

2) Contraexemple: $A = B = \emptyset$, $C = \Omega = \{1\}$. Es compleix que $B \cap C^c = \emptyset$, que $A \setminus (A \setminus B) = \emptyset$ i que $C = \{1\}$. Per tant, $C \nsubseteq A \setminus (A \setminus B)$.

226

1) f és injectiva si, i només si:

$$\forall (x, y), (x', y') \in \mathbb{Z} \times \mathbb{Z}(f(x, y) = f(x', y') \to (x, y) = (x', y'))$$

És a dir, f és injectiva si, i només si:

$$\forall x, y, x', y' \in \mathbb{Z}(333x + 120y = 333x' + 120y' \to x = x' \wedge y = y')$$

En altres paraules, f és injectiva si, i només si:

$$\forall x, y, x', y' \in \mathbb{Z}(333(x - x') = 120(y' - y) \to x = x' \wedge y = y')$$

afirmació que evidentment és falsa $x = 120$, $x' = 0$, $y' = 333$, $y = 0$ n'és un contraexemple.

2) f és exhaustiva si, i només si:

$$\forall z \in \mathbb{Z}\ \exists (x, y) \in \mathbb{Z} \times \mathbb{Z}(f(x, y) = z)$$

és a dir, si, i només si:

$$\forall z \in \mathbb{Z}\ \exists (x, y) \in \mathbb{Z} \times \mathbb{Z}(333x + 120y = z)$$

Però l'equació diofàntica $333x + 120y = z$ té solució en $x, y \in \mathbb{Z}$ si, i només si, $\text{mcd}(333, 120) \mid z$. Ara bé, $\text{mcd}(333, 120) = 3$ (calculat a l'apartat següent). Per tant, si z no és múltiple de 3, l'equació no té solució. Per exemple, si $z = 1$, no hi ha solució. És a dir, f no és exhaustiva perquè, per exemple, $z = 1$ no té antiimatge.

3) Tenim:

$$\begin{aligned} f^{-1}[\{3\}] &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : f(x,y) = 3\} \\ &= \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : 333x + 120y = 3\} \end{aligned}$$

Resolem, doncs, l'equació diofàntica $333x + 120y = 3$. L'equació admet solució si, i només si, $\mathrm{mcd}(333, 120) \mid 3$. Calculem aquest mcd via l'algorisme d'Euclides i, si es compleix aquesta condició de divisibilitat, estenem l'algorisme per a poder trobar coeficients per a la identitat de Bézout.

X	1	0	1	-1	4	-9
Y	0	1	-2	3	-11	25
Q		2	1	3	2	4
R	333	120	93	27	12	3

Com que $\mathrm{mcd}(333, 120) = 3$, l'equació diofàntica té solució. Busquem, via la identitat de Bézout, una solució particular. Amb l'algorisme d'Euclides estès trobem que:

$$(-9) \cdot 333 + 25 \cdot 120 = 3$$

Comparant amb l'equació a resoldre veiem que $x_0 = -9$, $y_0 = 25$ és una solució particular. La solució general és:

$$\begin{aligned} x &= -9 + \frac{120}{3}t = -9 + 40t \\ y &= 25 + \frac{333}{3}t = 25 + 111t \end{aligned}$$

on $t \in \mathbb{Z}$.

Per tant:

$$f^{-1}[\{3\}] = \{(x,y) \in \mathbb{Z} \times \mathbb{Z} : \exists t \in \mathbb{Z}\ x = -9 + 40t, y = 25 + 111t\}$$

227 Afirmar que els dos últims dígits d'un nombre són 01 equival a afirmar que el nombre en qüestió és congruent amb 1 mòdul 100 o que:

$$11^n - 10n - 1 \equiv 0 \pmod{100}$$

Farem la demostració per inducció.

Pas bàsic $n = 2$. Hem de comprovar que $11^2 - 10 \cdot 2 - 1 = 100 \equiv 0 \pmod{100}$, la qual cosa és certa.

Pas inductiu. Sigui $n \geq 2$. Hem de demostrar que partint de que

$$11^n - 10n - 1 \equiv 0 \pmod{100} \quad \text{(H.I.)}$$

s'arriba a que:

$$11^{n+1} - 10(n+1) - 1 \equiv 0 \pmod{100}).$$

Som-hi:

$$11^{n+1} - 10(n+1) - 1 \equiv 11 \cdot 11^n - 10n - 11 \pmod{100}$$

Per aplicar la hipòtesi d'inducció seria interessant disposar de l'invers de 11 mòdul 100, el qual invers existeix per ser $\mathrm{mcd}(11, 100) = 1$. En aquest cas no cal ni tan sols aplicar l'algorisme d'Euclides estès per al seu càlcul, n'hi ha prou que ens adonem que $11 \cdot 9 \equiv 99 \equiv -1 \pmod{100}$ i que, per tant, $11 \cdot (-9) \equiv 1 \pmod{100}$. Continuem amb la demostració:

$$\begin{aligned}
11^{n+1} - 10(n+1) - 1 &\equiv 11 \cdot (11^n - (-9) \cdot 10n - 1) \\
&\equiv 11 \cdot (11^n + 90n - 1) \\
&\equiv 11 \cdot (11^n - 10n - 1) \\
&\equiv 11 \cdot 0 && \text{(H.I.)} \\
&\equiv 0
\end{aligned}$$

228

a) Per veure que la relació és d'equivalència, comprovem que és reflexiva, simètrica i transitiva.

- Reflexiva. Hem de veure que per a tot $x \in \mathbb{Z}$ és xRx; és a dir, hem de veure que per a tot $x \in \mathbb{Z}$, $\mathrm{mcd}(x, 4) = \mathrm{mcd}(x, 4)$, la qual cosa és certa.
- Simètrica. Hem de veure que per a tot $x, y \in \mathbb{Z}$, si xRy, llavors yRx; és a dir, hem de comprovar que per a tot $x, y \in \mathbb{Z}$, si $\mathrm{mcd}(x, 4) = \mathrm{mcd}(y, 4)$, llavors $\mathrm{mcd}(y, 4) = \mathrm{mcd}(x, 4)$, la qual cosa és certa.
- Transitiva. Hem de veure que per a tot $x, y, z \in \mathbb{Z}$, si xRy i yRz, llavors xRz; és a dir, hem de comprovar que per a tot $x, y, z \in \mathbb{Z}$, $\mathrm{mcd}(x, 4) = \mathrm{mcd}(y, 4)$ i $\mathrm{mcd}(y, 4) = \mathrm{mcd}(z, 4)$, llavors $\mathrm{mcd}(x, 4) = \mathrm{mcd}(z, 4)$, la qual cosa és certa.

b) Per definició de classe d'equivalència, tenim:

$$[x] = \{y \in \mathbb{Z} : xRy\} = \{y \in \mathbb{Z} : \mathrm{mcd}(x, 4) = \mathrm{mcd}(y, 4)\}$$

Però $\mathrm{mcd}(x, 4) \mid 4$. Per tant, només pot valer 1, 2 o 4 i $\mathrm{mcd}(1, 4) = 1$, $\mathrm{mcd}(2, 4) = 2$ i $\mathrm{mcd}(4, 4) = 4$. Per tant, només hi haurà tres classes:

$$\begin{aligned}
[1] &= \{x \in \mathbb{Z} : 1Rx\} \\
&= \{x \in \mathbb{Z} : \mathrm{mcd}(x, 4) = 1\} \\
&= \{x \in \mathbb{Z} : x \text{ és senar}\} \\
[2] &= \{x \in \mathbb{Z} : 2Rx\} \\
&= \{x \in \mathbb{Z} : \mathrm{mcd}(x, 4) = 2\} \\
&= \{x \in \mathbb{Z} : x \text{ és parell no múltiple de } 4\} \\
[4] &= \{x \in \mathbb{Z} : 3Rx\} \\
&= \{x \in \mathbb{Z} : \mathrm{mcd}(x, 4) = 4\} \\
&= \{x \in \mathbb{Z} : x \text{ és múltiple de } 4\}
\end{aligned}$$

Finalment, el conjunt quocient és $\mathbb{Z}/R = \{[1], [2], [4]\}$.

2.25 Examen parcial 20/03/2014

229

Pas base: comprovem que la propietat és certa per a $n = 1$:

$$\sum_{k=1}^{1} k(k+2) = 1 + 2 = 3 = \frac{2 \cdot 9}{6}.$$

Pas inductiu: fixem un enter $m \geq 1$ i suposem que la propietat és certa per a aquest enter m (hipòtesi d'inducció):

$$\sum_{k=1}^{m} k(k+2) = \frac{m(m+1)(2m+7)}{6}$$

Volem demostrar que la propietat és certa per a l'enter $m+1$; és a dir:

$$\sum_{k=1}^{m+1} k(k+2) = \frac{(m+1)(m+2)(2(m+1)+7)}{6} = \frac{(m+1)(m+2)(2m+9)}{6}$$

Tenim:

$$\begin{aligned}\sum_{k=1}^{m+1} k(k+2) &= \sum_{k=1}^{m} k(k+2) + (m+1)(m+3) \\ &= \frac{m(m+1)(2m+7)}{6} + (m+1)(m+3) \qquad \text{per H.I.} \\ &= \frac{m(m+1)(2m+7) + 6(m+1)(m+3)}{6} \\ &= \frac{2m^3 + 15m^2 + 31m + 18}{6}\end{aligned}$$

D'altra banda, tenim:

$$\frac{(m+1)(m+2)(2m+9)}{6} = \frac{2m^3 + 15m^2 + 31m + 18}{6}$$

Per tant, hem demostrat que la propietat és certa per a $m+1$.

Pel principi d'inducció, deduïm que la propietat és certa per a tot enter $n \geq 1$.

230 Per a demostrar que aquestes proposicions són equivalents, n'hi ha prou amb demostrar que a) $\Rightarrow$ b), que b) $\Rightarrow$ c) i que c) $\Rightarrow$ a).

Sigui $x, y \in \mathbb{Z}$ arbitraris.

a) $\Rightarrow$ b) Suposem que $x - y$ és un enter senar. Volem demostrar que $x + y$ és un enter senar. Tenim:

$$x + y = (x - y) + 2y$$

i, com que la suma d'un enter senar i un enter parell és senar, obtenim que $x + y$ és senar.

b) $\Rightarrow$ **c)** Suposem que $x+y$ és un enter senar. Volem demostrar que $3x+y$ és un enter senar. Tenim:

$$3x+y=(x+y)+2x$$

i, com que la suma d'un enter senar i un enter parell és senar, obtenim que $3x+y$ és senar.

c) $\Rightarrow$ **a)** Suposem que $3x+y$ és un enter senar. Volem demostrar que $x-y$ és un enter senar. Tenim:

$$x-y=(3x+y)-2(x+y)$$

i, com que la suma d'un enter senar i un enter parell és senar, obtenim que $x-y$ és senar.

2.26 Examen parcial 30/04/2014

231

a) S és reflexiva: per a tot $x\in\mathbb{R}$, tenim que $x-x=0\in\mathbb{Q}$. Per tant, xSx.

S és simètrica: suposem que xSy; és a dir: $x-y\in\mathbb{Q}$. Llavors $y-x=-(x-y)\in\mathbb{Q}$ i, per tant, ySx.

S és transitiva: suposem que xSy i ySz. És a dir, $x-y\in\mathbb{Q}$ i $y-z\in\mathbb{Q}$. Com que la suma de nombres racionals és racional, tenim:

$$x-z=(x-y)+(y-z)\in\mathbb{Q}.$$

Per tant, xSz.

b) La classe d'equivalència de 0 és el conjunt dels nombres racionals. Efectivament:

$$[0]=\{x\in\mathbb{R}:xS0\}=\{x\in\mathbb{R}:x-0=x\in\mathbb{Q}\}=\mathbb{Q}$$

232

a) Sigui $n\in\mathbb{Z}$. Tenim:

$$\begin{aligned}(g\circ f)(n)=g(f(n))&=\begin{cases}g(n^2), & \text{si } n \text{ és parell}\\ g((n-1)^2), & \text{si } n \text{ és senar}\end{cases}\\ &=\begin{cases}3n^2, & \text{si } n \text{ és parell}\\ 3(n-1)^2, & \text{si } n \text{ és senar}\end{cases}\\ &=3f(n)\end{aligned}$$

ja que si n és parell, llavors n^2 és parell; i, si n és senar, llavors $n-1$ és parell i $(n-1)^2$ és parell.

En qualsevol cas, hem vist que $(g\circ f)(n)=3f(n)$. Per tant, hem demostrat el que volíem.

b) L'aplicació f no és injectiva. Ho demostrem amb un contraexemple: $f(2) = 2^2 = 4$ i $f(3) = (3-1)^2 = 2^2 = 4$, però $2 \neq 3$.

c) L'aplicació g no és exhaustiva. Ho demostrem amb un contraexemple: hem de trobar un enter que no tingui cap antiimatge. Per exemple, el 2. Observem que les imatges dels enters per g o bé són múltiples de 3 o bé són múltiples de 3 més 1. En qualsevol cas, no existeix cap enter n tal que $g(n) = 2$.

d) Els elements de T són els enters múltiples de 3. Calculem primer $g^{-1}[T]$:

$$g^{-1}[T] = \{n \in \mathbb{Z} : g(n) \in T\}$$

Sigui $3k \in T$. Hem de trobar els enters n tals que $g(n) = 3k$. Observem que l'equació $g(n) = 3k$ només té solució quan n és parell, i llavors $g(n) = 3n = 3k$ té solució $n = k$ si i només si k és parell (és a dir, si k és senar, l'equació $g(n) = 3k$ no té solució). Per tant, el conjunt antiimatge de T per g està format pels nombres enters parells:

$$g^{-1}[T] = \{2m : m \in \mathbb{Z}\}.$$

Ara, per definició de f, la imatge d'un nombre parell és el seu quadrat. per tant:

$$\begin{aligned} f[g^{-1}[T]] &= f[\{2m : m \in \mathbb{Z}\}] \\ &= \{f(2m) : m \in \mathbb{Z}\} \\ &= \{4m^2 : m \in \mathbb{Z}\} \\ &= \{0, 1, 4, 9, 16, \ldots\}. \end{aligned}$$

2.27 Examen final 12/06/2014

233 Suposem que existeixen $n, m \in \mathbb{Z}$ tals que $5n^2 + 10 = m^2$.

1) D'aquesta hipòtesi deduïm que $5(n^2 + 2) = m^2$. Per tant, tenim que $5 \mid m^2$; i com que 5 és un nombre primer, pel lema d'Euclides, obtenim que $5 \mid m$.

2) De l'apartat anterior, sabem que $5 \mid m$; és a dir, $m = 5k$, per a cert enter k. Substituïm a la igualtat de la hipòtesi i obtenim:

$$5n^2 + 10 = m^2 = (5k)^2 = 25k^2$$

i si simplifiquem per 5 tenim que: $n^2 + 2 = 5k^2$; és a dir, $5 \mid n^2 + 2$.

3) Finalment, considerem la classe de l'enter $n^2 + 2$ a $\mathbb{Z}_5$, que per l'apartat anterior és múltiple de 5:

$$\overline{n^2 + 2} = \overline{n}^2 + \overline{2} = \overline{0}$$

d'on $\overline{n}^2 = -\overline{2} = \overline{3}$. És a dir, la classe $\overline{3}$ és un quadrat a $\mathbb{Z}_5$.

Anem a demostrar, per reducció a l'absurd, que si $n \in \mathbb{N}$, llavors $5n^2+10$ no és un quadrat. Suposem que ho és: $5n^2 + 10 = m^2$, on $n, m \in \mathbb{N}$. Llavors pel que hem demostrat en els apartats anteriors, $\overline{3} \in \mathbb{Z}_5$ és el quadrat d'una classe. Ara bé, si calculem els quadrats a $\mathbb{Z}_5$, obtenim les classes $\overline{0}, \overline{1}, \overline{4}$, però no la classe $\overline{3}$. Per tant, tenim una contradicció.

234 Sigui x la solució que busquem. Llavors x és l'enter positiu més petit que verifica el sistema de congruències següent:

$$x \equiv 8 \pmod{13}, \quad x \equiv 3 \pmod{11}, \quad x \equiv 5 \pmod{8}$$

Observem que els mòduls són primers entre si dos a dos. Llavors hi ha solució, que és única mòdul el producte dels mòduls $m_1m_2m_3 = 1144$. Notem:

$$\begin{array}{lll} m_1 = 13 & M_1 = m_2m_3 = 88 & y_1 = 4 \\ m_2 = 11 & M_2 = m_1m_3 = 104 & y_2 = 9 \\ m_3 = 8 & M_3 = m_1m_2 = 143 & y_3 = 7 \end{array}$$

on y_j és un invers de M_j mòdul m_j, per a $j = 1, 2, 3$, calculats usant l'algorisme d'Euclides i la identitat de Bézout. Llavors la solució és:

$$x \equiv 8M_1y_1 + 3M_2y_2 + 5M_3y_3 = 10629 \equiv 333 \pmod{1144}$$

Per tant, la solució és 333 monedes.

235

a) En primer lloc, observem que els coeficients 13 i -47 són primers entre ells (de fet, 13 i 47 són primers). És a dir, $\mathrm{mcd}(13, -47) = 1$. Per tant, com que $1 \mid 10$, hi ha solució. Busquem una solució particular usant l'algorisme d'Euclides i escrivint la identitat de Bézout corresponent als nombres positius 13 i 47 i després la modifiquem convenientment.

1	0	1	-1	2	-3	5
0	1	-3	4	-7	11	-18
	3	1	1	1	1	2
47	13	8	5	3	2	1

La identitat de Bézout és $13 \cdot (-18) + 47 \cdot 5 = 1$. Multiplicant per 10 i canviant de signe el coeficient de 47, i per tant també del 5, obtenim una solució particular de l'equació:

$$13 \cdot (-180) - 47 \cdot (-50) = 10$$

Per tant, la solució general és:

$$\begin{aligned} x &= -180 - (-47)t = -180 + 47t \\ y &= -50 + 13t \end{aligned}$$

on $t \in \mathbb{Z}$.

b) Busquem ara la solució (x, y) que tingui la y negativa més gran possible. Volem que $y < 0$; és a dir:

$$y < 0 \Leftrightarrow -50 + 13t < 0 \Leftrightarrow t < \frac{50}{13} \approx 3,8 \Leftrightarrow t \leq 3$$

l'última equivalència és certa perquè t és un enter. Ara bé la funció $f(t) = -50+13t$ és una funció estrictament creixent (per exemple, perquè la primera derivada és sempre positiva). Per tant, si $t_1 < t_2$, llavors $y_1 = -50 + 13t_1 < y_2 = -50 + 13t_2$. Per tant, el valor negatiu més gran de y s'obté per a $t = 3$ i és $y = -11$. El valor corresponent de la x quan $t = 3$ és $x = -39$.

Una altra solució: sabem que $y = -50 + 13t$, amb $t \in \mathbb{Z}$; és a dir $y \equiv -50 \equiv 2 \pmod{13}$. I l'enter negatiu més gran congruent amb 2 mòdul 13 és $2 - 13 = -11$, que correspon al valor de $t = 3$, obtenint que $x = -39$.

2.28 Examen de recuperació del primer parcial 12/06/2014

236

Pas base: per a $n = 0$, tenim:

$$\sum_{k=0}^{0} 2^k \cdot (2k+1) \cdot k! = 2^0 \cdot 1 \cdot 0! = 1$$

D'altra banda: $(0 + 1)! \cdot 2^{0+1} - 1 = 2 - 1 = 1$.

Pas inductiu: fixem un natural $m \geq 0$ i suposem que la propietat és certa per a m (hipòtesi d'inducció):

$$\sum_{k=0}^{m} 2^k \cdot (2k+1) \cdot k! = (m+1)! \cdot 2^{m+1} - 1$$

Volem demostrar que la propietat també és certa per l'enter $m + 1$; és a dir, volem demostrar que:

$$\sum_{k=0}^{m+1} 2^k \cdot (2k+1) \cdot k! = (m+2)! \cdot 2^{m+2} - 1$$

Tenim:

$$\begin{aligned}
\sum_{k=0}^{m+1} 2^k \cdot (2k+1) \cdot k! &= \sum_{k=0}^{m} 2^k \cdot (2k+1) \cdot k! + 2^{m+1}(2m+3)(m+1)! \\
&= ((m+1)! \cdot 2^{m+1} - 1) + 2^{m+1}(2m+3)(m+1)! \quad \text{(per H.I.)} \\
&= (m+1)! \cdot 2^{m+1}(2m+4) - 1 \\
&= (m+1)! \cdot 2^{m+1} \cdot 2 \cdot (m+2) - 1 \\
&= (m+2)! \cdot 2^{m+2} - 1
\end{aligned}$$

Pel principi d'inducció, la propietat és certa per a tot nombre natural $n \geq 0$.

237

a) Construïm les taules de veritat de les dues fórmules. Sabem que una fórmula proposicional és una tautologia si a la seva taula de veritat semper tenim el valor 1. Siguin:

$$\alpha \equiv ((p \vee q) \to r) \to ((p \to r) \vee (q \to r))$$
$$\beta \equiv ((p \to r) \vee (q \to r)) \to ((p \vee q) \to r)$$

Les taules són:

p	q	r	$p \vee q$	$p \vee q \to r$	$p \to r$	$q \to r$	$(p \to r) \vee (q \to r)$	α	β
0	0	0	0	1	1	1	1	1	1
0	0	1	0	1	1	1	1	1	1
0	1	0	1	0	1	0	1	1	0
0	1	1	1	1	1	1	1	1	1
1	0	0	1	0	0	1	1	1	0
1	0	1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	0	1	1
1	1	1	1	1	1	1	1	1	1

Observem que la fórmula α sempre té valor de veritat 1, mentre que β de vegades té el 0. Per tant, α és una tautologia i β no ho és.

b) Siguin $a, b, c \in \mathbb{Z}$ tals que $a + b = c$. Volem demostrar que a és parell o b és parell o c és parell. Ho fem per reducció a l'absurd. Suposem que la negació del que volem demostrar és certa. És a dir, suposem que a és senar i b és senar i c és senar. Llavors la suma $a + b$ és un nombre parell i tenim una contradicció.

2.29 Examen de recuperació del segon parcial 12/06/2014

238

a) Per a tot $(x, y), (a, b), (c, d) \in \mathbb{R}^2$, es compleix:

- $(x, y)S(x, y)$, ja que $x + y = x + y$; per tant, S és reflexiva.
- Si $(x, y)S(a, b)$, llavors $x + y = a + b$ i, per tant, $(a, b)S(x, y)$. És a dir, S és simètrica.
- Si $(x, y)S(a, b)$ i $(a, b)S(c, d)$, llavors tenim que $x + y = a + b$ i $a + b = c + d$; per tant, $x + y = c + d$ i conseqüentment $(x, y)S(c, d)$. Per tant, S és transitiva.

b) Tenim:

$$[(3, 1)] = \{(x, y) \in \mathbb{R}^2 : (x, y)S(3, 1)\} = \{x, y) \in \mathbb{R}^2 : x + y = 3 + 1 = 4\}$$

Per tant, la classe d'equivalència de $(3, 1)$ està formada pels punts (x, y) de $\mathbb{R}^2$ que satisfan $x + y = 4$. És a dir, $[(3, 1)]$ és la recta d'equació $x + y = 4$.

c) En general, la classe d'equivalència de (a,b) és la recta d'equació $x+y=a+b$. D'altra banda, el conjunt D és la recta d'equació $y=x$. Per tant, hem de demostrar que la recta $y=x$ talla la recta $x+y=a+b$ en un punt. Però si resolem el sistema d'equacions, tenim que $x=y=(a+b)/2$. És a dir, per a cada classe $[(a,b)]$, la intersecció amb el conjunt D és:

$$D \cap [(a,b)] = \left\{ \left(\frac{a+b}{2}, \frac{a+b}{2} \right) \right\}$$

239

a) Hem de demostrar que per a tot $(x,y),(x',y') \in \mathbb{R}^2$, si $f(x,y)=f(x',y')$, llavors $(x,y)=(x',y')$. Tenim:

$$\begin{aligned} f(x,y)=f(x',y') &\Rightarrow (x+y,x-y)=(x'+y',x'-y') \\ &\Rightarrow x+y=x'+y' \ \wedge \ x-y=x'-y' \qquad (1) \\ &\Rightarrow 2x=2x' \ \wedge \ 2y=2y' \\ &\Rightarrow x=x' \ \wedge \ y=y' \end{aligned}$$

(1): sumant i restant terme a terme.

Per tant, f és injectiva.

b) Hem de demostrar que per a tot $(z,t)\in\mathbb{R}^2$, existeix $(x,y)\in\mathbb{R}^2$ tal que $f(x,y)=(z,t)$. Plantegem l'equació $f(x,y)=(z,t)$ i aïllem x,y en funció de z,t:

$$\begin{aligned} x+y&=z \\ x-y&=t \end{aligned}$$

Sumant i restant terme a terme, obtenim $2x=z+t$ i $2y=z-t$; per tant: $x=(z+t)/2$ i $y=(z-t)/2$. Conclusió: donat $(z,t)\in\mathbb{R}^2$, tenim que:

$$f\left(\frac{z+t}{2},\frac{z-t}{2}\right)=(z,t)$$

Per tant, f és exhaustiva. *Observació*: com que donat (z,t) hi ha solució *única* en (x,y), deduïm que f, a més, és injectiva.

c) Dels dos apartats anteriors, deduïm que f és una aplicació bijectiva (és injectiva i exhaustiva). Per tant, f té inversa. L'aplicació inversa f^{-1} satisfà, per definició:

$$f^{-1}(z,t)=(x,y) \Leftrightarrow f(x,y)=(z,t)$$

Per tant, plantegem l'equació $f(x,y)=(z,t)$ i aïllem x,y en funció de z,t. De l'apartat anterior, tenim que $x=(z+t)/2$ i $y=(z-t)/2$; és a dir:

$$f^{-1}(z,t)=\left(\frac{z+t}{2},\frac{z-t}{2}\right)$$

d) Per a calcular $f^{-1}(6,2)$ podem substituir $(6,2)$ a la fórmula que obtingut de f^{-1}:

$$f^{-1}(6,2)=\left(\frac{6+2}{2},\frac{6-2}{2}\right)=(4,2)$$

2.30 Examen final de reavaluació 11/07/2014

240

1) Tenim, per hipòtesi, que, per a qualsevol $x \in X$, si $A(x)$ és certa, és a dir, si $x \in U$, llavors també $B(x)$ és certa, és a dir, $x \in V$. Per tant, tenim que $U \subseteq V$.

2) Demostrem el contrarecíproc:

$$f(a) = 0 \Rightarrow a^3 + a = 0 \Rightarrow a(a^2 + 1) = 0 \Rightarrow a = 0,$$

donat que $a^2 + 1$ no s'anul·la a $\mathbb{R}$.

3) Passem a $\mathbb{Z}_7$. Escrivim $n = 3k$, amb $k \in \mathbb{N}$:

$$\overline{15} \cdot \overline{2}^{3k} = \overline{1} \cdot \left(\overline{2}^3\right)^k = \overline{1} \cdot \overline{1}^k = \overline{1}.$$

241

1) Si a, b, c són elements qualssevol de A:

$$aRb \wedge bRc \Rightarrow aRc \Rightarrow cRa.$$

La primera implicació perquè R és transitiva i la segona perquè R és simètrica.

2) Si a, b són elements qualssevol de A:

$$aRb \Rightarrow aRb \wedge bRb \Rightarrow bRa.$$

La primera implicació perquè R és reflexiva i la segona perquè R és circular.

3) Per 2) és simètrica, per tant és suficient amb provar que és transitiva. Si a, b, c són elements qualssevol de A:

$$aRb \wedge bRc \Rightarrow cRa \Rightarrow aRc.$$

La primera implicació perquè R és circular i la segona perquè R és simètrica.

242

1) El sistema té solució en x si, i només si, existeixen $r, s \in \mathbb{Z}$ tals que $x = a+mr = b+ns$ i l'equació diofàntica $ns-mr = a-b$ té solució si i només si $d \mid a-b$, on $d = \text{mcd}(m, n)$.

2) Si apliquem el resultat de 1), i donat que $d = \text{mcd}(12, 14) = 2$, tenim que el sistema té solució si, i només si, $2 \mid 1 - b$, la qual cosa equival evidentment a que b sigui de la forma $b = 1 + 2t$, $t \in \mathbb{Z}$; és a dir, que b sigui senar.

3) El sistema té solució perquè 17 és senar. Resolem $1+12r = 17+14s$, és a dir $6r-7s = 8$. Passant a $\mathbb{Z}_6$, tenim: $-\overline{s} = \overline{2}$, d'on $\overline{s} = -\overline{2} = \overline{4}$, i s és de la forma $s = 4 + 6t$, $t \in \mathbb{Z}$.

   Finalment, les x solució del sistema són: $x = 17 + 14s = 17 + 14(4 + 6t) = 73 + 84t$, $t \in \mathbb{Z}$.

2.31 Examen parcial 16/10/2014

243

a) Hi ha diverses maneres de formalitzar aquesta proposició. En primer lloc, per a indicar que l'enter x és múltiple de 4, podem escriure '$4 \mid x$' o bé usar un predicat com ara $Q(x)$: 'x és múltiple de 4'. Per a les variables quantificades, podem indicar que l'univers de discurs és el conjunt dels enters o bé expressar directament que són elements de $\mathbb{Z}$. Aquí hi ha algunes solucions:

- $\forall m, n\,(4 \mid (m-n) \to 4 \mid (m^2-n^2))$
- $\forall m, n\,(Q(m-n) \to Q(m^2-n^2))$
- $\forall m, n \in \mathbb{Z}\,(4 \mid (m-n) \to 4 \mid (m^2-n^2))$
- $\forall m, n \in \mathbb{Z}\,(Q(m-n) \to Q(m^2-n^2))$

b) Si usem la tercera expressió de l'apartat anterior, obtenim:

$$\neg\forall m, n \in \mathbb{Z}\,(4 \mid (m-n) \to 4 \mid (m^2-n^2)) \equiv \exists m, n \in \mathbb{Z}\,(4 \mid (m-n) \wedge 4 \nmid (m^2-n^2))$$

c) Farem una demostració directa. Siguin m, n nombres enters tals que $m-n$ és múltiple de 4. Volem demostrar que m^2-n^2 també és múltiple de 4.

$$\begin{aligned} 4 \mid (m-n) &\Leftrightarrow \exists k \in \mathbb{Z}\,(m-n=4k) && \text{(per definició)} \\ &\Rightarrow m^2-n^2=(m+n)(m-n)=(m+n)\cdot 4k && \text{(per hipòtesi)} \\ &\Rightarrow m^2-n^2=4\cdot((m+n)k) \end{aligned}$$

Per tant, m^2-n^2 és també un múltiple de 4.

d) Per a demostrar que R és falsa, hem de provar que la seva negació és certa. És a dir, hem de provar que *existeixen* enters m, n tals que m^2-n^2 *és* múltiple de 4, però $m-n$ *no és* múltiple de 4; és a dir, un contraexemple. Provant per a diversos valors petits de m i n trobem, per exemple, que $m=4$ i $n=2$ funcionen. En efecte, si $m=4$ i $n=2$, llavors $m-n=2$, que no és múltiple de 4, i $m^2-n^2=4^2-2^2=16-4=12$, que sí és múltiple de 4.

244

Tenim:

$$\sum_{k=-n}^{n}(3k+5)=3\cdot\sum_{k=-n}^{n}k+\sum_{k=-n}^{n}5$$

La primera suma es pot expressar així:

$$3\cdot\sum_{k=-n}^{n}k=3\cdot\left(\sum_{k=-n}^{-1}k+\sum_{k=1}^{n}k\right)=3\cdot\sum_{k=1}^{n}(-k+k)=3\cdot 0=0$$

i la segona és:

$$\sum_{k=-n}^{n}5=5(2n+1)$$

Per tant, hem de resoldre l'equació $5(2n+1) = 1005$ i la solució és $n = 100$.

Solució 2: Una altra manera és aplicar la fórmula de la suma de termes consecutius d'una progressió aritmètica. La successió $a_k = 3k+5$ és una progressió aritmètica de diferència 5. Per tant, la suma que hem de calcular és la suma de $2n+1$ termes consecutius d'aquesta progressió amb primer terme igual a $-3n+5$ i últim terme igual a $3n+5$. Per tant:

$$\sum_{k=-n}^{n}(3k+5) = \frac{((-3n+5)+(3n+5))(2n+1)}{2} = \frac{10(2n+1)}{2} = 5(2n+1) = 1005$$

d'on obtenim que $n = 100$.

2.32 Examen parcial 17/11/2014

245

a) Una relació és d'equivalència si és reflexiva, simètrica i transitiva.

- R és reflexiva. Sigui $A \in \mathcal{P}(X)$. Per definició $A\,R\,A$ si, i només si, $A \cup Y = A \cup Y$, que és cert. Per tant, R és reflexiva.
- R és simètrica. Siguin $A, B \in \mathcal{P}(X)$. Si $A\,R\,B$, llavors $A \cup Y = B \cup Y$; per tant, $B \cup Y = A \cup Y$. És a dir, $B\,R\,A$.
- R és transitiva. Siguin $A, B, C \in \mathcal{P}(X)$. Si $A\,R\,B$ i $B\,R\,C$, llavors $A \cup Y = B \cup Y$ i $B \cup Y = C \cup Y$. Per tant, $A \cup Y = C \cup Y$ i això vol dir que $A\,R\,C$.

b) Escrivim, en primer lloc, el conjunt $\mathcal{P}(X)$:

$$\begin{aligned}\mathcal{P}(X) = \{&\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{1,3\}, \{1,4\}, \{2,3\}, \{2,4\}, \{3,4\},\\ &\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \{1,2,3,4\}\}\end{aligned}$$

Per definició de classe d'equivalència, si $A \in \mathcal{P}(X)$, llavors:

$$[A] = \{B \in \mathcal{P}(X) : B\,R\,A\} = \{B \in \mathcal{P}(X) : B \cup \{4\} = A \cup \{4\}\}$$

Tenim:

$$\begin{aligned}
[\emptyset] &= \{B : B \cup \{4\} = \emptyset \cup \{4\} = \{4\}\} = \{\emptyset, \{4\}\}\\
[\{1\}] &= \{B \in \mathcal{P}(X) : B \cup \{4\} = \{1\} \cup \{4\} = \{1,4\}\} = \{\{1\}, \{1,4\}\}\\
[\{2\}] &= \{B \in \mathcal{P}(X) : B \cup \{4\} = \{2\} \cup \{4\} = \{2,4\}\} = \{\{2\}, \{2,4\}\}\\
[\{3\}] &= \{B \in \mathcal{P}(X) : B \cup \{4\} = \{3\} \cup \{4\} = \{3,4\}\} = \{\{3\}, \{3,4\}\}\\
[\{1,2\}] &= \{B \in \mathcal{P}(X) : B \cup \{4\} = \{1,2\} \cup \{4\} = \{1,2,4\}\} = \{\{1,2\}, \{1,2,4\}\}\\
[\{1,3\}] &= \{B \in \mathcal{P}(X) : B \cup \{4\} = \{1,3\} \cup \{4\} = \{1,3,4\}\} = \{\{1,3\}, \{1,3,4\}\}\\
[\{2,3\}] &= \{B \in \mathcal{P}(X) : B \cup \{4\} = \{2,3\} \cup \{4\} = \{2,3,4\}\} = \{\{2,3\}, \{2,3,4\}\}\\
[\{1,2,3\}] &= \{B \in \mathcal{P}(X) : B \cup \{4\} = \{1,2,3\} \cup \{4\} = \{1,2,3,4\}\} = \{\{1,2,3\}, \{1,2,3,4\}\}
\end{aligned}$$

És a dir, hi ha tantes classes d'equivalència com subconjunts de $\{1,2,3\}$, és a dir, tantes com elements de $\mathcal{P}(\{1,2,3\})$.

c) Per definició, el conjunt quocient és el conjunt que té per elements les classes d'equivalència. En aquest cas, el conjunt quocient té exactament 8 elements:

$$\mathcal{P}(X)/R = \{[A] : A \in \mathcal{P}(X)\} = \{[\emptyset], [\{1\}], [\{2\}], [\{3\}], [\{1,2\}], [\{1,3\}], [\{2,3\}], [\{1,2,3\}]\}$$

246

Cas base $n = 2$. Tenim:

$$\prod_{k=2}^{2}\left(1-\frac{1}{k^2}\right) = 1-\frac{1}{2^2} = \frac{3}{4}$$

que és igual a $\dfrac{1+2}{2\cdot 2}$. Per tant, la propietat és certa per a $n = 2$.

Pas inductiu. Fixem un enter $n \geq 2$ i suposem que la propietat és certa per a n:

$$\prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right) = \frac{1+n}{2n} \qquad \text{(hipòtesi d'inducció)}$$

Volem demostrar que la propietat és certa per a l'enter $n+1$; és a dir, volem veure que:

$$\prod_{k=2}^{n+1}\left(1-\frac{1}{k^2}\right) = \frac{2+n}{2(n+1)}$$

Tenim:

$$\begin{aligned}
\prod_{k=2}^{n+1}\left(1-\frac{1}{k^2}\right) &= \prod_{k=2}^{n}\left(1-\frac{1}{k^2}\right)\cdot\left(1-\frac{1}{(n+1)^2}\right)\\
&= \frac{1+n}{2n}\cdot\left(1-\frac{1}{(n+1)^2}\right) \qquad \text{(per hipòtesi d'inducció)}\\
&= \frac{(1+n)((n+1)^2-1)}{2n(n+1)^2}\\
&= \frac{n(n+1)(n+2)}{2n(n+1)^2}\\
&= \frac{n+2}{2(n+1)}
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot enter $n \geq 2$.

2.33 Examen final 14/01/2015

247

a) Tenim $f[A] = \{f(\overline{1}), f(\overline{3}), f(\overline{22}), f(\overline{43}) = \{\overline{3}, \overline{7}, \overline{45}\}$, perquè: $f(\overline{1}) = \overline{2} \cdot \overline{1} + \overline{1} = \overline{3}$; $f(\overline{3}) = \overline{2} \cdot \overline{3} + \overline{1} = \overline{7}$; $f(\overline{22}) = \overline{2} \cdot \overline{22} + \overline{1} = \overline{45}$; $f(\overline{43}) = \overline{2} \cdot \overline{43} + \overline{1} = \overline{7}$. D'altra banda, per a calcular $f^{-1}[B]$, hem de resoldre les equacions $\overline{2} \cdot \overline{x} + \overline{1} = \overline{3}$ i $\overline{2} \cdot \overline{x} + \overline{1} = \overline{50}$. Tenim: $\overline{2} \cdot \overline{x} + \overline{1} = \overline{3} \Leftrightarrow \overline{2} \cdot \overline{x} = \overline{2}$. Però com que $\text{mcd}(2, 80) = 2 \neq 1$, no podem simplificar el coeficient $\overline{2}$ (la classe $\overline{2}$ no té inversa a $\mathbb{Z}_{80}$). No obstant, podem escriure aquesta igualtat en forma de congruència i tenim:

$$\overline{2} \cdot \overline{x} = \overline{2} \Leftrightarrow 2x \equiv 2 \pmod{80} \Leftrightarrow x \equiv 1 \pmod{40}$$

Per tant, les solucions de $\overline{2} \cdot \overline{x} = \overline{2}$ són $\overline{x} = \overline{1}$ i $\overline{x} = \overline{41}$ (perquè 1 i 41 són els únics enters entre 0 i 79 que són congruents amb 1 mòdul 40). Per tant: $f^{-1}[\{\overline{3}\}] = \{\overline{1}, \overline{41}\}$.

Considerem ara l'equació $\overline{2} \cdot \overline{x} + \overline{1} = \overline{50}$:

$$\overline{2} \cdot \overline{x} + \overline{1} = \overline{50} \Leftrightarrow \overline{2} \cdot \overline{x} = \overline{49} \Leftrightarrow 2x \equiv 49 \pmod{80} \equiv \exists y \in \mathbb{Z}\, (2x + 80y = 49)$$

Però aquesta última equació diofàntica no té solució perquè $\text{mcd}(2, 80) = 2 \nmid 49$.

Per tant: $f^{-1}[B] = \{\overline{1}, \overline{41}\}$.

b) A l'apartat anterior hem vist que $f(\overline{3}) = f(\overline{43}) = \overline{7}$. Per tant, f no és injectiva. També hem comprovat que la classe $\overline{50}$ no té antiimatge. Per tant, f no és exhaustiva.

c) Tenim: $A \cap f^{-1}[B] = \{\overline{1}, \overline{3}, \overline{22}, \overline{43}\} \cap \{\overline{1}, \overline{41}\} = \{\overline{1}\}$, $f[A \cap f^{-1}[B]] = f[\{\overline{1}\}] = \{\overline{3}\}$. D'altra banda $f[A] \cap B = \{\overline{3}, \overline{7}, \overline{45}\} \cap \{\overline{3}, \overline{50}\} = \{\overline{3}\}$.

248 En primer lloc, $21456 \equiv 44 \pmod{101}$. En segon lloc, observem que 101 és un nombre primer (perquè no és divisible per $2, 3, 5, 7$, que són els primers més petits o igual que $\sqrt{101}$). Per tant, podem aplicar el teorema de Fermat: si $101 \nmid a$, llavors $a^{101-1} = a^{100} \equiv 1 \pmod{101}$. Ara dividim l'exponent 16140 entre 100: $16140 = 100 \cdot 161 + 40$. Resumint, tenim:

$$21456^{16140} \equiv 44^{16140} \equiv (44^{100})^{161} \cdot 44^{40} \equiv 1 \cdot 44^{40} \pmod{101}$$

Ara hem d'escriure l'exponent 40 en base 2: $40 = 2^5 + 2^3$. Posem $b_0 = 44$ i calculem $b_i \equiv b_{i-1}^2$, per a $i = 1, \ldots, 5$:

$$b_0 = 44,\ b_1 \equiv 44^2 \equiv 17,\ b_2 \equiv 17^2 \equiv 87,\ b_3 \equiv 87^2 \equiv 95,\ b_4 \equiv 95^2 \equiv 36,\ b_5 \equiv 36^2 \equiv 84$$

Finalment: $44^{40} \equiv b_5 \cdot b_3 \equiv 84 \cdot 95 \equiv 1 \pmod{101}$. És a dir: $21456^{16140} \equiv 1 \pmod{101}$.

249

a) Suposem que $a \equiv b \pmod{pq}$. Per definició, tenim que $pq \mid (a - b)$. Però $p \mid pq$ i, per la propietat transitiva de la relació de divisibilitat, deduïm que $p \mid (a - b)$. De la mateixa manera, obtenim que $q \mid (a - b)$. Per tant $a \equiv b \pmod{p}$ i $a \equiv b \pmod{q}$. Recíprocament, suposem que $a \equiv b \pmod{p}$ i $a \equiv b \pmod{q}$. Llavors, per definició, tenim que $p \mid (a - b)$ i $q \mid (a - b)$. Per una propietat del mínim comú múltiple, obtenim que $\text{mcm}(p, q) \mid (a - b)$. Però com que p i q són primers, $\text{mcm}(p, q) = pq$.

b) Sigui p un primer senar. Si $x^2 \equiv 4 \pmod{p}$, llavors $p \mid (x^2-4) = (x-2)(x+2)$. Pel lema d'Euclides, $p \mid (x-2)$ o $p \mid (x+2)$. Per tant, $x \equiv 2 \pmod{p}$ o $x \equiv -2 \pmod{p}$. D'altra banda, és obvi que $x \equiv 2$ i $x \equiv -2$ són solucions de la congruència.

c) Observem que $35 = 5 \cdot 7$ i que 5 i 7 són primers senars. Pel primer apartat, tenim que $x^2 \equiv 4 \pmod{35}$ és equivalent a $x^2 \equiv 4 \pmod{5}$ i $x^2 \equiv 4 \pmod{7}$. Pel segon apartat, les solucions de $x^2 \equiv 4 \pmod{5}$ són $x \equiv 2 \pmod{5}$ i $x \equiv -2 \pmod{5}$ i les solucions de $x^2 \equiv 4 \pmod{7}$ són $x \equiv 2 \pmod{7}$ i $x \equiv -2 \pmod{7}$. Per tant, les solucions de la congruència $x^2 \equiv 4 \pmod{35}$ són les solucions dels sistemes xinesos següents:

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \quad \begin{cases} x \equiv 2 \pmod{5} \\ x \equiv -2 \pmod{7} \end{cases} \quad \begin{cases} x \equiv -2 \pmod{5} \\ x \equiv 2 \pmod{7} \end{cases} \quad \begin{cases} x \equiv -2 \pmod{5} \\ x \equiv -2 \pmod{7} \end{cases}$$

Cada sistema té solució única, perquè els mòduls són primers entre ells. Per tant, hi ha 4 solucions. El primer i últim sistemes tenen per solució $x \equiv 2 \pmod{35}$ i $x \equiv -2 \pmod{35}$, respectivament. Resolem els altres dos.

a_i	2	-2
m_i	5	7
M_i	7	5
y_i	3	3

a_i	-2	2
m_i	5	7
M_i	7	5
y_i	3	3

Per tant, la solució del segon sistema (primera taula) és $x = a_1M_1y_1 + a_2M_2y_2 = 12 \pmod{35}$ i la solució del tercer sistema (segona taula) és $x = a_1M_1y_1 + a_2M_2y_2 = 23 \pmod{35}$

2.34 Examen de recuperació del primer parcial 14/01/2015

250

1) Sigui $n \in \mathbb{N}$.

($\Rightarrow$) Suposem que n és parell. Volem demostrar que n^3 és parell. Si n és parell, llavors $n = 2k$, per a algun $k \in \mathbb{N}$. Aleshores $n^3 = (2k)^3 = 8k^3$, que és parell. (Demostració directa.)

($\Leftarrow$) Demostrem el contrarecíproc: si n és senar, llavors n^3 és senar. Suposem que n és senar. Llavors $n = 2k+1$, per a cert $k \in \mathbb{N}$. Llavors $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, que és senar.

2) Per reducció a l'absurd. Suposem que $\sqrt[3]{2}$ és racional. Podem escriure $\sqrt[3]{2} = a/b$, on $a, b \in \mathbb{N}$, $b \neq 0$ i $\mathrm{mcd}(a,b) = 1$ (fracció irreductible). Llavors $2b^3 = a^3$, d'on deduïm que a^3 és parell. Per l'apartat anterior, a és parell. Per tant, $a = 2k$, amb $k \in \mathbb{N}$. Elevant al cub, substituint i simplificant, obtenim: $b^3 = 4k^3$. Per tant, b^3 també és parell i, també per l'apartat anterior, b és parell. Ara tenim que a i b són parells i d'altra banda $\mathrm{mcd}(a,b) = 1$, per hipòtesi. Contradicció. Per tant, $\sqrt[3]{2}$ és irracional.

251 La proposició "Hi ha un nombre natural que és més petit o igual que tots els nombres naturals" es pot formalitzar així: $\exists x\,\forall y\,(x \leq y)$, on s'entén que l'univers de discurs és $\mathbb{N}$. També podem escriure: $\exists x \in \mathbb{N}\,\forall y \in \mathbb{N}\,(x \leq y)$.

La negació és:

$$\neg\exists x\,\forall y\,(x \leq y) \equiv \forall x\,\neg\forall y\,(x \leq y) \equiv \forall x\,\exists y\,\neg(x \leq y) \equiv \forall x\,\exists y\,(x > y)$$

2.35 Examen de recuperació del segon parcial 14/01/2015

252

a) Provem que R és d'equivalència.

- R és reflexiva: per a tot $A \in \mathcal{P}(X)$, tenim que $|A| = |A|$; per tant, ARA.
- R és simètrica: si $A, B \in \mathcal{P}(X)$ i ARB, llavors $|A| = |B|$ i per tant $|B| = |A|$; és a dir BRA.
- R és transitiva: si $A, B, C \in \mathcal{P}(X)$ i ARB i BRC, llavors $|A| = |B|$ i $|B| = |C|$. Per tant, $|A| = |C|$; és a dir ARC.

b) Siguin $X = \{1, 2, 3, 4, 5\}$ i $A = \{1, 3, 4, 5\}$. Llavors:

$$[A] = \{B \in \mathcal{P}(X) : BRA\} = \{B \in \mathcal{P}(X) : |B| = |A| = 4\}$$

És a dir, els elements de la classe de A són els subconjunts de X de cardinal 4:

$$[A] = \{\{1, 2, 3, 4\}, \{1, 2, 3, 5\}, \{1, 2, 4, 5, \}, \{1, 3, 4, 5\}, \{2, 3, 4, 5\}\}$$

c) El conjunt quocient $\mathcal{P}(X)/R$ és:

$$\mathcal{P}(X)/R = \{[A] : A \in \mathcal{P}(X)\}$$

Com que dos subconjunts de X estan relacionats si tenen el mateix nombre d'elements, per a cada possible cardinal hi ha una classe d'equivalència. Per tant, el conjunt quocient té $n + 1$ classes d'equivalència, una per a cada cardinal k tal que $0 \leq k \leq n$.

253 Ho provem per inducció sobre $n \geq 1$.

Pas base: $n = 1$. Tenim: $\sum_{k=1}^{1} k5^k = 5$ i d'altra banda $(5 + (4n - 1)5^{n+1})/16 = 5$, si $n = 1$.

Pas inductiu: suposem que $n \geq 1$ i que:

$$\sum_{k=1}^{n} k5^k = \frac{5 + (4n - 1)5^{n+1}}{16} \qquad \text{(hipòtesi d'inducció)}$$

Volem demostrar que:

$$\sum_{k=1}^{n+1} k5^k = \frac{5+(4n+3)5^{n+2}}{16}$$

Tenim:

$$\begin{aligned}
\sum_{k=1}^{n+1} k5^k &= \sum_{k=1}^{n} k5^k + (n+1)5^{n+1} \\
&= \frac{5+(4n-1)5^{n+1}}{16} + (n+1)5^{n+1} && \text{per H.I.} \\
&= \frac{5+(4n-1)5^{n+1}+16(n+1)5^{n+1}}{16} \\
&= \frac{5+(20n+15)5^{n+1}}{16} \\
&= \frac{5+5(4n+3)5^{n+1}}{16} \\
&= \frac{5+(4n+3)5^{n+2}}{16}
\end{aligned}$$

Pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

2.36 Examen parcial 23/03/2015

259

a) Si prenem l'univers de discurs com a el conjunt dels nombres enters $\mathbb{Z}$, llavors podem escriure:

$$\forall x \left(\frac{x}{2} \in \mathbb{Z} \vee \frac{x}{2} + \frac{1}{2} \in \mathbb{Z} \right)$$

b) Per tant, la seva negació serà:

$$\neg\forall x \left(\frac{x}{2} \in \mathbb{Z} \vee \frac{x}{2} + \frac{1}{2} \in \mathbb{Z} \right) \equiv \exists x \left(\frac{x}{2} \notin \mathbb{Z} \wedge \frac{x}{2} + \frac{1}{2} \notin \mathbb{Z} \right)$$

c) El mètode de reducció a l'absurd comença suposant que la proposició que volem demostrar és falsa. És a dir, la hipòtesi que s'ha de plantejar és:

$$\exists x \left(\frac{x}{2} \notin \mathbb{Z} \wedge \frac{x}{2} + \frac{1}{2} \notin \mathbb{Z} \right)$$

d) Fem una prova directa. Sigui $x \in \mathbb{Z}$. Volem demostrar que o bé $x/2$ és un enter o bé que $x/2 + 1/2$ és un enter. Com que el que volem demostrar és una disjunció, neguem una de les clàusules i provem l'altra. Suposem doncs que $x/2$ *no* és un enter. Això és equivalent a dir que x és un nombre senar. Per tant, existeix un enter k tal que $x = 2k + 1$. Ara tenim:

$$\frac{x}{2} + \frac{1}{2} = \frac{2k+1+1}{2} = \frac{2k+2}{2} = k + 1 \in \mathbb{Z},$$

com volíem demostrar.

També podem fer una demostració per casos, depenent de la paritat de l'enter x. Cas que x sigui parell: llavors existeix un enter k tal que $x = 2k$. En aquesta situació, tenim que $x/2 = k \in \mathbb{Z}$. Cas que x sigui senar: llavors existeix un enter k tal que $x = 2k + 1$. En aquest cas, tenim que $x/2 + 1/2 = (2k + 2)/2 = k + 1 \in \mathbb{Z}$.

260 **Pas inicial:** $n = 2$. Efectivament, tenim d'una banda:

$$\sum_{i=2}^{2} \frac{1}{i^2 - 1} = \frac{1}{3}$$

i d'altra banda, si $n = 2$:

$$\frac{(n-1)(3n+2)}{4n(n+1)} = \frac{1}{3}$$

Pas d'inducció: fixem un enter $n \geq 2$ i suposem (hipòtesi d'inducció) que:

$$\sum_{i=2}^{n} \frac{1}{i^2 - 1} = \frac{(n-1)(3n+2)}{4n(n+1)}.$$

Volem demostrar que:

$$\sum_{i=2}^{n+1} \frac{1}{i^2 - 1} = \frac{n(3n+5)}{4(n+1)(n+2)}.$$

Tenim:

$$\begin{aligned}
\sum_{i=2}^{n+1} \frac{1}{i^2 - 1} &= \sum_{i=2}^{n} \frac{1}{i^2 - 1} + \frac{1}{(n+1)^2 - 1} \\
&= \frac{(n-1)(3n+2)}{4n(n+1)} + \frac{1}{(n+1)^2 - 1} && \text{per hip. d'inducció} \\
&= \frac{(n-1)(3n+2)}{4n(n+1)} + \frac{1}{n(n+2)} \\
&= \frac{(n-1)(3n+2)(n+2)}{4n(n+1)(n+2)} + \frac{4(n+1)1}{4n(n+1)(n+2)} \\
&= \frac{3n^3 + 5n^2}{4n(n+1)(n+2)} \\
&= \frac{n^2(3n+5)}{4n(n+1)(n+2)} \\
&= \frac{n(3n+5)}{4(n+1)(n+2)}
\end{aligned}$$

Pel principi d'inducció, la propietat és certa per a tot $n \geq 2$.

2.37 Examen parcial 11/05/2015

261

1) Com que $A \subseteq B$, tenim que $A \cap B = A$. Per tant, $A = \{1\}$ i $1 \in B$. A més, es demana que $A \in B$. Per tant $B = \{1, \{1\}\}$ i $A = \{1\}$ és una possible solució.

2) Sigui $x \in C$. Tenim:

$$\begin{aligned} x \in (C \setminus B) \cup (B \setminus A) &\Leftrightarrow (x \in C \wedge x \notin B) \vee (x \in B \wedge x \notin A) \\ &\Leftrightarrow (x \in C \vee x \in B) \wedge (x \in C \vee x \notin A) \wedge \\ &\quad\ (x \notin B \vee x \in B) \wedge (x \notin B \vee x \notin A) \end{aligned}$$

Ara bé: $x \in C \vee x \in B$ és equivalent a $x \in C$, ja que $B \subseteq C$; $x \in C \vee x \notin A$ és, per definició, equivalent a $x \in C \setminus A$; $x \notin B \vee x \in B$ és sempre cert; i $x \notin B \vee x \notin A$ és equivalent a $x \notin A$, ja que $A \subseteq B$. Per tant, hem vist:

$$x \in (C \setminus B) \cup (B \setminus A) \Leftrightarrow x \in C \setminus A.$$

3) Siguin $X = \{1, 2, 3, 4\}$ i $M = \{1, 2\}$.

   a) $\mathcal{P}(X) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{4\}, \{1, 2\}, \{1, 3\}, \{1, 4\}, \{2, 3\}, \{2, 4\}, \{3, 4\}, \{1, 2, 3\}, \{1, 2, 4\}, \{1, 3, 4\}, \{2, 3, 4\}, X\}$.

   b) Observem que $f(A) = A \cap M \subseteq M$, per a tot $A \in \mathcal{P}(X)$. Per tant, f no pot ser ni injectiva ni exhaustiva. Per exemple: $f(\{1\}) = f(\{1, 3\}) = \{1\}$. Per tant, no és injectiva. A més, no hi ha cap $A \in \mathcal{P}(X)$ tal que $f(A) = \{4\}$, per exemple, ja que $\{4\}$ no és un subconjunt de M.

262

1) **Reflexiva.** Tenim que $a - 1/a = a - 1/a$. Per tant $a\,R\,a$.

   Simètrica. Si $a\,R\,b$, llavors $a - 1/a = b - 1/b$. Per tant, $b - 1/b = a - 1/a$ i això vol dir que $b\,R\,a$.

   Transitiva. Si $a\,R\,b$ i $b\,R\,c$, llavors $a - 1/a = b - 1/b$ i $b - 1/b = c - 1/c$. Per tant, $a - 1/a = c - 1/c$ i això vol dir que $a\,R\,c$.

   Per tant, R és una relació d'equivalència.

2) Tenim:

$$\begin{aligned} a\,R\,b \Leftrightarrow a - \frac{1}{a} = b - \frac{1}{b} &\Leftrightarrow \frac{a^2 - 1}{a} = \frac{b^2 - 1}{b} \\ &\Leftrightarrow b(a^2 - 1) = a(b^2 - 1) \Leftrightarrow ba^2 - ab^2 - b + a = 0 \\ &\Leftrightarrow (a - b)ab + (a - b) = 0 \Leftrightarrow (a - b)(ab + 1) = 0 \end{aligned}$$

3) Per definició:

$$[a] = \{x \in \mathbb{R} - \{0\} : x\,R\,a\}$$

Però acabem de demostrar a l'apartat anterior que si $x\,R\,a$, llavors $(x-a)(xa+1)=0$. Per tant, tenim que o bé $x=a$ o bé $xa+1=0$. És a dir, $x=a$ o $x=-1/a$. Comprovem ara que $(-1/a)\,R\,a$:

$$(-1/a)-\frac{1}{-1/a}=-\frac{1}{a}+a$$

Conclusió:

$$[a]=\{a,-1/a\}$$

4) El conjunt quocient és el conjunt format per les classes d'equivalència:

$$(\mathbb{R}-\{0\})/R=\{[a]:a\in\mathbb{R}-\{0\}\}=\{\{a,-1/a\}:a\in\mathbb{R}-\{0\}\}.$$

2.38 Examen final 09/06/2015

263 En primer lloc, observem que els mòduls son primers entre ells dos a dos. Per tant, el sistema de congruències té solució, que és única mòdul $7\cdot 8\cdot 9\cdot 11=5544$. Una possible solució ve donada per la fórmula:

$$x=\sum_{i=1}^{4}M_iy_ia_i$$

on $m_1=7$, $m_2=8$, $m_3=9$, $m_4=11$; $M_i=\prod_{j\neq i}m_j$; $M_iy_i\equiv 1 \pmod{m_i}$, per a $i=1,\dots,4$; i $a_1=5$, $a_2=12\equiv 4 \pmod 8$, $a_3=13\equiv 4 \mod 9$ i $a_4=16\equiv 5 \pmod{11}$. Per a calcular els y_i, apliquem l'algorisme d'Euclides i escrivim la corresponent identitat de Bézout dels parells (M_i,m_i), $i=1,\dots,4$. Tenim:

m_i	M_i	y_i	a_i	$M_iy_ia_i$
7	792	1	5	3960
8	693	5	4	13860
9	616	7	4	17248
11	504	5	5	12600

Els càlculs dels y_i és com segueix:

$$\begin{aligned}
&792y_1\equiv 1 \pmod 7 \Leftrightarrow y_1\equiv 1 \pmod 7\\
&693y_2\equiv 1 \pmod 8 \Leftrightarrow 5y_2\equiv 1 \pmod 8 \Leftrightarrow y_2\equiv 5 \pmod 8\\
&616y_3\equiv 1 \pmod 9 \Leftrightarrow 4y_3\equiv 1 \pmod 9 \Leftrightarrow y_3\equiv 7 \pmod 9\\
&504y_4\equiv 1 \pmod{11} \Leftrightarrow 9y_4\equiv 1 \pmod{11} \Leftrightarrow y_4\equiv 5 \pmod{11}
\end{aligned}$$

Finalment, tenim:

$$x=\sum_{i=1}^{4}M_iy_ia_i=47668\equiv 3316 \pmod{5544}$$

Per tant, l'enter demanat és 3316.

264

a) Com que $p \neq q$, llavors $\mathrm{mcd}(p,q) = 1$ i podem aplicar el teorema petit de Fermat mòdul p i també mòdul q. Mòdul p tenim que $p^{q-1} \equiv 0$ i $q^{p-1} \equiv 1$, pel teorema esmentat. Anàlogament es demostra la congruència mòdul q.

b) Sigui $x = p^{q-1} + q^{p-1}$. Hem vist a l'apartat anterior que $x \equiv 1 \pmod{p}$ i $x \equiv 1 \pmod{q}$. Per definició de congruència, $p \mid (x-1)$ i $q \mid (x-1)$. Per tant, $x-1$ és múltiple del mínim comú múltiple de p i q, que és pq. És a dir, $x \equiv 1 \pmod{pq}$.

c) Observem que 23 i 29 són nombres primers tals que $23 \cdot 29 = 667$. Podem aplicar l'apartat anterior i tenim:

$$23^{29-1} + 29^{23-1} = 23^{28} + 29^{22} \equiv 1 \pmod{667}$$

És a dir, $\overline{23}^{28} + \overline{29}^{22} = \overline{1}$ a $\mathbb{Z}_{667}$.

265

a) L'equació diofàntica $2m + 3d = 78$ té solució perquè $\mathrm{mcd}(2,3) = 1 \mid 78$. Escrivim l'identitat de Bézout: $2 \cdot (-1) + 3 \cdot 1 = 1$, d'on una solució particular és $m_0 = -78$ i $d_0 = 78$. Per tant, la solució general és:

$$m = -78 + 3t, \quad d = 78 - 2t, \quad t \in \mathbb{Z}$$

Imposem ara que $m \geq 1$ i $d \geq 1$. D'una part, tenim:

$$m \geq 1 \Leftrightarrow -78 + 3t \geq 1 \Leftrightarrow 3t \geq 79 \Leftrightarrow t \geq 27$$

D'altra banda:

$$d \geq 1 \Leftrightarrow 78 - 2t \geq 1 \Leftrightarrow 77 \geq 2t \Leftrightarrow t \leq 38$$

Per tant, si $27 \leq t \leq 38$, obtenim els parells (m,d) següents:

$$(3,24), (6,22), (9,20), (12,18), (15,16), (18,14), (21,12), (24,10), (27,8), (30,6), (33,4), (36,2)$$

b) Donem dues solucions d'aquest apartat. Per inspecció dels valors obtinguts a l'apartat anterior, veiem que $d \mid m$ si i només si $(m,d) = (30,6)$ o $(m,d) = (36,2)$.

També els podem calcular directament. Com que $d \mid m$, i òbviament $d \mid d$, per la propietat de la linealitat, tenim que $d \mid (2m + 3d)$. És a dir d és un divisor positiu de $78 = 2 \cdot 3 \cdot 13$. A més, donat que $3d = 78 - 2m$, resulta que d ha de ser parell. Els únics valors possibles són $d = 2$, $d = 6$ i $d = 26$. Els corresponents valors de m són $m = 36$, $m = 30$ i $m = 0$. Per tant, les solucions són $(m,d) = (36,2)$ i $(m,d) = (30,6)$.

c) Si $0 < a < b$, $d = \mathrm{mcd}(a,b)$ i $m = \mathrm{mcm}(a,b)$, llavors $d \mid m$. Si, a més, $2m + 3d = 78$, llavors, per l'apartat anterior, els possibles valors de m i d són: $(m,d) = (36,2)$ i $(m,d) = (30,6)$. En el primer cas, busquem enters positius a i b tals que $\mathrm{mcd}(a,b) = 2$ i $\mathrm{mcm}(a,b) = 36$. Hi ha dues solucions: $a = 2$, $b = 36$; $a = 4$, $b = 18$. En el segon cas, busquem enters positius a i b tals que $\mathrm{mcd}(a,b) = 6$ i $\mathrm{mcm}(a,b) = 30$. La única solució és $a = 6$ i $b = 30$.

2.39 Examen de recuperació del primer parcial 09/06/2015

266 **Pas inicial** $n = 1$: d'una banda $\sum_{k=1}^{1} \frac{1}{(4k-3)(4k+1)} = \frac{1}{5}$. De l'altra: $\frac{1}{4+1} = \frac{1}{5}$.
Pas inductiu. Sigui $n \geq 1$ un enter i suposem que:

$$\sum_{k=1}^{n} \frac{1}{(4k-3)(4k+1)} = \frac{n}{4n+1}, \quad \text{(hipòtesi d'inducció)}$$

Volem demostrar que:

$$\sum_{k=1}^{n+1} \frac{1}{(4k-3)(4k+1)} = \frac{n+1}{4n+5}.$$

Tenim:

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{(4k-3)(4k+1)} &= \sum_{k=1}^{n} \frac{1}{(4k-3)(4k+1)} + \frac{1}{(4n+1)(4n+5)} \\
&= \frac{n}{4n+1} + \frac{1}{(4n+1)(4n+5)} && \text{per H.I.} \\
&= \frac{n(4n+5)}{(4n+1)(4n+5)} + \frac{1}{(4n+1)(4n+5)} \\
&= \frac{4n^2+5n+1}{(4n+1)(4n+5)} \\
&= \frac{(4n+1)(n+1)}{(4n+1)(4n+5)} \\
&= \frac{n+1}{4n+5}
\end{aligned}$$

267

a) $\forall x \in \mathbb{Q}\, \exists n \in \mathbb{Z}\, (nx \in \mathbb{Z})$.

b) $\exists x \in \mathbb{Q}\, \forall n \in \mathbb{Z}\, (nx \notin \mathbb{Z})$.

c) La proposició és certa. Sigui $x \in \mathbb{Q}$, $x = a/b$, on $a, b \in \mathbb{Z}$ i $b \neq 0$. Llavors $bx = a \in \mathbb{Z}$. És a dir, hi ha un enter que multiplicat per x dóna un enter.

2.40 Examen de recuperació del segon parcial 09/06/2015

268

a) R és reflexiva: si $(a, b) \in X$, llavors $g(a) + g(b) = g(a) + g(b)$. És a dir, $(a, b)R(a, b)$.

R és simètrica: si $(a, b)R(c, d)$, llavors $g(a) + g(b) = g(c) + g(d)$. D'aqui tenim que $g(c) + g(d) = g(a) + g(b)$ i, per tant, $(c, d)R(a, b)$.

R és transitiva: si $(a, b)R(c, d)$ i $(c, d)R(e, f)$, llavors $g(a) + g(b) = g(c) + g(d)$ i $g(c) + g(d) = g(e) + g(f)$; per tant, $g(a) + g(b) = g(e) + g(f)$; és a dir, $(a, b)R(e, f)$.

b) Sigui $(a, b) \in X$. La seva classe és, per definició:

$$[(a, b)] = \{(x, y) \in X : (x, y)R(a, b)\} = \{(x, y) \in X : g(x) + g(y) = g(a) + g(b)\}$$

Però donat (a, b), el valor de $g(a) + g(b)$ pot ser un enter qualsevol entre 2 i 16. Per tant, per a qualsevol $k \in \{2, \dots, 16\}$, tenim una classe:

$$C_k = \{(x, y) \in X : g(x) + g(y) = k\}$$

c) El conjunt quocient X/R és per definició el conjunt de totes les classes:

$$X/R = \{[(a, b)] : (a, b) \in X\} = \{C_k : 2 \leq k \leq 16\}$$

Hi ha, per tant, 15 classes.

269

a) Tenim que $f(2) = 2 \cdot 2 + 1 = 5$ i $f(3) = 3 + 2 = 5$. Per tant, no és injectiva. Tampoc és exhaustiva, perquè, per exemple, el 2 no té cap antiimatge (és fàcil veure que les imatges per f són sempre senars). Efectivament: l'equació $2n + 1 = 2$ not té cap solució amb n parell (ni senar!) i l'equació $n + 2 = 2$ no té cap solució amb n senar.

b) Per exemple, si $A = \{1, 2\}$, $B = \{2, 3\}$, tenim:

$$f[A \cap B] = f[\{2\}] = \{5\}, \quad f[A] \cap f[B] = \{3, 5\} \cap \{5, 9\} = \{5\}.$$

c) Per exemple, si $A = \{2, 3, 4\}$ i $B = \{2, 3, 7\}$, tenim:

$$f[A \cap B] = f[\{2, 3\}] = \{5\}, \quad f[A] \cap f[B] = \{5, 9\} \cap \{5, 9\} = \{5, 9\}.$$

2.41 Examen parcial 15/10/2015

273

a) Tenim:

$$\begin{aligned} \neg\forall x\,(P(x) \to (Q(x) \vee R(x))) &\equiv \exists x\,\neg(P(x) \to (Q(x) \vee R(x))) && (1)\\ &\equiv \exists x\,(P(x) \wedge \neg(Q(x) \vee R(x))) && (2)\\ &\equiv \exists x\,(P(x) \wedge (\neg Q(x) \wedge \neg R(x))) && (3) \end{aligned}$$

Justificacions: (1), negació del quantificador $\neg\forall x(A(x)) \equiv \exists x(\neg A(x))$; (2), negació de la implicació $\neg(p \to q) \equiv p \wedge \neg q$; (3), llei de De Morgan $\neg(p \vee q) \equiv (\neg p) \wedge (\neg q)$.

En el cas $R(x) = \neg Q(x)$, la proposició donada s'expressa com:

$$\forall x\,(P(x) \to (Q(x) \vee \neg Q(x)))$$

Però, per a tot x, o bé $Q(x)$ és cert o bé $\neg Q(x)$ és cert (principi del tercer exclòs). Per tant, el conseqüent de la implicació sempre és cert i, per tant, la implicació sempre serà certa.

b) Donem tres possibles solucions d'aquest apartat.

Solució 1: El conseqüent de la implicació té la forma d'una disjunció. Per tant, neguem dues de les afirmacions i demostrem la tercera. Així doncs, prenem com a hipòtesi:

$$a+b+c=0, \quad a \text{ és senar}, \quad b \text{ és senar}$$

i volem demostrar (tesi): c és parell. Efectivament, tenim:

$$c=-a-b$$

i sabem que la suma de dos nombres enters senars és un nombre parell.

Solució 2: Demostració pel contrarrecíproc. Suposem (hipòtesi) que a és senar, i que b és senar i que c és senar. Volem demostrar (tesi) que $a+b+c \neq 0$. Efectivament, la suma de tres nombres enters senars és un nombre enter senar i, per tant, diferent de 0, que és parell.

Solució 3: Demostració per reducció a l'absurd. Suposem que $a+b+c=0$ i, a més, que a és senar, b és senar i c és senar. Llavors tenim: d'una banda la suma $a+b+c$ és un nombre enter senar i d'altra banda la suma val 0, que és un nombre parell. Contradicció.

274 Al primer sumatori fem el canvi d'índex següent: $j=k-4$; és a dir $k=j+4$. D'aquesta manera, si $k=5$, llavors $j=1$; i si $k=n+35$, llavors $j=n+31$. Per tant:

$$\sum_{k=5}^{n+35}(k+7)^2=\sum_{j=1}^{n+31}(j+4+7)^2=\sum_{j=1}^{n+31}(j+11)^2=\sum_{j=1}^{n+31}(j^2+22j+121).$$

Al segon sumatori fem el canvi d'índex $j=k+31$; és a dir $k=j-31$. Així, quan $k=-30$, tenim que $j=1$; i quan $k=n$, tenim que $j=n+31$. Per tant,

$$\sum_{k=-30}^{n}(k+28)^2=\sum_{j=1}^{n+31}(j-31+28)^2=\sum_{j=1}^{n+31}(j-3)^2=\sum_{j=1}^{n+31}(j^2-6j+9).$$

Finalment, si notem per A la diferència d'aquests dos sumatoris, tenim:

$$A=\sum_{j=1}^{n+31}(j^2+22j+121)-\sum_{j=1}^{n+31}(j^2-6j+9)=\sum_{j=1}^{n+31}(28j+112),$$

com volíem demostrar.

2.42 Examen parcial 16/11/2015

275 Donem dues possibles solucions.

Solució 1. Sigui $x \in (A \cup B) \setminus (A \cap B)$ un element arbitrari. Llavors:

$$\begin{aligned} x \in (A \cup B) \setminus (A \cap B) &\Leftrightarrow x \in (A \cup B) \wedge x \notin (A \cap B) && (1) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge \neg(x \in A \wedge x \in B) && (2) \\ &\Leftrightarrow (x \in A \vee x \in B) \wedge (x \notin A \vee x \notin B) && (3) \\ &\Leftrightarrow (x \in A \wedge x \notin A) \vee (x \in A \wedge x \notin B) \\ &\qquad \vee (x \in B \wedge x \notin A) \vee (x \in B \wedge x \notin B) && (4) \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A) && (5) \\ &\Leftrightarrow (x \in A \setminus B) \vee (x \in B \setminus A) && (6) \\ &\Leftrightarrow x \in (A \setminus B) \cup (B \setminus A) && (7) \end{aligned}$$

És a dir, hem demostrat que, per a tot x:

$$x \in (A \cup B) \setminus (A \cap B) \Leftrightarrow x \in (A \setminus B) \cup (B \setminus A).$$

Per tant, pel principi d'extensionalitat, els dos conjunts són iguals, com volíem demostrar.

Justificacions:

(1) Per definició de diferència de conjunts.

(2) Per definició d'unió i d'intersecció de conjunts.

(3) Per les lleis de De Morgan per a proposicions (negació d'una conjunció).

(4) Per la propietat distributiva de la disjunció respecte de la conjunció.

(5) Les proposicions "$x \in A \wedge x \notin A$" i "$x \in B \wedge x \notin B$" són falses. D'altra banda, si p és una proposició falsa i q és una proposició arbitrària, llavors $p \vee q \equiv q$.

(6) Per definició de diferència de conjunts.

(7) Per definició d'unió de conjunts.

Solució 2. Considerem l'univers $\Omega = A \cup B$. Llavors, si $C, D \subseteq \Omega$, tenim que $C \setminus D = C \cap D^c$. Tenint en compte aquesta propietat, podem demostrar la igualtat que ens demanen de la manera següent:

$$\begin{aligned} (A \cup B) \setminus (A \cap B) &= (A \cup B) \cap (A \cap B)^c \\ &= (A \cup B) \cap (A^c \cup B^c) && (1) \\ &= (A \cap A^c) \cup (A \cap B^c) \cup (B \cap A^c) \cup (B \cap B^c) && (2) \\ &= \emptyset \cup (A \cap B^c) \cup (B \cap A^c) \cup \emptyset && (3) \\ &= (A \cap B^c) \cup (B \cap A^c) && (4) \\ &= (A \setminus B) \cup (B \setminus A) \end{aligned}$$

Justificacions:

(1) Per les lleis de De Morgan per a conjunts (complementari d'una intersecció).

(2) Per la propietat distributiva de la intersecció respecte de la unió.

(3) Ja que $C \cap C^c = \emptyset$.

(4) Ja que $C \cup \emptyset = C$.

276

Pas base: comprovem la igualtat per a $n = 1$. D'una banda tenim:

$$\prod_{i=1}^{1} \left(1 - \frac{1}{(i+1)^2}\right) = 1 - \frac{1}{4} = \frac{3}{4},$$

i de l'altra tenim:

$$\frac{n+2}{2(n+1)} = \frac{1+2}{2(1+1)} = \frac{3}{4}.$$

Per tant, se satisfà la igualtat.

Pas inductiu: fixem un $n \geq 1$ arbitrari i suposem que la propietat és certa per a n (hipòtesi d'inducció):

$$\prod_{i=1}^{n} \left(1 - \frac{1}{(i+1)^2}\right) = \frac{n+2}{2(n+1)}.$$

Hem de demostrar que la propietat és certa per a $n+1$ (tesi); és a dir:

$$\prod_{i=1}^{n+1} \left(1 - \frac{1}{(i+1)^2}\right) = \frac{n+3}{2(n+2)}.$$

Tenim que:

$$\begin{aligned}
\prod_{i=1}^{n+1} \left(1 - \frac{1}{(i+1)^2}\right) &= \prod_{i=1}^{n} \left(1 - \frac{1}{(i+1)^2}\right) \cdot \left(1 - \frac{1}{(n+2)^2}\right) \\
&= \frac{n+2}{2(n+1)} \cdot \left(1 - \frac{1}{(n+2)^2}\right) && \text{per H.I.} \\
&= \frac{n+2}{2(n+1)} \cdot \frac{(n+2)^2 - 1}{(n+2)^2} \\
&= \frac{n^2+4n+3}{2(n+1)(n+2)} \\
&= \frac{(n+1)(n+3)}{2(n+1)(n+2)} \\
&= \frac{n+3}{2(n+2)}.
\end{aligned}$$

Per tant, pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

277 Per definició, la classe d'equivalència d'un element $A \in \mathcal{P}(\Omega)$ és el conjunt dels elements $B \in \mathcal{P}(\Omega)$ que estan relacionats amb ell; és a dir:

$$[A] = \{B \in \mathcal{P}(\Omega) : A\ R\ B\} = \{B \in \mathcal{P}(\Omega) : A \setminus X = B \setminus X\}.$$

Observem que $A \setminus X = A \cap X^c = A \cap \{4\}$. Per tant, hi ha només dues opcions: que $A \setminus X = \emptyset$ o que $A \setminus X = \{4\}$. El primer cas és equivalent a dir que $A \subseteq X$ o bé que $4 \notin A$. El segon cas és equivalent a dir que $4 \in A$.

Per tant, només hi ha dues classes:

$$\begin{aligned}
[\emptyset] &= \{B \in \mathcal{P}(\Omega) : B \setminus X = \emptyset \setminus X = \emptyset\} \\
&= \{B \in \mathcal{P}(\Omega) : B \subseteq X\} \\
&= \{\emptyset, \{1\}, \{2\}, \{3\}, \{1,2\}, \{1,3\}, \{2,3\}, X\},
\end{aligned}$$

$$\begin{aligned}
[\{4\}] &= \{B \in \mathcal{P}(\Omega) : B \setminus X = \{4\} \setminus X = \{4\}\} \\
&= \{B \in \mathcal{P}(\Omega) : 4 \in B\} \\
&= \{\{4\}, \{1,4\}, \{2,4\}, \{3,4\}, \{1,2,4\}, \{1,3,4\}, \{2,3,4\}, \Omega\}.
\end{aligned}$$

També podem argumentar que no hi ha més classes, perquè $\mathcal{P}(\Omega)$ té $2^4 = 16$ elements i $[\emptyset] \cup [\{4\}]$ també té 16 elements.

2.43 Examen final 12/01/2016

278

a) Sigui $a \in \mathbb{Z}$ i suposem que $\mathrm{mcd}(a, 100) = 1$. Llavors $\overline{a} \in \mathbb{Z}_{100}$ té invers; és a dir, existeix $\overline{b} \in \mathbb{Z}_{100}$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$.

- f_a és injectiva. Siguin $\overline{x}, \overline{x'} \in \mathbb{Z}_{100}$. Tenim que:

$$\begin{aligned}
f_a(\overline{x}) = f_a(\overline{x'}) &\Rightarrow \overline{a} \cdot \overline{x} + \overline{4} = \overline{a} \cdot \overline{x'} + \overline{4} \\
&\Rightarrow \overline{a} \cdot \overline{x} = \overline{a} \cdot \overline{x'} \\
&\Rightarrow \overline{b} \cdot \overline{a} \cdot \overline{x} = \overline{b} \cdot \overline{a} \cdot \overline{x'} \\
&\Rightarrow \overline{x} = \overline{x'}.
\end{aligned}$$

  Per tant, f_a és injectiva.

- f_a és exhaustiva. Sigui $\overline{y} \in \mathbb{Z}_{100}$. Hem de veure que existeix un $\overline{x} \in \mathbb{Z}_{100}$ tal que $f_a(\overline{x}) = \overline{y}$. Plantegem l'equació $\overline{a} \cdot \overline{x} + \overline{4} = \overline{y}$ i aïllem la $\overline{x}$:

$$\overline{a} \cdot \overline{x} + \overline{4} = \overline{y} \Leftrightarrow \overline{a} \cdot \overline{x} = \overline{y} - \overline{4} \Leftrightarrow \overline{b} \cdot \overline{a} \cdot \overline{x} = \overline{b} \cdot (\overline{y} - \overline{4}) \Leftrightarrow \overline{x} = \overline{b} \cdot (\overline{y} - \overline{4})$$

  Com que, per a tot $\overline{x}$, hi ha solució, l'aplicació f_a és exhaustiva.

Per tant, f_a és bijectiva. A més, hem trobat la seva funció inversa: $f_a^{-1}(\overline{x}) = \overline{b} \cdot (\overline{x} - \overline{4})$, on $\overline{b}$ és la classe inverse de la classe $\overline{a}$.

b) Tenim que $\operatorname{mcd}(77, 100) = 1$. Per l'apartat anterior, l'aplicació f_{77} és bijectiva i, per tant, té inversa. A més, hem vist que la inversa és:

$$f_{77}^{-1}(\overline{x}) = \overline{77}^{-1} \cdot (\overline{x} - \overline{4}) = \overline{13} \cdot (\overline{x} - \overline{4}) = \overline{13} \cdot \overline{x} + \overline{48}.$$

Per a calcular $f_{77}^{-1}[\{\overline{30}\}]$, donat que l'aplicació és bijectiva, podem calcular directament la imatge de $\overline{30}$ per l'aplicació inversa:

$$f_{77}^{-1}(\overline{30}) = \overline{13} \cdot \overline{30} + \overline{48} = \overline{38}.$$

Per tant: $f_{77}^{-1}[\{\overline{30}\}] = \{\overline{38}\}$.

Càlcul de l'invers de 77 mòdul 100:

1	0	1	-3	7	-10
0	1	-1	4	-9	13
	1	3	2	1	7
100	77	23	8	7	1
23	8	7	1	0	

És a dir: $100 \cdot (-10) + 77 \cdot 13 = 1$ (identitat de Bézout) i, per tant, $\overline{77}^{-1} = \overline{13}$ a $\mathbb{Z}_{100}$.

c) Per a veure que f_{55} no és ni injectiva ni exhaustiva, trobarem un contraexemple en cada cas.

- Per a demostrar que f_{55} no és injectiva, hem de trobar dues classes diferents $\overline{x} \neq \overline{x'}$ tals que $f_{55}(\overline{x}) = f_{55}(\overline{x'})$. Tenim:

$$\begin{aligned} f_{55}(\overline{x}) = f_{55}(\overline{x'}) &\Leftrightarrow \overline{55} \cdot \overline{x} + \overline{4} = \overline{55} \cdot \overline{x} + \overline{4} \\ &\Leftrightarrow \overline{55} \cdot \overline{x} = \overline{55} \cdot \overline{x} \\ &\Leftrightarrow 55x \equiv 55x' \pmod{100} && (1) \\ &\Leftrightarrow 11x \equiv 11x' \pmod{20} && (2) \\ &\Leftrightarrow x \equiv x' \pmod{20} \end{aligned}$$

  (1) El 55 no es pot simplificar mòdul 100; però podem simplificar un 5 i obtenir una congruència mòdul 20. (2) L'enter 11 té invers mòdul 20, perquè $\operatorname{mcd}(11, 20) = 1$.

  Per tant, si x i x' són congruents entre ells mòdul 20, però no mòdul 100, tenim un contraexemple. Per exemple: $x = 0$, $x' = 20$. D'una banda, $\overline{0} \neq \overline{20}$ a $\mathbb{Z}_{100}$, però $f_{55}(\overline{0}) = f_{55}(\overline{20})$.

- Per a veure que f_{55} no és exhaustiva, hem de veure que existeix un $\overline{y} \in \mathbb{Z}_{100}$ que no té antiimatge. És a dir, l'equació $\overline{55} \cdot \overline{x} + \overline{4} = \overline{y}$, no té cap solució en $\overline{x}$. Per exemple, si fem $\overline{y} = \overline{5}$, llavors l'equació anterior és equivalent a $\overline{55} \cdot \overline{x} = \overline{1}$, que no té solució perquè $\overline{55}$ no té invers a $\mathbb{Z}_{100}$, ja que $\operatorname{mcd}(55, 100) = 5 \neq 1$.

  Una altra manera: f_{55} és una aplicació entre dos conjunts amb el mateix cardinal, 100, i ja sabem que no és injectiva. Per tant, no pot ser exhaustiva.

279 Tenint en compte la identitat polinomial donada i substituint x per $\overline{11}$, obtenim:

$$S \cdot (\overline{11} - \overline{1}) = \overline{11}^{32} - \overline{1}$$

Però $\overline{11} - \overline{1} = \overline{10}$, que té invers a $\mathbb{Z}_{53}$, perquè $\text{mcd}(10, 53) = 1$. Aplicant l'algorisme d'Ecuclides i escrivint la identitat de Bézout per a 53 i 10, obtenim que $\overline{10}^{-1} = \overline{16}$. Per tant:

$$S = \overline{16} \cdot (\overline{11}^{32} - \overline{1})$$

Calculem ara $\overline{11}^{32}$. Si posem $b_0 = 11$ i $b_k \equiv b_{k-1}^2 \pmod{53}$, $k \geq 1$, tenim:

$$\begin{array}{ll} b_0 = 11 & b_3 \equiv 13^2 \equiv 10 \\ b_1 = 11^2 \equiv 15 & b_4 \equiv 10^2 \equiv 47 \equiv -6 \\ b_2 \equiv 15^2 \equiv 13 & b_5 \equiv (-6)^2 = 36 \end{array}$$

Finalment:

$$S = \overline{16} \cdot (\overline{11}^{32} - \overline{1}) = \overline{16} \cdot (\overline{36} - \overline{1}) = \overline{16} \cdot \overline{35} = \overline{30}.$$

280 Si comencem a comptar els minuts a les 10h i x és el nombre de minuts que falten pel primer bloqueig, llavors:

$$x \equiv 0 \pmod{5}, \qquad x \equiv 2 \pmod{12}, \qquad x \equiv 6 \pmod{7}$$

Els mòduls són primers entre ells, dos a dos. Per tant, el sistema xinés té solució única mòdul el producte dels mòduls: $5 \cdot 12 \cdot 7 = 420$. Trobem doncs una solució (aplicant, per exemple, l'algorisme estudiat a classe):

m_i	M_i	y_i	a_i	$M_i y_i a_i$
5	84	(no cal)	0	0
12	35	-1	2	-70
7	60	2	6	720

Càlculs:

$$35y_2 \equiv 1 \pmod{12} \Leftrightarrow -y_2 \equiv 1 \pmod{12} \Leftrightarrow y_2 \equiv -1 \pmod{12}$$
$$60y_3 \equiv 1 \pmod{7} \Leftrightarrow 4y_3 \equiv 1 \pmod{7} \Leftrightarrow y_3 \equiv 2 \pmod{7}$$

Per tant, una solució del sistema és:

$$x = \sum_{i=1}^{3} M_i y_i a_i = -70 + 720 = 650 \equiv 230 \pmod{420}$$

És a dir, la solució és:

$$x \equiv 230 \pmod{420}$$

Les respostes a les preguntes del problema són: els bloquejos es produeixen cada 420 minuts (o 7 hores) i falten 230 minuts (o 3 hores i 50 minuts) pel primer bloqueig. És a dir, el primer bloqueig es produirà a les 13:50h.

2.44 Examen de recuperació del primer parcial 12/01/2016

281

a) P1) $\exists x, y(x \neq y \wedge 1 \leq x \leq 20 \wedge 1 \leq y \leq 20 \wedge 4 \nmid x \wedge \nmid y)$.

P2) $\forall x, y((x \neq y \wedge 1 \leq x \leq 20 \wedge 1 \leq y \leq 20) \rightarrow (4 \mid x \vee 4 \mid y))$.

b) Tenim:

$$\begin{aligned}\neg\forall x, y((x \neq y \wedge 1 \leq x \leq 20 \wedge 1 \leq y \leq 20) \rightarrow (4 \mid x \vee 4 \mid y)) \equiv \\ \equiv \exists x, y\neg((x \neq y \wedge 1 \leq x \leq 20 \wedge 1 \leq y \leq 20) \rightarrow (4 \mid x \vee 4 \mid y) \equiv \\ \equiv \exists x, y((x \neq y \wedge 1 \leq x \leq 20 \wedge 1 \leq y \leq 20) \wedge \neg(4 \mid x \vee 4 \mid y)) \equiv \\ \equiv \exists x, y(x \neq y \wedge 1 \leq x \leq 20 \wedge 1 \leq y \leq 20 \wedge 4 \nmid x \wedge 4 \nmid y)\end{aligned}$$

Hem aplicat les propietats: (1) $\neg\forall x(P(x)) \equiv \exists x(\neg P(x))$; (2) $\neg(\alpha \rightarrow \beta) \equiv (\alpha \wedge \neg\beta)$; (3) $\neg(\alpha \vee \beta) \equiv (\neg\alpha) \wedge (\neg\beta)$.

282 Notem $P(x) = x^3 - 3x^2 + 8x - 17$.

a) Volem provar que si $P(a) = 0$, llavors $a \neq 0$. Ho fem pel contrarecíproc. Suposem que $a = 0$. Llavors $P(a) = P(0) = 1 \neq 0$.

b) La implicació recíproca és: $a \neq 0 \Rightarrow P(a) = 0$. Aquesta implicació és falsa, com mostra el contraexemple següent: per a $a = 1$, tenim $P(a) = P(1) = -11 \neq 0$.

2.45 Examen parcial 12/01/2016

283

a) R és reflexiva: si $a \in \mathbb{Z}$, llavors $a^2 - a = a^2 - a$. Per tant, $a\ R\ a$.

R és simètrica: si $x\ R\ y$, llavors $x^2 - x = y^2 - y$. És a dir, $y^2 - y = x^2 - x$ i, per tant, $y\ R\ x$.

R és transitiva: si $x\ R\ y$ i $y\ R\ z$, llavors $x^2 - x = y^2 - y$ i $y^2 - y = z^2 - z$. Deduïm que $x^2 - x = z^2 - z$ i, per tant, $x\ R\ z$.

b) Sigui $a \in \mathbb{Z}$. Calculem $[a]$:

$$[a] = \{x \in \mathbb{Z} : x\ R\ a\} = \{x \in \mathbb{Z} : x^2 - x = a^2 - a\}$$

Si fixem l'enter a, les solucions de l'equació quadràtica $x^2 - x - (a^2 - a) = 0$ són $x = a$ i $x = 1 - a$. Per tant:

$$[a] = \{a, 1 - a\}.$$

És a dir, cada classe té dos elements. El conjunt quocient és:

$$\mathbb{Z}/R = \big\{[a] : a \in \mathbb{Z}\big\} = \big\{\{a, 1 - a\} : a \in \mathbb{Z}\big\}.$$

284 Ho demostrem per inducció sobre $n \geq 2$.

Pas base: $n = 2$. Per a $n = 2$, tenim:

$$\prod_{i=1}^{2} \frac{2i-1}{2i} = \frac{1}{2} \cdot \frac{3}{4} = \frac{3}{8} > \frac{1}{4},$$

ja que $3 \cdot 4 > 8 \cdot 1$.

Pas inductiu. Fixem un enter $n \geq 2$ i suposem que la propietat és certa per aquest n:

$$\prod_{i=1}^{n} \frac{2i-1}{2i} > \frac{1}{2n}, \qquad \text{(hipòtesi d'inducció).}$$

Volem demostrar que la propietat és certa per a $n+1$; és a dir, que:

$$\prod_{i=1}^{n+1} \frac{2i-1}{2i} > \frac{1}{2n+2}.$$

Tenim:

$$\begin{aligned}
\prod_{i=1}^{n+1} \frac{2i-1}{2i} &= \left(\prod_{i=1}^{n} \frac{2i-1}{2i}\right) \cdot \frac{2n+1}{2n+2} \\
&> \frac{1}{2n} \cdot \frac{2n+1}{2n+2} && (1) \\
&= \frac{2n+1}{2n} \cdot \frac{1}{2n+2} && (2) \\
&> \frac{1}{2n+2}
\end{aligned}$$

(1) per hipòtesi d'inducció; (2) perquè $\frac{2n+1}{2n} > 1$.

Pel principi d'inducció, la propietat és certa per a tot $n \geq 2$.

2.46 Examen parcial 30/04/2016

289

a) Solució 1: Es tracta d'una implicació on el conseqüent és una disjunció. Tenint en compte l'equivalència de fórmules proposicionals $(p \to (q \vee r)) \equiv ((p \wedge \neg q) \to r)$, demostrem que si $c = a + 2b$ i $a > c/2$, aleshores $b \leq c/4$. Suposem que $c = a + 2b$. Aleshores $a = c - 2b$ i com que $a > c/2$, tenim:

$$a = c - 2b > \frac{c}{2}$$

d'on deduïm que $2b < c - c/2 = c/2$. És a dir, $b < c/4$.

Solució 2: Demostrem el contrarecíproc: si $a > c/2$ i $b > c/4$, aleshores $c \neq a + 2b$. Efectivament:

$$a > \frac{c}{2} \wedge b > \frac{c}{4} \Rightarrow a + 2b > \frac{c}{2} + \frac{c}{2} = c.$$

b) Per a demostrar l'equivalència de les tres proposicions, demostrem que $a) \Rightarrow b)$, $b) \Rightarrow c)$ i $c) \Rightarrow a)$. A més, a cada implicació demostrarem, de fet, la forma contrarecíproca.

$a) \Rightarrow b)$ Suposem que $6x - 1$ és racional. Llavors tenim $6x - 1 = a/b$, on a i b són enters i $b \neq 0$, d'on deduïm que $x = (a + b)/6b$, que també és racional.

$b) \Rightarrow c)$ Suposem que $x/(x + 1)$ és racional (recordem que $x \neq -1$). Observem també que $x/(x + 1)$ no pot ser igual a 1. Aleshores podem escriure $x/(x + 1) = a/b$, on a i b són enters, $b \neq 0$ i $a \neq b$. Llavors $x = a/(b - a)$, que també és racional, perquè $a \neq b$, doncs hem dit que a/b no pot ser 1.

$c) \Rightarrow a)$ Suposem que x és racional. Llavors podem escriure $x = a/b$, on a i b són enters i $b \neq 0$. Per tant, $x/(x + 1) = a/(a + b)$, que també és racional.

290 **Pas base:** si $n = 1$, tenim, d'una banda:

$$\sum_{j=1}^{1} \frac{j}{2^j} = \frac{1}{2},$$

i d'altra: $2 - (n + 2)/2^n = 2 - 3/2 = 1/2$.

Pas inductiu: fixem $n \geq 1$ i suposem (hipòtesi d'inducció):

$$\sum_{j=1}^{n} \frac{j}{2^j} = 2 - \frac{n+2}{2^n}.$$

Volem demostrar (tesi):

$$\sum_{j=1}^{n+1} \frac{j}{2^j} = 2 - \frac{n+3}{2^{n+1}}.$$

Tenim:

$$\begin{aligned}
\sum_{j=1}^{n+1} \frac{j}{2^j} &= \sum_{j=1}^{n} \frac{j}{2^j} + \frac{n+1}{2^{n+1}} \\
&= 2 - \frac{n+2}{2^n} + \frac{n+1}{2^{n+1}} && \text{per hip. d'ind.} \\
&= 2 - \frac{2n+4}{2^{n+1}} + \frac{n+1}{2^{n+1}} \\
&= 2 - \frac{n+3}{2^{n+1}}.
\end{aligned}$$

Pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

291 Sabem que $E \vee H$ és certa. Llavors E és certa o H és certa. Fem-ho per casos.

- Suposem que E és certa. Llavors, com que $E \to F$ és certa també, deduïm que F és certa. Però, per la forma contrarecírpoca de $\neg G \to \neg F$, sabem doncs que G és certa. Per tant, en aquest cas tenim que la disjunció $G \vee I$ és certa.

- Suposem ara que H és certa. En aquest cas podem deduir que I és certa, ja que $H \to I$ és certa. Per tant, també en aquest cas provem que $G \vee I$ és certa.

Conclusió: si les fórmules proposiconals donades són certes, llavors $G \vee I$ és una fórmula proposicional certa.

2.47 Examen parcial 02/05/2016

292

a) Demostració formal:

$$\begin{aligned} x \in X \cap Y &\Rightarrow x \in X \wedge x \in Y && \text{(def. de } \cap\text{)} \\ &\Rightarrow x \in Y^c \wedge x \in Y && \text{(hipòtesi} \\ &\Rightarrow x \notin Y \wedge x \in Y && \text{(def. de } Y^c\text{)} \end{aligned}$$

Contradicció. Per tant $X \cap Y = \emptyset$.

Demostració no formal: Per hipòtesi, els elements de X són de Y^c, és a dir, no són de Y, per tant X i Y no tenen elements en comú.

b) El recíproc és cert: $X \cap Y = \emptyset \Rightarrow X \subset Y^c$.

Demostració formal:

$$\begin{aligned} x \in X &\Rightarrow x \notin Y && \text{(hipòtesi)} \\ &\Rightarrow x \in Y^c && \text{(def. } Y^c\text{).} \end{aligned}$$

Demostració no formal: Si X i Y no tenen elements en comú, cap element de X és de Y, és a dir, tot element de X és de Y^c.

293

a) Tenim:

$$\begin{aligned} x \in [a]_T &\Leftrightarrow x \; T \; a && \text{(def. de classe } [a]_T\text{)} \\ &\Leftrightarrow x \; R \; a \wedge x \; S \; a && \text{(def. de } T\text{)} \\ &\Leftrightarrow x \in [a]_R \wedge x \in [a]_S && \text{(def. de classes } [a]_R \text{ i } [a]_S\text{)} \\ &\Leftrightarrow x \in [a]_R \cap [a]_S && \text{(def. de } \cap\text{).} \end{aligned}$$

b) Apliquem l'apartat a):

$$\begin{aligned} [1]_T &= \{1,3,7,9\} \cap \{1,7,9,10,11,12\} = \{1,7,9\}. \\ [2]_T &= \{2,4,5,6,8\} \cap \{2,3,4,5,6,8\} = \{2,4,5,6,8\}. \\ [3]_T &= \{1,3,7,9\} \cap \{2,3,4,5,6,8\} = \{3\}. \\ [10]_T &= \{10,11\} \cap \{1,7,9,10,11,12\} = \{10,11\}. \\ [12]_T &= \{12\} \cap \{1,7,9,10,11,12\} = \{12\}. \end{aligned}$$

Per tant $A/T = \{\{1,7,9\}, \{2,4,5,6,8\}, \{3\}, \{10,11\}, \{12\}\}$.

294

a) $h = g \circ f : \mathbb{R} - \{0\} \to \mathbb{R} - \{2\}$, i, per a cada $x \in \mathbb{R} - \{0\}$, es té:

$$h(x) = g(f(x)) = g\left(\frac{x+5}{x}\right) = \frac{2((x+5)/x)}{((x+5)/x) - 1} = \frac{(2x+10)/x}{5/x} = \frac{2x+10}{5}.$$

b) Càlculs:

$$h(x) = y\ (y \neq 2) \Leftrightarrow \frac{2x+10}{5} = y\ (y \neq 2) \Leftrightarrow x = \frac{5y-10}{2}\ (x \neq 0).$$

Interpretació: Cada $y \in \mathbb{R} - \{2\}$ té una antiimatge, i només una, en $\mathbb{R} - \{0\}$, que és $x = \frac{5y-10}{2} \in \mathbb{R} - \{0\}$. Per tant h és bijectiva.

c) Es té que $h^{-1} : \mathbb{R} - \{2\} \to \mathbb{R} - \{0\}$, i, segons b), $h^{-1}(y) = \frac{5y-10}{2}$, $\forall y \in \mathbb{R} - \{2\}$.

2.48 Examen final 20/06/2016

295

a) $\Rightarrow$) Hipòtesi: a és una potència de 2. Tesi: existeix un enter h tal que a és divisor de $2^h b, 2^{h+1} b, 2^{h+2} b, \ldots$

És evident ja que si $a = 2^k$, llavors a divideix a $2^k b, 2^{k+1} b, 2^{k+2} b, \ldots$

$\Leftarrow$) Hipòtesi: existeix un enter h tal que a és divisor de $2^h b, 2^{h+1} b, 2^{h+2} b, \ldots$ Tesi: a és una potència de 2.

Tenim: $a \mid 2^h b$, i com que a i b són primers entre ells, aplicant el lema d'Euclides es té: $a \mid 2^h$. Per tant, l'únic factor primer de a és 2, i així a és una potència de 2.

b) La implicació $\Rightarrow$) és certa siguin quins siguin a i b. En canvi, la implicació $\Leftarrow$) és falsa quan a i b no són primers entre ells. Contraexemple: basta prendre $a = b = 6$ i es té que $a \mid 2^n b$, $\forall n \geq 0$, i en canvi a no és potència de 2.

296

a) $7 \mid a \wedge 7 \mid b \Rightarrow \exists r \in \mathbb{Z}\ (a = 7r) \wedge \exists s \in \mathbb{Z}\ (b = 7s) \Rightarrow a^2 + b^2 = 7(7r^2 + 7s^2) \Rightarrow 7 \mid (a^2 + b^2)$.

b) Tenim: $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{4}$, $\overline{3}^2 = \overline{9} = \overline{2}$, $\overline{4}^2 = \overline{16} = \overline{2}$, $\overline{5}^2 = \overline{25} = \overline{4}$, $\overline{6}^2 = \overline{36} = \overline{1}$. Per tant, $\{\overline{a}^2 \mid \overline{a} \in \mathbb{Z}_7\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{4}\}$.

c) Per calcular totes les possibles sumes $\overline{a}^2 + \overline{b}^2$, utilitzem els quadrats calculats a l'apartat anterior:

$$\boxed{\overline{0} + \overline{0} = \overline{0}}, \quad \overline{0} + \overline{1} = \overline{1}, \quad \overline{0} + \overline{2} = \overline{2}, \quad \overline{0} + \overline{4} = \overline{4}, \quad \overline{1} + \overline{1} = \overline{2},$$
$$\overline{1} + \overline{2} = \overline{3}, \quad \overline{1} + \overline{4} = \overline{5}, \quad \overline{2} + \overline{2} = \overline{4}, \quad \overline{2} + \overline{4} = \overline{6}, \quad \overline{4} + \overline{4} = \overline{8} = \overline{1}$$

Per tant, $\{\overline{a}^2 + \overline{b}^2 \mid \overline{a}, \overline{b} \in \mathbb{Z}_7\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}, \overline{6}\}$.

d) $7 \mid (a^2+b^2) \Rightarrow \overline{a}^2+\overline{b}^2=\overline{0}$ a $\mathbb{Z}_7$. Segons l'apartat anterior, l'única manera d'expressar $\overline{0}$ de la forma $\overline{a}^2+\overline{b}^2$ és $\overline{0}^2+\overline{0}^2$. Per tant, $\overline{a}^2+\overline{b}^2=\overline{0} \Rightarrow \overline{a}=\overline{b}=\overline{0} \Rightarrow 7 \mid a \wedge 7 \mid b$.

297 Hem de trobar tots els enters a i b tals que:

$$\frac{a}{17}-\frac{b}{4}=\frac{1}{34}.$$

Això equival a resoldre l'equació diofàntica $4a-17b=2$, que té solució perquè $\operatorname{mcd}(4,17)=1$ i $1 \mid 2$. Passant a $\mathbb{Z}_4$: $\overline{-b}=\overline{2}$, d'on $\overline{b}=\overline{-2}=\overline{2}$ i $b=2+4t$, on $t\in\mathbb{Z}$. Llavors $a=(2+17(2+4t))/4=9+17t$. L'expressió genèrica demanada és doncs:

$$\frac{1}{34}=\frac{9+17t}{17}-\frac{2+4t}{4},$$

on t és un enter qualsevol.

2.49 Recuperació del primer parcial 20/06/2016

298

a) $(\forall x)(\forall y)(I(x+y)\longrightarrow(I(x)\vee I(y)))$.

b) $(\exists x)(\exists y)(I(x+y)\wedge\neg I(x)\wedge\neg I(y))$: existeixen dos racionals tals que la seva suma és irracional.

c) Demostració de a) pel contrarecíproc: la suma de dos racionals és racional:

$$\frac{a}{b},\frac{c}{d}\in\mathbb{Q}\Longrightarrow\frac{a}{b}+\frac{c}{d}=\frac{ad}{bd}+\frac{bc}{bd}=\frac{ad+bc}{bd}\in\mathbb{Q}.$$

299

a) Pas bàsic: $\dfrac{1}{3}+\dfrac{1}{2}+\dfrac{1}{6}=\dfrac{2+3+1}{6}=1$, que és natural.

b) Pas inductiu:

Hipòtesi d'inducció: $\dfrac{n}{3}+\dfrac{n^2}{2}+\dfrac{n^3}{6}\in\mathbb{N}$.

Tesi: $\dfrac{n+1}{3}+\dfrac{(n+1)^2}{2}+\dfrac{(n+1)^3}{6}\in\mathbb{N}$.

Tenim:

$$\begin{aligned}\frac{n+1}{3}+\frac{(n+1)^2}{2}+\frac{(n+1)^3}{6}&=\left(\frac{n}{3}+\frac{n^2}{2}+\frac{n^3}{6}\right)+\left(\frac{1}{3}+\frac{2n+1}{2}+\frac{3n^2+3n+1}{6}\right)\\&=\left(\frac{n}{3}+\frac{n^2}{2}+\frac{n^3}{6}\right)+\frac{6+9n+3n^2}{6}\\&=\left(\frac{n}{3}+\frac{n^2}{2}+\frac{n^3}{6}\right)+\frac{(n+1)(n+2)}{2},\end{aligned}$$

i aquest nombre es natural per ser-ho el primer sumand (per hipòtesi d'inducció) i el segon, donat que $(n+1)(n+2)$ és sempre un nombre parell.

2.50 Recuperació del segon parcial 20/06/2016

300

a) i) Reflexiva: $x\,S\,x$, $\forall x \in I$, donat que $x > 1 \Longrightarrow x + x > 1 + 1 = 2$.

ii) Simètrica: $x\,S\,y \Longrightarrow x + y > 2 \Longrightarrow y + x > 2 \Longrightarrow y\,S\,x$.

iii) Transitiva: $x\,S\,y \wedge y\,S\,z \Longrightarrow x\,S\,z$, donat que $x\,S\,z$ és cert, atès que $x + z > 2$ en ser $x > 1$ i $z > 1$.

b) Hem vist en la transitivitat anterior que $x\,S\,z$ és sempre certa, siguin quins siguin els valors de $x, z \in I$, per tant hi ha una única classe d'equivalència i el conjunt quocient és $I/S = \{I\}$.

c) Falla la reflexivitat: $x\,S\,x$ no és cert per a tot $x \in \mathbb{R}$: $0\,S\,0$ és fals, donat que $0+0 \not> 2$.

301

a) El conjunt de les parts de A és:

$$\begin{aligned}\mathcal{P}(A) = \{&\emptyset, \{0\}, \{1\}, \{2\}, \{3\}, \{0,1\}, \{0,2\}, \{0,3\}, \{1,2\}, \{1,3\}, \{2,3\},\\ &\{0,1,2\}, \{0,1,3\}, \{0,2,3\}, \{1,2,3\}, A\}\,.\end{aligned}$$

b) i) No és injectiva ja que $\{0\}$ i $\{1\}$ tenen la mateixa imatge: $\{1\}$.

ii) No és exhaustiva ja que, per exemple, $\emptyset$ no té cap antiimatge. De fet, els únics subconjunts de A que tenen antiimatge són: $\{1\}, \{1,2\}, \{1,3\}, \{1,2,3\}$.

2.51 Examen parcial 7/11/2016

306

1) Considerem l'univers de discurs el conjunts dels nombres reals. Llavors les proposicions donades es poden escriure:

$$\forall x, y\,((x > 0 \wedge y > 0) \to (x/y + y/x \geq 2))$$
$$\forall x, y\,((x > 0 \wedge y > 0) \to (x/y - y/x \geq 2))$$

2) Siguin x, y nombres reals estrictament positius. Llavors tenim les equivalències següents:

$$\begin{aligned}\frac{x}{y}+\frac{y}{x}\geq 2 \Leftrightarrow \frac{x^2+y^2}{xy}&\geq 2\\ &\Leftrightarrow x^2+y^2\geq 2xy \qquad (1)\\ &\Leftrightarrow x^2+y^2-2xy\geq 0\\ &\Leftrightarrow (x-y)^2\geq 0,\end{aligned}$$

i com que la desigualtat $(x-y)^2 \geq 0$ és certa sempre, la desigualtat original també ho és.

(1): aquesta equivalència és certa perquè $xy > 0$; i si multipliquem o dividim una desigualtat per un nombre estrictament positiu, llavors la desigualtat es manté.

3) Que la segona proposició sigui falsa vol dir que la seva negació és certa. La negació de la segona proposició és:

$$\exists x, y\,((x > 0 \wedge y > 0) \wedge (x/y - y/x < 2)).$$

Per tant, hem de trobar nombres reals estrictament positius x i y que compleixin $x/y - y/x < 2$: és a dir, un contraexemple de la proposició donada. Per exemple, si considerem $x = y = 1$, tenim que $x/y - y/x = 0 < 2$.

307

a) **Pas base:** per a $n = 1$, el membre de l'esquerra val:

$$6\cdot\sum_{k=0}^{0}(k^2+1) = 6\cdot(0^2+1) = 6,$$

i el de la dreta val: $2 \cdot 1^3 - 3 \cdot 1^2 + 7 \cdot 1 = 6$.

Pas inductiu: fixem un enter $m \geq 1$ i suposem que la propietat és certa per a aquest enter; és a dir:

$$6\cdot\sum_{k=0}^{m-1}(k^2+1) = 2m^3-3m^2+7m \quad \text{(hipòtesi d'inducció)}.$$

Volem demostrar que la propietat és certa per a l'enter $m + 1$; és a dir:

$$6\cdot\sum_{k=0}^{m}(k^2+1) = 2(m+1)^3-3(m+1)^2+7(m+1) \quad \text{(tesi)}.$$

Tenim:

$$\begin{aligned}6\cdot\sum_{k=0}^{m}(k^2+1) &= 6\cdot\sum_{k=0}^{m-1}(k^2+1)+6(m^2+1)\\ &= (2m^3-3m^2+7m)+6(m^2+1) \quad \text{(per hip. d'inducció)}\\ &= 2m^3+3m^2+7m+6.\end{aligned}$$

D'altra banda, desenvolupant obtenim:

$$2(m+1)^3 - 3(m+1)^2 + 7(m+1) = 2m^3 + 3m^2 + 7m + 6.$$

Pel principi d'inducció, la propietat és certa per a tot nombre natural $n \geq 1$.

b) Llavors tenim que:

$$\begin{aligned}
6 \cdot \sum_{k=0}^{n-1}(k^2+1) &= 6 \cdot \sum_{k=0}^{n-1} k^2 + 6 \cdot \sum_{k=0}^{n-1} 1 \\
&= 6\left(\sum_{k=1}^{n} k^2 - n^2\right) + 6n \\
&= 6 \cdot \sum_{k=1}^{n} k^2 - 6n^2 + 6n \\
&= n(n+1)(2n+1) - 6n^2 + 6n \\
&= 2n^3 - 3n^2 + 7n.
\end{aligned}$$

2.52 Examen parcial 5/12/2016

308

1) Hem de demostrar que $B \subseteq C$ i que $C \subseteq B$.

Sigui $x \in B$. Tenim dos casos: $x \in A$ o $x \notin A$.

$x \in A$: en aquest cas $x \in B$ i $x \in A$. Per tant, $x \in A \cap B$. Però, per hipòtesi, $A \cap B = A \cap C$. Per tant, $x \in A \cap C$, d'on deduïm que $x \in C$.

$x \notin A$: en aquest cas $x \in B$ i $x \notin A$. Per tant, $x \in A^c \cap B$. Però, per hipòtesi, $A^c \cap B = A^c \cap C$. Per tant, $x \in A^c \cap C$, d'on deduïm que $x \in C$.

Per tant, hem demostrat que si $x \in B$, llavors $x \in C$.

Per simetria, intercanviant els papers de B i C, tenim l'altra inclusió $C \subseteq B$.

Una altra solució. Sabem que $X = A \cup A^c$ i que $X \cap B = B$. Per tant:

$$\begin{aligned}
B = X \cap B &= (A \cup A^c) \cap B \\
&= (A \cap B) \cup (A^c \cap B) && \text{prop. distributiva} \\
&= (C \cap A) \cup (A^c \cap C) && \text{per hipòtesi} \\
&= C \cap (A \cup A^c) && \text{prop. distributiva} \\
&= C \cap X = C.
\end{aligned}$$

2) Veiem que R és una relació d'equivalència. És a dir: R és reflexiva, simètrica i transitiva.

Reflexiva: tenim que $(x+1)^2 = (x+1)^2$, per a qualsevol enter x. Per tant, $x\,R\,x$, per a tot $x \in \mathbb{Z}$.

Simètrica: si $x, y \in \mathbb{Z}$, tenim:

$$x\,R\,y \Rightarrow (x+1)^2 = (y+1)^2 \Rightarrow (y+1)^2 = (x+1)^2 \Rightarrow y\,R\,x.$$

Transitiva: si $x, y, z \in \mathbb{Z}$, tenim:

$$\begin{aligned} x\,R\,y \,\wedge\, y\,R\,z &\Rightarrow (x+1)^2 = (y+1)^2 \,\wedge\, (y+1)^2 = (z+1)^2 \\ &\Rightarrow (x+1)^2 = (z+1)^2 \Rightarrow x\,R\,z. \end{aligned}$$

Calculem ara la classe d'equivalència d'un enter a:

$$\begin{aligned} [a] &= \{x \in \mathbb{Z} : x\,R\,a\} \\ &= \{x \in \mathbb{Z} : (x+1)^2 = (a+1)^2\} \\ &= \{x \in \mathbb{Z} : x+1 = a+1 \,\vee\, x+1 = -(a+1)\} \\ &= \{x \in \mathbb{Z} : x = a \,\vee\, x = -a-2\} = \{a, -a-2\}. \end{aligned}$$

Observem que $[a]$ té sempre dos elements, excepte per a $a = -1$: $[-1] = \{-1\}$.

El conjunt quocient és:

$$\mathbb{Z}/R = \{[a] : a \in \mathbb{Z}\} = \{\{-1\}, \{0, -2\}, \{1, -3\}, \{2, -4\}, \ldots\}.$$

309

1) Hem de demostrar que g és una aplicació ben definida; és a dir, si $x \in D$, llavors $x/(x-1) \in D$. Suposem que x és un nombre real tal que $x > 1$. Llavors $x - 1 > 0$ i, per tant, si dividim els dos membres de la desigualtat $x > x-1$ per $x-1$, la desigualtat es manté; és a dir:

$$(x > x-1) \,\wedge\, (x-1 > 0) \Rightarrow \frac{x}{x-1} > \frac{x-1}{x-1} = 1.$$

Per tant, hem vist que si $x > 1$, llavors $x/(x-1) > 1$.

2) Hem de demostrar que g és injectiva i exhaustiva. Provem que és injectiva. Siguin $x, x' \in D$ tals que $g(x) = g(x')$. Hem de demostrar que $x = x'$. Tenim:

$$\begin{aligned} g(x) = g(x') &\Rightarrow \frac{x}{x-1} = \frac{x'}{x'-1} \\ &\Rightarrow x(x'-1) = x'(x-1) \\ &\Rightarrow xx' - x = x'x - x' \\ &\Rightarrow x = x'. \end{aligned}$$

Demostrem ara que g és exhaustiva. Sigui $y \in D$. Hem de veure que existeix $x \in D$ tal que $g(x) = y$. Tenim:

$$\begin{aligned} g(x) = y &\Leftrightarrow \frac{x}{x-1} = y \\ &\Leftrightarrow x = y(x-1) && \text{perquè } x \neq 1 \\ &\Leftrightarrow x(y-1) = y \\ &\Leftrightarrow x = \frac{y}{y-1} && \text{perquè } y \neq 1. \end{aligned}$$

Finalment, hem de comprovar que aquesta x que hem obtingut és un element de D; és a dir, que si $y > 1$, llavors $x = y/(y-1) > 1$. Aquesta implicació es demostra de la mateixa manera que l'apartat 1.

Observem que al demostrar que g és exhaustiva, hem vist que donat un $y \in D$ existeix *un únic* $x \in D$ tal que $g(x) = y$. La unicitat implica que g és injectiva.

3) Per definició de composició d'aplicacions: $(g \circ g)(x) = g(g(x))$. Per tant:

$$g(g(x)) = \frac{g(x)}{g(x)-1} = \frac{\frac{x}{x-1}}{\frac{x}{x-1} - 1} = \frac{x}{x-(x-1)} = x.$$

Per tant, $(g \circ g)(x) = x$, per a tot $x \in D$. És a dir: $g \circ g = I_D$, l'aplicació identitat de D.

Observació: d'aquesta propietat es pot deduir directament que G és una aplicació bijectiva i que $g^{-1} = g$. Efectivament, sabem que I_D és una aplicació bijectiva. A més, sabem que si $f \circ h$ és bijectiva, llavors f és exhaustiva i h és injectiva. En el nostre cas, deduïm que g és exhaustiva i injectiva. D'altra banda, f i h són bijectives i mútuament inverses una de l'altra si i només si $f \circ h$ i $h \circ f$ són les corresponents aplicacions identitat. En el nostre cas, deduïm directament que g és la seva pròpia inversa.

4) Sabem que g és bijectiva. Per tant, si $x, y \in D$, llavors, per definició d'inversa:

$$g(x) = y \Leftrightarrow g^{-1}(y) = x.$$

A l'apartat 2, hem vist:

$$g(x) = y \Leftrightarrow x = \frac{y}{y-1}.$$

Per tant, l'aplicació inversa $g^{-1} : D \to D$ és:

$$g^{-1}(y) = \frac{y}{y-1}.$$

2.53 Examen final 12/01/2017

310 Donarem dues solucions. Comencem per la primera.

($\Leftarrow$) Si $a, b \geq 1$ són enters, llavors tenim:

$$a \mid b \Rightarrow \exists k \in \mathbb{Z} \;\; (b = ak) \Rightarrow \exists k' \in \mathbb{Z}(b^n = a^n k' \wedge k' = k^n) \Rightarrow a^n \mid b^n.$$

($\Rightarrow$) Suposem ara que $a^n \mid b^n$. Llavors existeix un enter t tal que $b^n = a^n t$. Volem demostrar que $a \mid b$.

Escrivim $a = a_1 d$, $b = b_1 d$, amb $d = \text{mcd}(a, b)$ i $\text{mcd}(a_1, b_1) = 1$. Com que $a, b \geq 1$, tenim que $d \neq 0$. Per tant, tenim:

$$b^n = a^n t \Rightarrow b_1^n d^n = a_1^n d^n t \Rightarrow b_1^n = a_1^n t \Rightarrow a_1 \mid b_1^n.$$

Ara bé, si $\text{mcd}(a_1, b_1) = 1$, llavors $\text{mcd}(a_1, b_1^m) = 1$, per a tot enter $m \geq 1$. Demostrem aquesta afirmació per reducció a l'absurd. Suposem doncs que $\text{mcd}(a_1, b_1) = 1$ i $\text{mcd}(a_1, b_1^m) \neq 1$. Llavors hi ha un nombre primer p tal que $p \mid a_1$ i $p \mid b_1^m$. Pel lema d'Euclides, si $p \mid b_1^m$, llavors $p \mid b_1$. Però ara tenim que hi ha un nombre primer p tal que $p \mid a_1$ i $p \mid b_1$. Contradicció, ja que $\text{mcd}(a_1, b_1) = 1$.

Per tant, $\text{mcd}(a_1, b_1^n) = 1$ i com que $a_1 \mid b_1^n$, $\text{mcd}(a_1, b_1^n) = a_1$. És a dir, $a_1 = 1$. Això vol dir que $a = a_1 d = d$, que divideix a b.

Segona solució.

Descomposem a i b en factors primers. Per tal de facilitar la notació, escrivim a les dues factoritzacions tots els primers que apareguin tant a a com a b. Per tant, existeixen $p_1, \ldots, p_k$, primer diferents entre ells tals que $a = \prod_{i=1}^k p_i^{\alpha_i}$, $b = \prod_{i=1}^k p_i^{\beta_i}$ amb $\alpha_i, \beta_i \geq 0$. Observem que les factoritzacions de a^n i b^n es poden escriure com $\prod_{i=1}^k p_i^{n\alpha_i}$ i $\prod_{i=1}^k p_i^{n\beta_i}$ respectivament.

Observem que, en general, es compleix:

$$a \mid b \Leftrightarrow \alpha_i \leq \beta_i \quad \text{per tot } i.$$

Així:

$$a^n \mid b^n \Leftrightarrow n\alpha_i \leq n\beta_i \text{ per tot } i \Leftrightarrow \alpha_i \leq \beta_i \text{ per tot } i \Leftrightarrow a \mid b.$$

311

a) Suposem primer que $ab \equiv ac \pmod{ad}$. Per definició de congruència, existeix un enter k tal que $ab - ac = k \cdot ad$. Com que $a \neq 0$, podem simplificar aquesta igualtat d'enters per a i obtenim $b - c = k \cdot d$. Per tant: $b \equiv c \pmod{d}$.

Demostrem ara el recíproc. Suposem que $b \equiv c \pmod{d}$. Llavors existeix un enter t tal que $b - c = t \cdot d$. Multiplicant per a els dos membres de la igualtat obtenim $ab - ac = t \cdot ad$. Per tant: $ab \equiv ac \pmod{ad}$.

b) Per l'apartat anterior, i donat que $35 = 5 \cdot 7$, tenim l'equivalència:

$$5 \cdot 8^n \equiv 5 \cdot n^{48} \pmod{35} \Leftrightarrow 8^n \equiv n^{48} \pmod{7}.$$

Ara bé, es compleix que $8^n \equiv 1^n \equiv 1 \pmod{7}$. Per tant, només hem de demostrar que $n^{48} \equiv 1 \pmod{7}$. Com que $\mathrm{mcd}(n, 7) = 1$ i 7 és primer, podem aplicar el teorema petit de Fermat i obtenim que $n^6 \equiv 1 \pmod{7}$. Finalment, tenim: $n^{48} = (n^6)^8 \equiv 1^8 \equiv 1 \pmod{7}$, com volíem demostrar.

312

a) Anomenem r_1, r_2 i r_3 els residus de que parla l'enunciat. Observem que $\mathrm{mcd}(13, 25) = \mathrm{mcd}(13, 37) = \mathrm{mcd}(25, 37) = 1$, és a dir que els nombres 13, 25 i 37 són primers entre ells dos a dos. El teorema xinès dels residus afirma que el sistema de congruències:

$$\begin{aligned} x &\equiv r_1 \pmod{13} \\ x &\equiv r_2 \pmod{25} \\ x &\equiv r_3 \pmod{37} \end{aligned}$$

té solució, que és única mòdul $13 \cdot 25 \cdot 37 = 12025$. En particular, si sabem que el sistema anterior té una solució x que està entre 0 i 10^4, amb aquestes condicions (estar entre 0 i 10^4) x serà única ja que $10^4 < 12015$.

b) Anem a resoldre el sistema:

$$\begin{aligned} x &\equiv 2 \pmod{13} \\ x &\equiv 4 \pmod{25} \\ x &\equiv 5 \pmod{37} \end{aligned}$$

Com que els mòduls són primers entre ells dos a dos, usarem l'algorisme que ens permet escriure x com:

$$x = a_1 \cdot y_1 \cdot M_1 + a_2 \cdot y_2 \cdot M_2 + a_3 \cdot y_3 \cdot M_3 \pmod{m_1 \cdot m_2 \cdot m_3}.$$

Fem una taula amb els a's, m's, M's i y's:

i	a_i	m_i	M_i	y_i
1	2	13	$25 \cdot 37 = 925$	$y_1 \cdot M_1 \equiv 1 \pmod{m_1}$
2	4	25	$13 \cdot 37 = 481$	$y_2 \cdot M_2 \equiv 1 \pmod{m_2}$
3	5	37	$25 \cdot 37 = 325$	$y_3 \cdot M_3 \equiv 1 \pmod{m_3}$

Càlcul dels y's:

- $y_1 \cdot 925 \equiv 1 \pmod{13} \Leftrightarrow y_1 \cdot 2 \equiv 1 \pmod{13} \Leftrightarrow y_1 \equiv 7 \pmod{13}$ (a ull).
- $y_2 \cdot 481 \equiv 1 \pmod{25} \Leftrightarrow y_2 \cdot 6 \equiv 1 \pmod{25} \Leftrightarrow y_2 \equiv -4 \pmod{25}$ (a ull).

- $y_3 \cdot 325 \equiv 1 \pmod{37} \Leftrightarrow y_3 \cdot 29 \equiv 1 \pmod{37}$. Com que no es veu la solució a ull, calculem-la mitjançant la identitat de Bézout que obtindrem via l'algorisme d'Euclides estès:

Y	0	1	-1	4	-5	9	-14
Q		1	3	1	1	1	2
R	37	29	8	5	3	2	1
	3	1	1	1	1	0	

  Identitat de Bézout: $37 \cdot * + 29 \cdot (-14) = 1$. Si reduïm mòdul 37, obtenim $(-14) \cdot 29 \equiv 1 \pmod{37}$. Per tant, prenem $y_3 = -14$.

La taula anterior queda:

i	a_i	m_i	M_i	y_i
1	2	13	925	7
2	4	25	481	-4
3	5	37	325	-14

Solució general del sistema:

$$x \equiv 2 \cdot 7 \cdot 925 + 4 \cdot (-4) \cdot 481 + 5 \cdot (-14) \cdot 325 \equiv -17496 \equiv 6554 \pmod{12025};$$

Com que ens demanen l'únic enter positiu més petit que 10^4 que és solució d'aquest sistema, aquest és 6554.

2.54 Recuperació del primer parcial 12/01/2017

313 Hem de demostrar que:

$$\forall a, b \in \mathbb{R} \left(a \geq \frac{a+b}{2} \vee b \geq \frac{a+b}{2} \right).$$

Siguin a i b nombres reals arbitraris. Donat que $p \vee q \equiv (\neg p \to q)$, per demostrar la disjunció, neguem una de les condicions i demostrem que s'ha de satisfer l'altra. Suposem doncs que $a < \frac{a+b}{2}$. Hem de demostrar que $b \geq \frac{a+b}{2}$. Tenim:

$$a < \frac{a+b}{2} \Rightarrow 2a < a+b \Rightarrow a < b \Rightarrow a+b < 2b \Rightarrow \frac{a+b}{2} < b \Rightarrow \frac{a+b}{2} \leq b.$$

314

Pas base: si $n = 1$, tenim:

$$\sum_{i=1}^{1} (2i)^2 = 2^2 = 4, \quad \frac{2n(n+1)(2n+1)}{3} = \frac{2 \cdot 2 \cdot 3}{3} = 4$$

Pas inductiu: sigui $m \geq 1$ i suposem que la propietat és certa per a m:

$$\sum_{i=1}^{m} (2i)^2 = \frac{2m(m+1)(2m+1)}{3} \quad \text{(hipòtesi d'inducció)}.$$

Hem de demostrar que la propietat és certa per a $m+1$; és a dir:

$$\sum_{i=1}^{m+1} (2i)^2 = \frac{2(m+1)(m+2)(2m+3)}{3}.$$

Tenim:

$$\begin{aligned}
\sum_{i=1}^{m+1} (2i)^2 &= \sum_{i=1}^{m} (2i)^2 + (2(m+1))^2 \\
&= \frac{2m(m+1)(2m+1)}{3} + 4(m+1)^2 && \text{per hip. d'inducció} \\
&= \frac{2m(m+1)(2m+1) + 12(m+1)^2}{3} \\
&= \frac{2(m+1)(m(2m+1) + 6(m+1))}{3} \\
&= \frac{2(m+1)(2m^2 + 7m + 6)}{3} \\
&= \frac{2(m+1)(m+2)(2m+3)}{3}.
\end{aligned}$$

Pel principi d'inducció, la propietat és certa per a tot $n \geq 1$.

2.55 Recuperació del segon parcial 12/01/2017

315

a) Suposem que f és injectiva. Volem demostrar que g és injectiva. Siguin $(x, y), (x', y') \in A \times C$. Llavors:

$$g(x, y) = g(x', y') \Rightarrow (f(x), y) = (f(x'), y') \Rightarrow f(x) = f(x') \wedge y = y' \Rightarrow x = x' \wedge y = y',$$

l'última implicació és certa perquè f és injectiva, per hipòtesi.

b) Suposem ara que f és exhaustiva. Volem demostrar que g és exhaustiva. Sigui $(b, c) \in B \times C$ un element arbitrari. Hem de demostrar que existeix un element $(x, y) \in A \times C$ tal que $g(x, y) = (b, c)$. Però:

$$g(x, y) = (f(x), y) = (b, c) \Leftrightarrow f(x) = b \wedge y = c.$$

Com que per hipòtesi f és exhaustiva, donat l'element $b \in B$, existeix $a \in A$ tal que $f(a) = b$. Podem prendre $x = a$, $y = c$. Efectivament:

$$g(a, c) = (f(a), c) = (b, c).$$

316

a) Reflexiva: $\mathrm{mcd}(a,p) = \mathrm{mcd}(a,p)$ i per tant $a\,R\,a$. Simètrica: $a\,R\,b \Rightarrow \mathrm{mcd}(a,p) = \mathrm{mcd}(b,p) \Rightarrow b\,R\,a$.

Transitiva: $aRb \wedge bRc \Rightarrow \mathrm{mcd}(a,p) = \mathrm{mcd}(b,p) \wedge \mathrm{mcd}(b,p) = \mathrm{mcd}(c,p) \Rightarrow \mathrm{mcd}(a,p) = \mathrm{mcd}(c,p) \Rightarrow a\,R\,c$.

b) Calculem la classe de 1:

$$[1] = \{x \in A : \mathrm{mcd}(x,5) = \mathrm{mcd}(1,5) = 1\} = \{1,2,3,4,6,7,8,9,11,12,13,14,16,17,18\}.$$

Prenem ara el 5, el primer element de A del que encara no tenim la seva classe:

$$[5] = \{x \in A : \mathrm{mcd}(x,5) = \mathrm{mcd}(5,5) = 5\} = \{5,10,15\}.$$

Per tant, les classes d'equivalència quan $n = 18$ i $p = 5$ són [1] i [5].

c) El conjunt quocient és el conjunt format per les classes d'equivalència:

$$A/R = \{[a] : a \in A\}.$$

Però $[a] = \{x \in A : \mathrm{mcd}(x,p) = \mathrm{mcd}(a,p)\}$. Per tant, tots els elements de $[a]$ tenen el mateix mcd amb p que a. Com que el mcd és un divisor de p, per a cada divisor d de p tal que $d \in A$ tenim una classe:

$$[d] = \{x \in A : \mathrm{mcd}(x,p) = d\}.$$

Per tant: $A/R = \{[d] : d \mid p \wedge d \in A\}$.

2.56 Examen parcial 20/04/2017

321

Pas base: si $n = 2$, tenim que:

$$\sum_{i=0}^{2} \frac{1}{2i+1} = 1 + \frac{1}{3} + \frac{1}{5} = \frac{23}{15}$$

que és més petit que $\frac{2}{3} + 1 = \frac{5}{3}$.

Pas inductiu: sigui $n \geq 2$ un enter i suposem que es compleix:

$$\sum_{i=0}^{n} \frac{1}{2i+1} < \frac{n}{3} + 1 \quad \text{(hipòtesi d'inducció).}$$

Volem demostrar que la propietat es compleix també per l'enter $n+1$; és a dir:

$$\sum_{i=0}^{n+1} \frac{1}{2i+1} < \frac{n+1}{3} + 1.$$

Tenim:

$$\sum_{i=0}^{n+1} \frac{1}{2i+1} = \sum_{i=0}^{n} \frac{1}{2i+1} + \frac{1}{2n+3} < \frac{n}{3} + 1 + \frac{1}{2n+3},$$

aquesta última desigualtat per hipòtesi d'inducció. Ara hem de demostrar que:

$$\frac{n}{3} + 1 + \frac{1}{2n+3} < \frac{n+1}{3} + 1.$$

Com que $n \geq 2$, tenim que $2n+3 \geq 7$ i, per tant, $1/(2n+3) \leq 1/7 < 1/3$. D'aqui deduïm:

$$\frac{n}{3} + 1 + \frac{1}{2n+3} < \frac{n}{3} + 1 + \frac{1}{3} = \frac{n+1}{3} + 1.$$

Pel principi d'inducció, la propietat és certa per a tot enter $n \geq 2$.

322 Per a demostrar que aquestes proposicions són equivalents, hem de demostrar que a) implica b), que b) implica c) i que c) implica a).

a)⇒b) Prova directa. Suposem que $n+3$ és senar; és a dir, n és parell: $n = 2k$, per a algun $k \in \mathbb{Z}$. Llavors tenim que:

$$5n^2 + 2n + 1 = 5(2k)^2 + 2 \cdot 2k + 1 = 2(10k^2 + 2k) + 1,$$

que és senar.

b)⇒c) Prova pel contrarecíproc. Suposem que $n+3$ és parell, és a dir, n és senar: $n = 2k+1$, per a cert $k \in \mathbb{Z}$. Llavors tenim que:

$$5n^2 + 2n + 1 = 5(2k+1)^2 + 2(2k+1) + 1 = 2(10k^2 + 12k + 6),$$

que és parell.

c)⇒a) Prova directa. Suposem que $n-2$ és parell. Llavors n és parell també i, per tant, $n+3$ és senar.

2.57 Examen parcial 15/05/2017

323

a) R és reflexiva: si $(a, B) \in X$, llavors $a = a$ i $|B| = |B|$. Per tant, $(a, B)\, R\, (a, B)$.

R és simètrica: si $(a, B)\, R\, (a', B')$, llavors $a = a'$ i $|B| = |B'|$; per tant, també es compleix que $(a', B')\, R\, (a, B)$.

R és transitiva: si $(a, B)\, R\, (a', B')$ i $(a', B')\, R\, (a'', B'')$, llavors $a = a'$, $|B| = |B'|$, $a' = a''$ i $|B'| = |B''|$; per tant, tenim que $a = a''$ i $|B| = |B''|$ i es compleix que $(a, B)\, R\, (a'', B'')$.

b) Sigui $(a, B) \in X$. Trobem la seva classe d'equivalència:

$$[(a, B)] = \{(x, C) : x = a, |C| = |B|\} = \{(a, C) : |C| = |B|\};$$

és a dir, la classe de (a, B) està formada pels parells de la forma (a, C) on C és un subconjunt de A amb el mateix cardinal que B. Per tant, tenim les classes:

$$\begin{aligned} [(a, \emptyset)] &= \{(a, \emptyset)\} && a = 1, 2, 3 \\ [(a, \{1\})] &= \{(a, \{1\}), (a, \{2\}), (a, \{3\})\} && a = 1, 2, 3 \\ [(a, \{1, 2\})] &= \{(a, \{1, 2\}), (a, \{1, 3\}), (a, \{2, 3\})\} && a = 1, 2, 3 \\ [(a, \{1, 2, 3\})] &= \{(a, \{1, 2, 3\})\} && a = 1, 2, 3 \end{aligned}$$

En total tenim 12 classes d'equivalència.

c) El conjunt quocient està format per totes les classes d'equivalència:

$$\begin{aligned} X/R = \{&[(1, \emptyset)], [(2, \emptyset)], [(3, \emptyset)], \\ &[(1, \{1\})], [(2, \{1\})], [(3, \{1\})], \\ &[(1, \{1, 2\})], [(2, \{1, 2\})], [(3, \{1, 2\})], \\ &[(1, \{1, 2, 3\})], [(2, \{1, 2, 3\})], [(3, \{1, 2, 3\})]\}. \end{aligned}$$

d) Si A té n elements, llavors hi ha una classe per a cada parell format per un element $a \in A$ i un possible cardinal k, $0 \leq k \leq n$. Per tant, hi ha $n(n + 1)$ classes.

324

a) Tenim:

$$\begin{aligned} f[\{0, 1, 2, 3, 4\}] &= \{f(0), f(1), f(2), f(3), f(4)\} = \{0, 1, -1, 2, -2\}. \\ g^{-1}[\{0, 1, 2, 3, 4\}] &= \{0, 1, -1, 2, -2\}. \end{aligned}$$

b) Tenim, si $n \in \mathbb{N}$:

$$(g \circ f)(n) = g(f(n)) = \begin{cases} g(-n/2) & \text{si } n \text{ és parell} \\ g((n + 1)/2) & \text{si } n \text{ és senar} \end{cases}$$

Si $n \in \mathbb{N}$ és parell, llavors $-n/2$ és un nombre enter negatiu. Per tant, $g(-n/2) = -2(-n/2) = n$. Si $n \in \mathbb{N}$ és senar, llavors $(n + 1)/2$ és un nombre enter positiu. Per tant, $g((n + 1)/2) = 2((n + 1)/2) - 1 = n$. És a dir, hem demostrat que la composició $g \circ f$ és l'aplicació identitat $I_{\mathbb{N}}$.

Ara si $n \in \mathbb{Z}$ tenim:

$$(f \circ g)(n) = \begin{cases} f(2n - 1) & \text{si } n > 0 \\ f(-2n) & \text{si } n \leq 0 \end{cases}$$

Si $n > 0$, llavors $2n - 1$ és un nombre natural senar. Per tant, $f(2n - 1) = (2n - 1 + 1)/2 = n$. Si $n \leq 0$, llavors $-2n$ és un nombre natural parell. Per tant, $f(-2n) = -(2n)/2 = n$. És a dir, hem demostrat que la composició $f \circ g$ és l'aplicació identitat $I_{\mathbb{Z}}$.

c) Hem provat a l'apartat anterior que $g \circ f = I_{\mathbb{N}}$ i que $f \circ g = I_{\mathbb{Z}}$. Com que l'aplicació identitat d'un conjunt és bijectiva, deduïm d'aquestes igualtats que tant f com a g són bijectives.

d) De les mateixes igualtats d'abans deduïm que les aplicacions f i g són mútuament inverses. És a dir, $f^{-1} = g$ i $g^{-1} = f$.

2.58 Examen final 09/06/2017

325

a) Substituïnt la solució al sistema, obtenim:

$$\begin{aligned}\overline{21} + \overline{32} &= \overline{53} = \overline{5}\\ \overline{42} + \overline{56} &= \overline{98} = \overline{8}\end{aligned}$$

És a dir, $\overline{53} - \overline{5} = \overline{48} = \overline{0}$ i $\overline{98} - \overline{8} = \overline{90} = \overline{0}$ a $\mathbb{Z}_n$. Per tant, $n \mid 48$ i $n \mid 90$, i d'aquí deduïm que $n \mid \mathrm{mcd}(48, 90) = 6$. Els possibles valors de n són $1, 2, 3, 6$.

b) Si $\mathrm{mcd}(a, b) = 5$, llavors d'una banda $5 \mid a$. Per tant, a acaba en 0 o en 5. Però sabem que $\mathrm{mcd}(a, c) = 4$, la qual cosa implica que a és parell. Per tant, deduïm que a acaba en 0. D'altra banda, $5 \mid b$. És a dir, b acaba en 0 o en 5. Si b acaba en 0, llavors b és parell. Com que ja sabem que a és parell, deduïm que $\mathrm{mcd}(a, b)$ és parell; i això no és cert. Per tant, b acaba en 5.

326

a) En primer lloc, observem que 223 és un nombre primer. En efecte, $14 < \sqrt{223} < 15$ i a més 223 no és divisible pels primers 2, 3, 5, 7, 11 ni 13.

Ara, pel teorema petit de Fermat, tenim que si $223 \nmid a$, llavors $a^{223-1} = a^{222} \equiv 1 \pmod{223}$. Com que l'exponent 1468 es pot escriure com $1468 = 222q + 136$, obtenim que:

$$2235^{1468} \equiv 5^{1468} \equiv 5^{136} \pmod{223}.$$

Ara escrivim l'exponent en binari: $136 = 2^3 + 2^7$ i calculem els b_i per a $i = 0, \dots, 7$:

$$\begin{array}{llll} b_0 \equiv 5 & b_1 \equiv b_0^2 \equiv 25 & b_2 \equiv b_1^2 \equiv 179 & b_3 \equiv b_2^2 \equiv 152 \\ b_4 \equiv b_3^2 \equiv 135 & b_5 \equiv b_4^2 \equiv 162 & b_6 \equiv b_5^2 \equiv 153 & b_7 \equiv b_6^2 \equiv 217. \end{array}$$

Finalment:

$$5^{136} = 5^{2^3+2^7} = 5^{2^3} \cdot 5^{2^7} \equiv b_3 \cdot b_7 \equiv 152 \cdot 217 \equiv 203 \pmod{223}.$$

b) Siguin d i m el dia i el mes de l'aniversari, respectivament. Llavors $12d + 31m = 492$, $1 \leq m \leq 12$ i $1 \leq d \leq f(m)$, on $f(m)$ indica el nombre de dies del mes m.

Resolem primer l'equació diofàntica. Els coeficients 12 i 31 són primers entre ells i, per tant, l'equació té solucions enteres. La identitat de Bézout per a 12 i 31 s'obté aplicant l'algorisme d'Eucilides i és $12 \cdot 13 + 31 \cdot (-5) = 1$. Multiplicant per 492, obtenim la solució particular $(d_0, m_0) = (6396, -2460)$. Per tant, la solució genereal de l'equació ve donada per:

$$d = 6396 - 31t, \quad m = -2460 + 12t, \qquad t \in \mathbb{Z}.$$

Ara imposem les condicions $1 \leq m \leq 12$:

$$\begin{aligned} 1 \leq m \leq 12 &\Leftrightarrow 1 \leq -2460 + 12t \leq 12 \\ &\Leftrightarrow 2461 \leq 12t \leq 2472 \\ &\Leftrightarrow \frac{2461}{12} \leq t \leq \frac{2472}{12} \\ &\Leftrightarrow 205,08 \leq t \leq 206. \end{aligned}$$

És a dir, $t = 206$. Per a aquest valor, obtenim $d = 10$ i $m = 12$. És a dir, l'aniversari és el 10 de desembre.

327

a) Si calculem les primeres potències de $\overline{5}$ a $\mathbb{Z}_{126}$, obtenim:

$$\overline{5}^0 = \overline{1}, \quad \overline{5}^1 = \overline{5}, \quad \overline{5}^2 = \overline{25}, \quad \overline{5}^3 = \overline{125} = -\overline{1}, \quad \overline{5}^4 = -\overline{5}, \quad \overline{5}^5 = -\overline{25}, \quad \overline{5}^6 = \overline{1}.$$

És a dir, si $n \geq 0$ és un enter i escrivim $n = 6q + r$, amb $0 \leq r \leq 5$, llavors $\overline{5}^n = (\overline{5}^6)^q \cdot \overline{5}^r = \overline{5}^r$. Per tant, tenim els casos següents:

$$\overline{5}^n = \begin{cases} 1, & \text{si } n \equiv 0 \pmod 6 \\ 5, & \text{si } n \equiv 1 \pmod 6 \\ 25, & \text{si } n \equiv 2 \pmod 6 \\ -1, & \text{si } n \equiv 3 \pmod 6 \\ -5, & \text{si } n \equiv 4 \pmod 6 \\ -25, & \text{si } n \equiv 5 \pmod 6 \end{cases}$$

b) Suposem que $\overline{5}^n + \overline{5}^m = \overline{0}$ a $\mathbb{Z}_{126}$. Tenint en compte els resultats de l'apartat anterior, les úniques possibilitats són $\overline{1} - \overline{1}$, $\overline{5} - \overline{5}$ i $\overline{25} - \overline{25}$. És a dir, $n \equiv 0 \pmod 6$ i $m \equiv 3 \pmod 6$; $n \equiv 1 \pmod 6$ i $n \equiv 4 \pmod 6$; o $n \equiv 2 \pmod 6$ i $m \equiv 5 \pmod 6$ (o al revés). Per tant, $n - m \equiv 3$ o $n - m \equiv -3 \equiv 3$.

Suposem ara que $n - m \equiv 3 \pmod 6$ i que $n \geq m$ (el cas $m \geq n$ és similar). Llavors existeix un enter $k \geq 0$ tal que $n = m + 3 + 6k$. En tal cas, tenim:

$$\overline{5}^n = \overline{5}^{m+3+6k} = \overline{5}^m \cdot \overline{5}^3 \cdot \overline{5}^{6k} \equiv \overline{5}^m \cdot (-\overline{1}) \cdot \overline{1} = -\overline{5}^m$$

i, per tant, $\overline{5}^n + \overline{5}^m = \overline{0}$.

2.59 Examen de recuperació del primer parcial 09/06/2017

328

a) $\forall\, a\ \exists\, b\ (a^2 - b^2 = x)$.

b) $\neg\forall\, a\ \exists\, b\ (a^2 - b^2 = x) \equiv \exists\, a\ \forall\, b\ (a^2 - b^2 \neq x)$.

c) La proposició $P(1)$ diu: $\forall\, a\ \exists\, b\ (a^2 - b^2 = 1)$. És a dir, l'equació $a^2 - b^2 = 1$ en b té solució per a tot valor del paràmetre a. Clarament això és fals com mostra el contraexemple següent: per a $a = 0$, l'equació $-b^2 = 1$ no té solució en $b \in \mathbb{R}$. La proposició $P(-1)$ diu: $\forall\, a\ \exists\, b\ (a^2 - b^2 = -1)$. És a dir, l'equació $a^2 - b^2 = -1$ en b té solució per a tot valor del paràmetre a. O equivalentment, l'equació $b^2 = a^2 + 1$ té solució en $b \in \mathbb{R}$ per a tot valor del paràmetre $a \in \mathbb{R}$. Això és clarament cert, perquè $a^2 + 1 > 0$ i podem prendre $b = \sqrt{a^2 + 1} \in \mathbb{R}$.

329

Pas base: per a $n = 1$ el primer membre de l'expressió és:

$$\sum_{k=1}^{1} \frac{1}{(2k-1)(2k+1)} = \frac{1}{1 \cdot 3} = \frac{1}{3},$$

i el segon membre val $1/3$.

Pas inductiu: fixem un enter $n \geq 1$ i suposem que (hipòtesi d'inducció):

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

Volem demostrar que la propietat és certa per a l'enter $n + 1$; és a dir:

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

Tenim:

$$\begin{aligned}
\sum_{k=1}^{n+1} \frac{1}{(2k-1)(2k+1)} &= \sum_{k=1}^{n} \frac{1}{(2k-1)(2k+1)} + \frac{1}{(2n+1)(2n+3)} \\
&= \frac{n}{2n+1} + \frac{1}{(2n+1)(2n+3)} \qquad (*) \\
&= \frac{n(2n+3)+1}{(2n+1)(2n+3)} \\
&= \frac{(2n+1)(n+1)}{(2n+1)(2n+3)} \\
&= \frac{n+1}{2n+3};
\end{aligned}$$

on a (*) hem aplicat la hipòtesi d'inducció.

Pel principi d'inducció, la propietat és certa per a toto enter $n \geq 1$.

2.60 Examen de recuperació del segon parcial 09/06/2017

330

a) Sigui (x, y) qualsevol. Tenim:

$$\begin{aligned}
(x, y) \in (A \times B) \setminus (A \times C) &\Leftrightarrow (x, y) \in A \times B \wedge (x.y) \notin A \times C \\
&\Leftrightarrow x \in A \wedge y \in B \wedge \neg(x \in A \wedge y \in C) \\
&\Leftrightarrow x \in A \wedge y \in B \wedge (x \notin A \vee y \notin C) \\
&\Leftrightarrow (x \in A \wedge y \in B \wedge x \notin A) \vee (x \in A \wedge y \in B \wedge y \notin C) \\
&\Leftrightarrow (x \in A \wedge y \in B \wedge y \notin C) \\
&\Leftrightarrow x \in A \wedge y \in B \setminus C \\
&\Leftrightarrow (x, y) \in A \times (B \setminus C).
\end{aligned}$$

Observació: hem aplicat les definicions d'operacions de conjunts i equivalències de lògica de proposicions, i per tant a tot arreu hem escrit equivalències.

b) Basta demostrar les dues implicacions: $A \subseteq B \Rightarrow \mathcal{P}(A) \subseteq \mathcal{P}(B)$ i $\mathcal{P}(A) \subseteq \mathcal{P}(B) \Rightarrow A \subseteq B$.

Suposem que $A \subseteq B$ i sigui $X \in \mathcal{P}(A)$. Llavors $X \subseteq A$ i com que $A \subseteq B$ i la relació d'inclusió és transitiva, tenim que $X \subseteq B$. Per tant, $X \in \mathcal{P}(B)$.

Suposem ara que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$. Tenim que $A \in \mathcal{P}(A)$ i per hipòtesi tenim que $A \in \mathcal{P}(B)$; és a dir, $A \subseteq B$.

331

a) Sigui $x \in \mathbb{R}$, $x \neq 1$. Llavors $\frac{1}{x-1} + 2$ és un nombre real. Suposem que és 2. Llavors tenim:

$$\frac{1}{x-1} + 2 = 2 \Rightarrow \frac{1}{x-1} = 0 \Rightarrow 1 = 0,$$

que és absurd. Per tant, $f(x) \in \mathbb{R} \setminus \{2\}$.

b) Siguin x, x' nombres reals diferents de 1 i suposem que $f(x) = f(x')$. Llavors tenim:

$$\frac{1}{x-1} + 2 = \frac{1}{x'-1} + 2 \Rightarrow \frac{1}{x-1} = \frac{1}{x'-1} \Rightarrow x - 1 = x' - 1 \Rightarrow x = x'.$$

Per tant, f és injectiva.

c) Per definició d'aplicació exhaustiva, basta demostrar que donat $y \in \mathbb{R} \setminus \{2\}$ arbitrari, existeix un $x \in \mathbb{R} \setminus \{1\}$ tal que $f(x) = y$. Tenim:

$$\begin{aligned}
f(x) = y \Leftrightarrow \frac{1}{x-1} + 2 = y \Leftrightarrow \frac{1}{x-1} = y - 2 \qquad (1)\\
\Leftrightarrow x - 1 = \frac{1}{y-2} \Leftrightarrow x = \frac{1}{y-2} + 1,
\end{aligned}$$

(1): perquè hem suposat que $y \neq 2$. Ara veiem que la x que hem obtingut és diferent de 1. En efecte, si $x = 1$, llavors:

$$\frac{1}{y-2} + 1 = x = 1 \Rightarrow \frac{1}{y-2} = 0 \Rightarrow 1 = 0,$$

que és absurd. Per tant, l'aplicació és exhaustiva.

d) Hem vist que f és injectiva i exhaustiva; per tant, f és bijectiva i conseqüentment f té inversa. Al càlcul que hem fet per a provar que f és exhaustiva, hem trobat de fet l'aplicació inversa de f:

$$f^{-1}(x) = \frac{1}{x-2} + 1.$$

2.61 Examen de reavaluació 10/07/2017

332 Per reducció a l'absurd. Suposem que $\sqrt[n]{p}$ és racional i arribarem a una contradicció. Si $\sqrt[n]{p}$ és racional, llavors $\sqrt[n]{p} = \frac{r}{s}$ per certs enters r i $s \neq 0$ tals que $\mathrm{mcd}(r, s) = 1$. Tenim que $p = r^n/s^n$; és a dir, $ps^n = r^n$. Com que $p \mid r^n$, pel lema d'Euclides, $p \mid r$. Així doncs, $r = pr_1$ i $r^n = p^n r_1^n$, per a un cert enter r_1. Per tant, $ps^n = p^n r_1^n$ o $s^n = p^{n-1} r_1^n$. Com que $p \mid p^{n-1} r_1^n$ (recordem que $n \geq 2$), tindrem que $p \mid s^n$. Una altra vegada pel lema d'Euclides tenim que $p \mid s$. I ja hem arribat a una contradicció: teníem que $\mathrm{mcd}(r, s) = 1$ i ara hem vist que $p \mid r$ i $p \mid s$.

333

a) Una relació d'equivalència és aquella que és reflexiva, simètrica i transitiva. Veiem que en el nostre cas es compleix cada una d'aquestes propietats.

- $\equiv$ reflexiva vol dir que per a tot element $a \in A$ se satisfà $a \equiv a$. En altres paraules, hem de veure que $f(a) = f(a)$ per a tot $a \in A$, que és cert.
- $\equiv$ simètrica vol dir que per a cada $a_1, a_2 \in A$, si $a_1 \equiv a_2$, llavors $a_2 \equiv a_1$. En altres paraules, si $f(a_1) = f(a_2)$, llavors $f(a_2) = f(a_1)$, que és cert.
- $\equiv$ transitiva vol dir que per a cada $a_1, a_2, a_3 \in A$, si $a_1 \equiv a_2$ i $a_2 \equiv a_3$, llavors $a_1 \equiv a_3$. En altres paraules, si $f(a_1) = f(a_2)$ i $f(a_2) = f(a_3)$, llavors $f(a_1) = f(a_3)$, que és cert.

b) L'aplicació $\tilde{f}$ està definida sobre el conjunt $A/\equiv$; és a dir, $\tilde{f}$ està definida sobre classes d'equivalència. Però en la definició de $\tilde{f}$ usem representants. Dir que $\tilde{f}$ està ben definida, doncs, vol dir que la seva definició no depèn del representant elegit. En altres paraules, hem de veure que si $[a_1] = [a_2]$, llavors $f(a_1) = f(a_2)$. Veiem-ho: $[a_1] = [a_2] \Rightarrow a_1 \equiv a_2 \Rightarrow f(a_1) = f(a_2)$.

$\tilde{f}$ injectiva vol dir que si $\tilde{f}([a_1]) = \tilde{f}([a_2])$, llavors $[a_1] = [a_2]$. Veiem-ho: $\tilde{f}([a_1]) = \tilde{f}([a_2]) \Rightarrow f(a_1) = f(a_2) \Rightarrow a_1 \equiv a_2 \Rightarrow [a_1] = [a_2]$.

334

Pas bàsic: $n = 2$. Hem de veure que $(2+2)! \geq \frac{4^{2+1}}{7}$; és a dir, hem de veure que $4! \geq \frac{4^3}{7}$, desigualtat que és certa perquè $4! = 24$ i $4^3/7 = 64/7$.

Pas inductiu: sigui $n \geq 2$ un enter. Suposem que $(n+2)! \geq \frac{4^{n+1}}{7}$ (hipòtesi d'inducció). Volem demostrar que $(n+3)! \geq \frac{4^{n+2}}{7}$. Procedim:

$$(n+3)! = (n+3) \cdot (n+2)! \geq (n+3) \cdot \frac{4^{n+1}}{7} \geq 4 \cdot \frac{4^{n+1}}{7} = \frac{4^{n+2}}{7},$$

la primera desigualtat per hipòtesi d'inducció, i la segona perquè $n \geq 2 \geq 1$.

335 En primer lloc, comprovem primer si l'equació diofàntica té solució: és a dir, mirem si $\text{mcd}(2005, 1015) \mid 15$. Comencem amb el càlcul del mcd mitjançant l'algorisme d'Euclides:

Q		1	1	39	1	1	
R	2005	1015	990	25	15	10	5

Com que el mcd és 5 i $5 \mid 15$, l'equació diofàntica té solució. Simplifiquem-la:

$$401x + 203y = 3, \quad \text{mcd}(401, 203) = 1.$$

Per a resoldre-la, busquem primer una solució particular mitjançant la identitat de Bézout, identitat que obtenim a partir de l'algorisme d'Euclides estès.

X	1	0	1	-1	40	-41	81
Y	0	1	-1	2	-79	81	-160
Q		1	1	39	1	1	
R	401	203	198	5	3	2	1

Identitat de Bézout: $401 \cdot 81 + 203 \cdot (-160) = 1$. Multiplicant per 3, obtenim la solució particular $x_0 = 243$, $y_0 = -480$. Per tant, la solució general és:

$$x = 243 - 203t,$$
$$y = -480 + 401t,$$

amb $t \in \mathbb{Z}$.

Si volem que $x = 243 - 203t \geq 0$, ha de ser $t \leq \frac{243}{203}$. I, com que $t \in \mathbb{Z}$, això equival a $t \leq 1$. Per a obtenir una x mínima amb aquestes condicions, agafem $t = 1$. La solució demanada és $x = 40$, $y = -79$.