José L. Bueso
Departamento de Álgebra

Grado en Matemáticas

ALGEBRA I

NEWS

WUOLAH

LUN 01 OCT

Noticias para el mundo universitario.

nº 4. Semana del 1 al 7

6 razones por las que las microempresas resultan más atractivas para los recién graduados.

Fuente: Universia

Las microempresas: la decisión más práctica y atractiva.

A pesar de que todos tienen muy claro el posicionamiento de los líderes de cada sector y actividad y los volúmenes de negocio que mueven, a la hora de pensar en una formación laboral eficaz, creen que las empresas de menor tamaño son la mejor opción para ir aprendiendo una profesión y estos son los motivos:

1. Visión global del negocio: Las empresas de pequeño tamaño son mejores entes para entender el funcionamiento de los diferentes mecanismos empresariales.

2. Aprendizaje experiencial: Es más fácil poder asistir y colaborar en las actividades de los profesionales que se encargan de tareas importantes.

3. Campo de acción de las microempresas: Resulta más sencillo entender el diseño de las estrategias cuando se conoce mejor el contexto en el que la empresa actúa.

4. Mando de toma de decisiones cercano: Posiblemente, el contacto con el gerente o director sea constante, lo que supone conocer las decisiones y cómo se han tomado.

5. Familiaridad y cercanía: Suele tratarse de ambientes laborales más amigables y donde es más sencillo entablar una relación con los compañeros y trabajar en equipo.

6. Espacio para afianzar competencias: Trabajar en una microempresa da la oportunidad de desarrollar diferentes competencias y analizar qué necesitas para controlar mejor tu profesión y trabajar de forma más efectiva.Por tanto, los egresados ven las microempresas como los mejores lugares donde realizar una formación laboral eficaz, ganar confianza y comenzar a desarrollar su iniciativa profesional.

Grandes empresas más atractivas para los egresados:La empresa automovilística Mercedes-Benz se lleva el primer premio en la valoración de lo profesionales, seguida de otras grandes empresas, como Nestlé, Telefónica, Repsol o Bayer. La envergadura de estas empresas, el reconocimiento de marca y su carácter multinacional son algunos de los elementos que resultan llamativos a los profesionales, sobre todo a los egresados

La postura correcta para sentarse en clase: Algunos consejos:

1. Posición
Es importante que te puedas sentar con los pies en el suelo y los brazos descansando cómodamente en el escritorio sin tener que inclinarte ni estirarte. Si tiene acceso a escritorios ajustables, ¡perfecto!, ya que este tipo de escritorios se pueden mover para adaptarse a las necesidades de cada estudiante en particular. En el mundo real, no todos los escritorios son ajustables, por lo que existen algunas soluciones simples que te pueden ayudar; agrega libros que hagan de escalón debajo de los pies para que no cuelguen o buscar una silla más alta, por ejemplo. Si agregas algún soporte debajo de los pies, asegúrate de que las rodillas no estén por encima de 90 grados para una alineación óptima.

2. Descansos de movimiento
El movimiento es esencial para promover una buena postura en el aula. Inquietarse y moverse en la silla hace que se pierda una buena postura, así como la atención. Es muy difícil enfocarse en una buena postura cuando estás inquieto/a.
Inquietarse a menudo es un signo de necesidad de moverse. Es recomendable hacer descansos razonables y levantarse para descansar de estar sentado/a.

3. Espalda recta
Cuando te sientes, trata de mantener la espalda recta. Lo ideal es que pongas tu espalda contra el respaldo de la silla. Recuerda que tus rodillas deben formar un ángulo recto y que no es nada recomendable que cruces las piernas.

4. Estiramiento y relajación de músculos.
Para conseguir una buena postura en lapsos de tiempo prolongados se recomienda también inclinarse hacia atrás varias veces para estirar los músculos y ayudarlos a relajarse. De esta manera tener siempre la postura correcta es más fácil.La postura correcta para sentarse en clase es crucial de cara a evitar posibles problemas de espalda, además recuerda que ayuda a la concentración y motiva al aprendizaje.

José L. Bueso

Ejercicios

Álgebra 1

Grado en Matemáticas

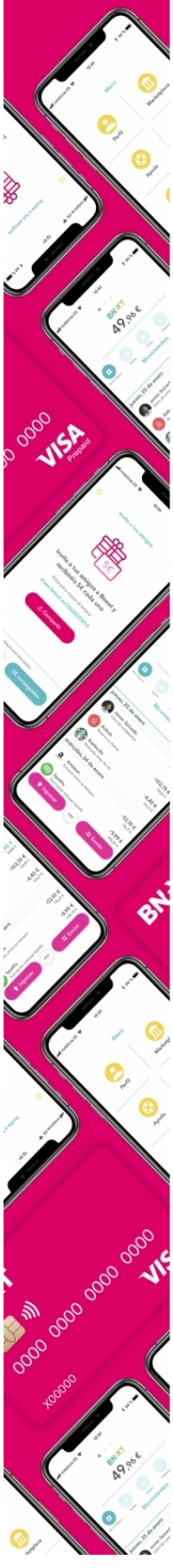
Facultad de Ciencias
Universidad de Granada. (http://prado.ugr.es/moodle/).

Índice general

BNEXT

10€ GRATIS

AL ACTIVAR TU TARJETA BNEXT



Capítulo

1

Teoría de conjuntos.

Ejercicios

Ejercicio 1.1

Si A y B son subconjuntos de un conjunto X demostrar:

i) $A \cap B = \emptyset \Leftrightarrow A \subseteq \overline{B} \Leftrightarrow B \subseteq \overline{A}$

ii) $A \cup B = X \Leftrightarrow \overline{B} \subseteq A \Leftrightarrow \overline{A} \subseteq B$

Solución:

i)
$A \cap B = \emptyset \Leftrightarrow A \subseteq \overline{B}$
$A \cap B = \emptyset \Rightarrow A \subseteq \overline{B})$
Sea $x \in A$, *entonces* $x \notin B$, *de donde* $x \in \overline{B}$.
$A \cap B = \emptyset \Leftarrow A \subseteq \overline{B})$
Si $A \cap B \neq \emptyset$, *entonces existe* $x \in A$ *y* $x \in B$, *luego existe* $x \in A$ *y* $x \notin \overline{B}$, *lo que es una contradicción.*
$A \subseteq \overline{B} \Leftrightarrow B \subseteq \overline{A}$
$A \subseteq \overline{B} \Rightarrow B \subseteq \overline{A})$
Sea $x \in B$, *entonces* $x \notin \overline{B}$, *de donde* $x \notin A$ *y así* $x \in \overline{A}$.
$A \subseteq \overline{B} \Leftarrow B \subseteq \overline{A})$
Sea $x \in A$, *entonces* $x \notin \overline{A}$, *de donde* $x \notin B$ *y así* $x \in \overline{B}$.
ii) Basta tomar complementarios y aplicar i).

Ejercicio 1.2

Sea X un conjunto y A, B, C subconjuntos de X. Demostrar que si $A \cup B \subseteq A \cup C$ y $A \cap B \subseteq A \cap C$ entonces $B \subseteq C$. Como consecuencia demostrar que si $A \cup B = A \cup C$ y $A \cap B = A \cap C$ entonces $B = C$.

Solución:

Sea $x \in B$, *entonces* $x \in A \cup B$ *y por tanto* $x \in A \cup C$. *Si* $x \in A$, *entonces* $x \in B \cap C$ *y por tanto* $x \in A \cap C$. *Así* $x \in C$. *Si* $x \in C$, *ya está.*
La consecuencia es inmediata, ya que la igualdad de conjuntos se corresponde a la doble inclusión.

Ejercicio 1.3

Verificar las siguientes fórmulas donde A, B y C son subconjuntos de un conjunto X y $A \setminus C = \{x \in X; x \in A \wedge x \notin C\}$:

i) $(A \setminus C) \setminus (B \setminus C) = (A \setminus B) \setminus C$

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

iii) $(A \setminus C) \cap (B \setminus C) = (A \cap B) \setminus C$

iv) $(A \setminus B) \setminus (A \setminus C) = A \cap (C \setminus B)$

v) $(A \setminus B) \cup (A \setminus C) = A \setminus (B \cap C)$

vi) $(A \setminus B) \cap (A \setminus C) = A \setminus (B \cup C)$

Solución:

i) Sea $x \in (A \setminus C) \setminus (B \setminus C)$. *Entonces* $x \in (A \setminus C)$, $x \notin (B \setminus C)$. *Así* $(x \in A, x \notin C)$, $(x \notin B$ *ó* $(x \in B, x \in C)$. *Esto último no puede ocurrir, luego de* $x \in A \setminus B$ *y* $x \notin C$, *deducimos que* $x \in (A \setminus B) \setminus C$.
Sea $x \in (A \setminus B) \setminus C$. *Entonces* $x \in (A \setminus B)$, $x \notin C$, *esto es,* $x \in A$, $x \notin B$, $x \notin C$. *Así* $x \in (A \setminus C)$, $x \notin (B \setminus C)$ *y por tanto* $x \in (A \setminus C) \setminus (B \setminus C)$.
ii) Sea $x \in (A \setminus C) \cup (B \setminus C)$. *Entonces* $x \in (A \setminus C)$ *ó* $x \in (B \setminus C)$. *Así* $(x \in A, x \notin C)$ *ó* $(x \in B, x \notin C)$. *Por tanto* $x \in A \cup B$, $x \notin C$ *y por consiguiente* $x \in (A \cup B) \setminus C$.
Sea $x \in (A \cup B) \setminus C$. *Entonces* $x \in A \cup B$, $x \notin C$, *de donde* $(x \in A$ *ó* $x \in B)$, $x \notin C$. *Así* $x \in A \setminus C$ *ó* $x \in B \setminus C$. *Por tanto* $x \in (A \setminus C) \cup (B \setminus C)$.
iii) Sea $x \in (A \setminus C) \cap (B \setminus C)$. *Entonces* $x \in (A \setminus C)$ *y* $x \in (B \setminus C)$. *Así* $(x \in A, x \notin C)$ *y* $(x \in B, x \notin C)$. *Por tanto* $x \in A \cap B$, $x \notin C$ *y por consiguiente* $x \in (A \cap B) \setminus C$.
Sea $x \in (A \cap B) \setminus C$. *Entonces* $x \in A \cap B$, $x \notin C$, *de donde* $(x \in A$ *y* $x \in B)$, $x \notin C$. *Así* $x \in A \setminus C$ *y* $x \in B \setminus C$. *Por tanto* $x \in (A \setminus C) \cap (B \setminus C)$.
iv) Sea $x \in (A \setminus B) \setminus (A \setminus C)$. *Entonces* $x \in (A \setminus B)$ *y* $x \notin (A \setminus C)$. *Así* $(x \in A, x \notin B)$ *y* $(x \in C)$. *Por tanto* $x \in A$, $x \in (C \setminus B)$ *y por consiguiente* $x \in A \cap (C \setminus B)$.
Sea $x \in A \cap (C \setminus B)$. *Entonces* $x \in A$, $x \in (C \setminus B)$, *de donde* $x \in A$ *y* $(x \in C, x \notin B)$. *Así* $x \in (A \setminus B)$ *y* $x \in (A \setminus C)$. *Por tanto* $x \in (A \setminus B) \cap (A \setminus C)$.
v) Sea $x \in (A \setminus B) \cup (A \setminus C)$. *Entonces* $x \in (A \setminus B)$ *ó* $x \notin (A \setminus C)$. *Así* $(x \in A, x \notin B)$ *ó* $(x \in A$ *y* $x \notin C)$. *Por tanto* $x \in A$, $x \notin (B \cap C)$ *y por consiguiente* $x \in A \setminus (B \cap C)$.
Sea $x \in A \setminus (B \cap C)$. *Entonces* $x \in A$, $x \notin (B \cap C)$, *de donde* $x \in A$ *y* $(x \notin B$ *ó* $x \notin C)$. *Así* $x \in (A \setminus B)$ *ó* $x \in (A \setminus C)$. *Por tanto* $x \in (A \setminus B) \cup (A \setminus C)$.
vi) Sea $x \in (A \setminus B) \cap (A \setminus C)$. *Entonces* $x \in (A \setminus B)$ *y* $x \notin (A \setminus C)$. *Así* $(x \in A, x \notin B)$ *y* $(x \in A$ *y* $x \notin C)$. *Por tanto* $x \in A$, $x \notin (B \cup C)$ *y por consiguiente* $x \in A \setminus (B \cup C)$.
Sea $x \in A \setminus (B \cup C)$. *Entonces* $x \in A$, $x \notin (B \cup C)$, *de donde* $x \in A$ *y* $(x \notin B$ *y* $x \notin C)$. *Así* $x \in (A \setminus B)$ *y* $x \in (A \setminus C)$. *Por tanto* $x \in (A \setminus B) \cap (A \setminus C)$.

Ejercicio 1.4

Se define la diferencia simétrica de dos subconjuntos A y B de un conjunto X por $A \triangle B = (A \setminus B) \cup (B \setminus A)$. *Demostrar que* $A \triangle B = (A \cup B) \setminus (A \cap B)$ *y que* $A \triangle B = \emptyset$ *si y solo si* $A = B$.

Solución:

$A \triangle B = (A \cup B) \setminus (A \cap B))$
Si $x \in \triangle B$, *entonces* $x \in (A \setminus B)$ *o* $x \in (B \setminus A)$. *En el primer caso* $x \in A$, $x \notin B$, *de donde* $x \in A \cup B$, $x \notin A \cap B$, *es decir* $(A \cup B) \setminus (A \cap B)$.
Si $(A \cup B) \setminus (A \cap B)$, *entonces* $x \in A \cup B$, $x \notin A \cap B$, *de donde* $x \in A$ *o* $x \in B$. *En el primer caso* $x \in A \setminus B$ *y por tanto* $x \in (A \setminus B) \cup (B \setminus A)$. *En el segundo caso* $x \in B \setminus A$ *y por tanto* $x \in (A \setminus B) \cup (B \setminus A)$.
El resto es inmediato de lo ya probado.

Ejercicio 1.5

Sean $A, B \subseteq X$. *Demostrar:*

i) $A = (A \cap B) \biguplus (A \setminus B)$ *es una representación de* A *como una unión disjunta.*

ii) $A \cup B = A \biguplus (B \setminus A)$ *es una representación de* $A \cup B$ *como una unión disjunta.*

Solución:

i) $A \subseteq (A \setminus B)$, *de donde* $A \subseteq (A \cap B) \cup (A \setminus B)$. $(A \cap B) \subseteq A$ *y* $(A \setminus B) \subseteq A$, *de donde* $(A \cap B) \cup (A \setminus B) \subseteq A$.
Además $(A \cap B) \cap (A \setminus B) = \emptyset$.
ii) $A \subseteq A \cup (B \setminus A)$ *y* $B \subseteq (B \setminus A)$, *luego* $B \subseteq A \cup (B \setminus A)$, *luego* $A \cup B \subseteq A \cup (B \setminus A)$.
$A \subseteq A \cup B$ *y* $(B \setminus A) \subseteq B$, *luego* $A \cup (B \setminus A) \subseteq A \cup B$.
Además $A \cap (B \setminus A) = \emptyset$

Ejercicio 1.6

Sean $A, B \subseteq X$. *Si* A *tiene* n *elementos y* B *tiene* m *elementos ¿Cuántos elementos tiene* $A \cup B$*?.*

Solución:

Tenemos que $\text{card}(A \cup B) = \text{card}(A) + \text{card}(B) - \text{card}(A \cap B)$.

Ejercicio 1.7

Sean $A, B \subseteq X$. *Demostrar que si* $A \subseteq B$ *entonces* $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

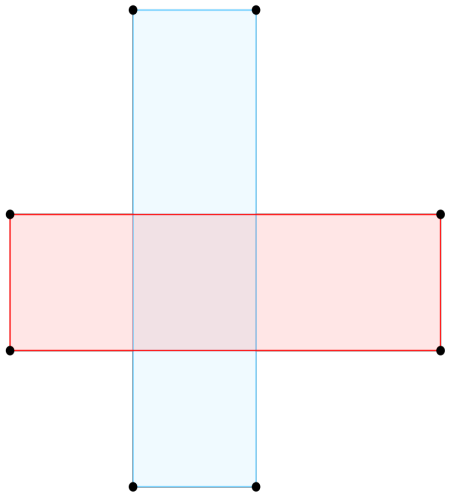
Solución:

Si $C \in \mathcal{P}(A)$, *entonces* $C \subseteq A$, *de donde* $C \subseteq B$, *y por tanto* $C \in \mathcal{P}(B)$.

Ejercicio 1.8

Se consideran los subconjuntos de $\mathbb{R}$, $A = [-1, 1]$ *y* $B = [-3, 4]$. *Describir los siguientes subconjuntos de* $\mathbb{R} \times \mathbb{R}$: $A \times B$, $B \times A$, $(A \times B) \cap (B \times A)$, $(A \times B) \setminus (B \times A)$, $(A \times B) \cup (B \times A)$.

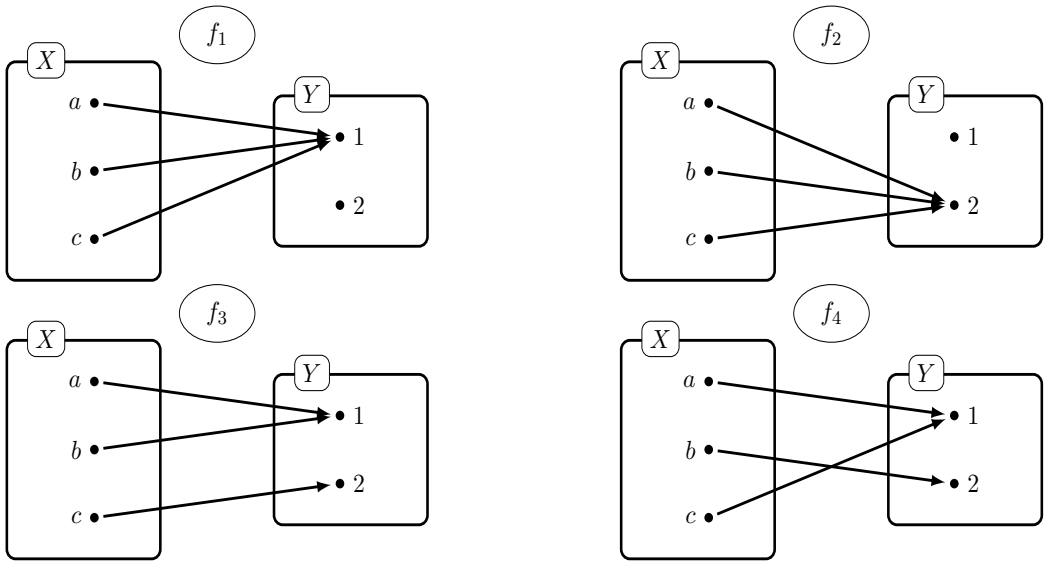
Solución:

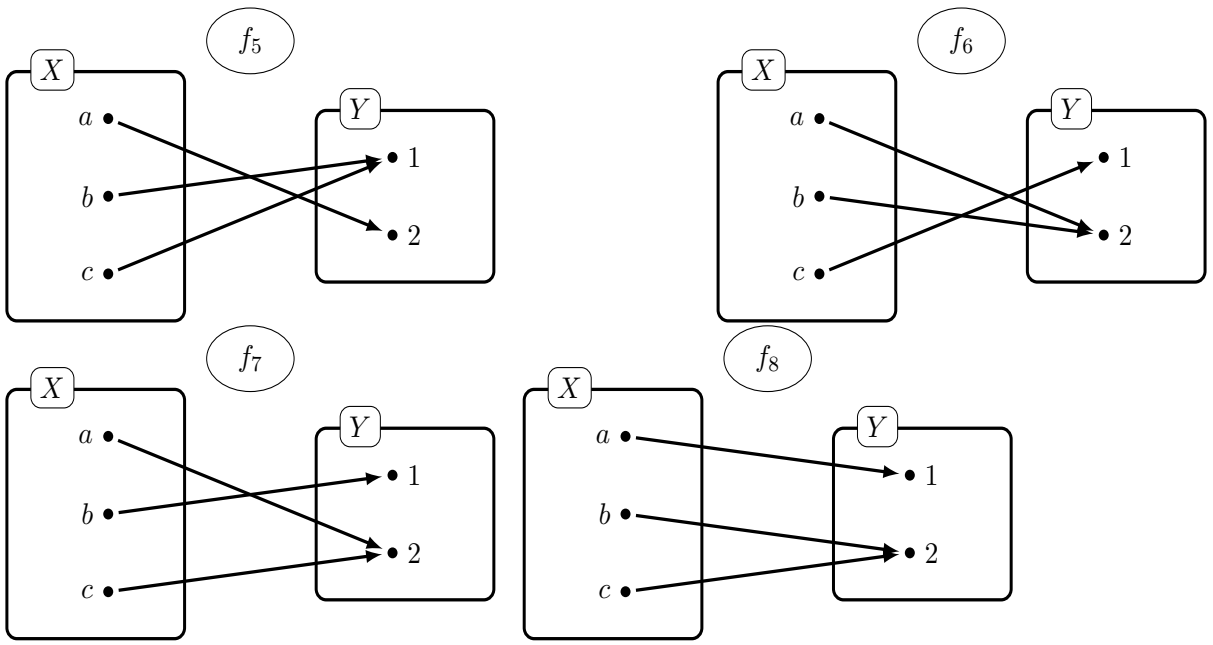


Ejercicio 1.9

Construir todas las aplicaciones del conjunto $X = \{a, b, c\}$ en el conjunto $Y = \{1, 2\}$ y clasificarlas según sean inyectivas, suprayectivas, biyectivas ó de ninguno de estos tipos.

Solución:





Ejercicio 1.10

Sea $f : \mathbb{R} \to \mathbb{R}$ definida por $f(x) = 5x - 3$. Demostrar que existe $g : \mathbb{R} \to \mathbb{R}$ tal que $gf = 1_{\mathbb{R}}$. ¿Es cierto también que $fg = 1_{\mathbb{R}}$?

Solución:

Sea $g : \mathbb{R} \to \mathbb{R}$ dada por $g(x) = \frac{1}{5}x + \frac{3}{5}$. Claramente es una aplicación y además $gf(x) = g(5x-3) = \frac{1}{5}(5x-3) + \frac{3}{5} = x = 1_{\mathbb{R}}(x)$. Además $fg(x) = f(\frac{1}{5}x + \frac{3}{5}) = 5(\frac{1}{5}x + \frac{3}{5}) - 3 = x = 1_{\mathbb{R}}(x)$.

Ejercicio 1.11

Sea $A \subseteq X$, $B \subseteq Y$ y $f : X \to Y$ una aplicación. Demostrar:

i) $f_*(f^*(B)) \subseteq B$ y se da la igualdad si f es suprayectiva.

ii) $A \subseteq f^*(f_*(A))$ y se da la igualdad si f es inyectiva.

Solución:

i) Sea $y \in f_*(f^*(B))$. Entonces existe $x \in f^*(B)$, tal que $y = f(x) \in B$.
$\Rightarrow$ Sea $y \in Y$ y sea $B = \{y\}$. Si $f^*(B) \neq \emptyset$, existe $x \in f^*(B) \subseteq X$, tal que $y = f(x) \in B$.
Si $f^*(B) = \emptyset$, entonces $B = f_*(f^*(B)) = f_*(\emptyset) = \emptyset$, lo que es una contradicción.
$\Leftarrow$ Sea $b \in B$. Ya que f es suprayectiva existe $x \in X$ tal que $f(x) = b$. Así $x \in f^*(B)$ y por tanto $b = f(x) \in f_*(f^*(B))$ y tenemos la igualdad $f_*(f^*(B)) = B$.
ii) Sea $a \in A$. Entonces $f(a) \in f_*(A)$, de donde $a \in f^*(f_*(A))$.
$\Rightarrow$ Sean $x, x' \in X$ con $f(x) = f(x')$. Sea $A = \{x\}$, entonces $f_*(A) = \{f(x)\}$ y $x, x' \in f^*(f_*(A)) = A$, de donde $x = x'$.
$\Leftarrow$ Sea $x \in f^*(f_*(A))$, Entonces $f(x) \in f_*(A)$ y por tanto existe $a \in A$ tal que $f(x) = f(a)$. Como f es inyectiva $x = a \in A$.

Ejercicio 1.12

Se consideran las aplicaciones $A \xrightarrow{f} B \xrightarrow{g} C$ *y* $X \xrightarrow{h} Y \xrightarrow{k} Z$ *. Demostrar que* f *y* h *inducen una única aplicación* $f \times h : A \times X \to B \times Y$ *verificando que* $f\,\mathrm{pr}_A = \mathrm{pr}_B(f \times h)$ *y* $h\,\mathrm{pr}_X = \mathrm{pr}_Y(f \times h)$. *Demostrar que* $(g \times k)(f \times h) = (gf) \times (kh)$.

Solución:

$$\begin{array}{ccc} A \times B & \xrightarrow{f\times h} & B \times Y \\ \downarrow{\scriptstyle pr_A} & & \downarrow{\scriptstyle pr_B} \\ A & \xrightarrow{f} & B \end{array} \qquad \begin{array}{ccc} A \times B & \xrightarrow{f\times h} & B \times Y \\ \downarrow{\scriptstyle pr_X} & & \downarrow{\scriptstyle pr_Y} \\ X & \xrightarrow{h} & Y \end{array}$$

Definamos $f \times h : A \times X \to B \times Y : (a, x) \mapsto (f(a), h(y)$. *Es aplicación, ya que si* $(a, x) = (a', x')$ *entonces* $a = a'$ *y* $x = x'$, *de donde* $f(a) = f(a')$ *y* $h(x) = h(x')$ *y así* $(f(a), h(x)) = (f(a'), h(x'))$. *Además,* $pr_B(f \times h)(a, x) = pr_B(f(a), h(x)) = f(a) = fpr_A(a, x)$ *y* $pr_Y(f \times h)(a, x) = pr_Y(f(a), h(x)) = h(x) = hpr_X(a, x)$.
Si $\varphi : A \times X \to B \times Y : (a, x) \mapsto (b, y)$, *verifica entonces* $b = pr_B(b, y) = pr_B\varphi(a, x) = fpr_A(a, x) = f(a)$ *y* $y = pr_Y(b, y) = pr_Y\varphi(a, x) = hpr_X(a, x) = h(x)$. *Así* $\varphi(a, x) = (f(a), h(x)) = (f \times h)(a, x)$.
También $(g \times k)(f \times h)(a, x) = (g \times k)(f(a), h(x)) = (gf(a), kh(x)) = (gf \times kh)(a, x)$.

Ejercicio 1.13

Sea $f : X \to Y$ *una aplicación,* $A \subseteq X$ *y* $B \subseteq Y$ *. Demostrar* $f_*(A \cap f^*(B)) = f_*(A) \cap B$.

Solución:

Sea $y \in f_*(A \cap f^*(B))$, *entonces* $y = f(x)$ *con* $x \in A \cap f^*(B)$, *de donde* $x \in A$ *y* $x \in f^*(B)$. *Así* $y = f(x) \in f_*(A)$, *e* $y = f(x) \in B$, *de donde* $y \in f_*(A) \cap B$.
Sea $y \in f_*(A) \cap B$, *de donde* $y \in f_*(A)$ *e* $y \in B$. *Así* $y = f(x)$ *con* $x \in A$, *y* $x \in f^*(B)$, *de donde* $x \in A \cap f^*(B)$ *y así* $y \in f(x) \in f_*(A \cap f^*(B))$.

Ejercicio 1.14

Sea $f : X \to Y$ *una aplicación. Demostrar que son equivalentes las siguientes afirmaciones:*

a) f *es inyectiva*

b) *Para cualesquiera* $A, B \in \mathcal{P}(X)$, $f_*(A \cap B) = f_*(A) \cap f_*(B)$.

Solución:

a) $\Rightarrow$ b) *Sean* $A, B \in \mathcal{P}(X)$. *Si* $f(x) \in f_*(A \cap B)$, *entonces* $x \in A \cap B$, *de donde* $f(x) \in f_*(A)$ *y* $f(x) \in f_*(B)$ *y por tanto* $f(x) \in f_*(A) \cap f_*(B)$. *Recíprocamente, si* $f(x) \in f_*(A) \cap f_*(B)$, *entonces* $x \in A$ *y* $x \in B$, *de donde* $x \in A \cap B$) *y por tanto* $f(x) \in f_*(A \cap B)$.
b) $\Rightarrow$ a) *Sean* $x, x' \in X$ *tales que* $f(x) = f(x')$.

Ejercicio 1.15

Sean $f : X \to Y$ y $g : Y \to Z$ dos aplicaciones y sea $h = gf$ la composición de dichas aplicaciones. Demostrar:

i) Si h es inyectiva entonces f es inyectiva.

ii) Si h es suprayectiva entonces g es suprayectiva.

iii) Si h es inyectiva y f es suprayectiva entonces g es inyectiva.

iv) Si h es suprayectiva y g es inyectiva entonces f es suprayectiva.

Solución:

i) Si $f(x) = f(x')$, entonces $h(x) = g(f(x)) = g(f(x')) = h(x')$, de donde $x = x'$.
ii) Sea $z \in Z$. Como h es suprayectiva, existe $x \in X$ tal que $z = h(x) = g(f(x))$. Por tanto g es suprayectiva.
iii) Supongamos que $g(y) = g(y')$ donde $y, y' \in Y$. Como f es suprayectiva existen $x, x' \in X$ tales que $y = f(x)$ e $y' = f(x')$. Por tanto $h(x) = g(f(x)) = g(y) = g(y') = g(f(x')) = h(x`)$. Como $h$ es intectiva tenemos $x = x`$ y así $y = f(x) = f(x') = y'$.
iv) Sea $y \in Y$. Entonces $g(y) \in Z$ y como h es suprayectiva, existe $x \in X$ tal que $h(x) = g(y)$. Así $g(f(x)) = g(y)$ y como g es inyectiva tenemos que $y = f(x)$, esto es, f es suprayectiva.

Ejercicio 1.16

Sean las aplicaciones $f : X \to Y$, $g : Y \to Z$ y $h : Z \to X$ tales que hgf es inyectiva, gfh es inyectiva y fhg es suprayectiva. Demostrar que las aplicaciones f, g y h son biyectivas

Solución:

Probaremos que son biyectivas, demostrando que son inyectivas y suprayectivas. f es inyectiva.)
Supongamos que $f(x) = f(x')$ con $x, x' \in X$. Entonces $hgf(x) = hgf(x')$, y por tanto $x = x'$.
f es suprayectiva.)
Sea $y \in Y$. Existe $y' \in Y$ tal que $y = fhg(y')$, esto es existe $hg(y') \in X$ tal que $y = f(hg(y'))$.
h es inyectiva.)
Supongamos que $h(z) = h(z')$ con $z, z' \in Z$. Entonces $gfh(z) = gfh(z')$, de donde $z = z'$.
h es suprayectiva.)
Sea $x \in X$.
g es inyectiva.)
Supongamos que $g(y) = g(y')$ con $y, y' \in Y$. Entonces $fhg(y) = fhg(y')$, de donde $hg(y) = hg(y')$ y así $y = y'$.

Ejercicio 1.17

Dar ejemplos de relaciones binarias en un conjunto que verifiquen una sola de las siguientes propiedades: reflexiva, simétrica, antisimétrica, transitiva.

Solución:

i) Sea $A = \{a, b, c\}$ *y* $\mathcal{R} = \{(a, a), (b, b), (c, c), (a, b), (b, c)\}$.
ii) Sea $A = \{a, b, c\}$ *y* $\mathcal{R} = \{(a, b), (b, a)\}$.
iii) Sea $A = \{a, b, c\}$ *y* $\mathcal{R} = \{(a, a), (a, b), (b, c)\}$.
iv) Sea $A = \{a, b, c\}$ *y* $\mathcal{R} = \{(a, b), (b, c), (a, c)\}$.

Ejercicio 1.18

Demostrar que las siguientes relaciones en $\mathbb{R} \times \mathbb{R}$ *son de equivalencia y describir geométricamente las clases de equivalencia:*

i) $(a, b)\mathcal{R}(c, d) \Leftrightarrow a^2 + b^2 = c^2 + d^2$

ii) $(a, b)\mathcal{R}(c, d) \Leftrightarrow ab = cd$

Solución:

i)
Reflexiva.) $(a, b)\mathcal{R}(a, b)$, *ya que* $a^b + b^2 = a^2 + b^2$.
Simétrica.) Si $(a, b)\mathcal{R}(c, d)$, *entonces* $a^2 + b^2 = c^2 + d^2$, *o lo que es lo mismo* $c^2 + d^2 = a^2 + b^2$, *esto es,* $(c, d)\mathcal{R}(a, b)$
Transitiva,) Si $(a, b)\mathcal{R}(c, d)$ *y* $(c, d)\mathcal{R}(e, f)$, *entonces* $a^2 + b^2 = c^2 + d^2$ *y* $c^2 + d^2 = e^2 + f^2$, *y por tanto* $a^2 + b^2 = e^2 + f^2$ *y así* $(a, b)\mathcal{R}(c, d)$.
El conjunto cociente es:

$$\mathbb{R} \times \mathbb{R}/\mathcal{R} = \{[(a, b)]; a^2 + b^2 = r, r \geq 0\}$$

Así es el conjunto de circunferencias de centro $(0, 0)$, *salvo el caso* $r = 0$ *que es el punto* $(0, 0)$.
ii)
Reflexiva.) $(a, b)\mathcal{R}(a, b)$, *ya que* $ab = ab$.
Simétrica.) Si $(a, b)\mathcal{R}(c, d)$, *entonces* $ab = cd$, *o lo que es lo mismo* $cd = ab$, *esto es,* $(c, d)\mathcal{R}(a, b)$
Transitiva,) Si $(a, b)\mathcal{R}(c, d)$ *y* $(c, d)\mathcal{R}(e, f)$, *entonces* $ab = cd$ *y* $cd = ef$, *y por tanto* $ab = ef$ *y así* $(a, b)\mathcal{R}(c, d)$.
El conjunto cociente es:

$$\mathbb{R} \times \mathbb{R}/\mathcal{R} = \{[(a, b)]; ab = k\}$$

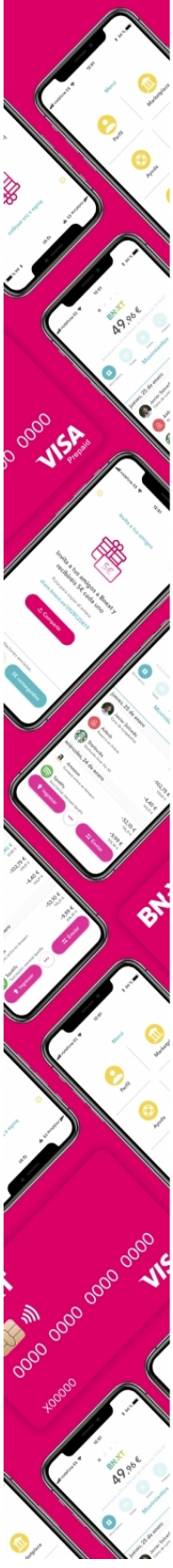
Así es el conjunto de hipérbolas de centro $(0, 0)$, *salvo el caso* $k = 0$ *que son los ejes de coordenadas.*

Ejercicio 1.19

Sea $f : \mathbb{R} \to \mathbb{R}$ *la aplicación definida por* $f(x) = x^2$. *Determinar* $\mathcal{R}_f$ *y el conjunto cociente de* $\mathbb{R}$ *bajo esta relación.*

Solución:

$x\mathcal{R}_f y$ *si y sólo si* $f(x) = f(y)$, *si y sólo si* $x^2 = y^2$ *si y sólo si* $y = \pm x$. *Así* $[x] = \{y \in \mathbb{R}; y = \pm x\}$.
Veamos que $\varphi : \mathbb{R}/\mathcal{R}_f \to \mathbb{R}^+ : [x] \mapsto |x|$ *es una aplicación biyectiva.*
Es aplicación: Si $[x] = [y]$ *entonces* $y = \pm x$ *de donde* $|x| = |y|$.



Es inyectiva: Si $|x| = |y|$ *entonces* $y = \pm x$ *de donde* $[x] = [y]$.
Es suprayectiva: Sea $x \in \mathbb{R}^+$, *entonces* $\varphi([x]) = |x| = x$.

Ejercicio 1.20

Se considera la aplicación $f : \mathbb{N} \to \mathbb{N}$ *dada por* $f(x) = E(+\sqrt{x})$ *donde* E *denota "parte entera".*

i) Demostrar que la relación $x \sim y \Leftrightarrow E(+\sqrt{x}) = E(+\sqrt{y})$ *es una relación de equivalencia en* $\mathbb{N}$.

ii) Calcular la clase de equivalencia de los elementos 1,2 y 5.

iii) Calcular la clase de equivalencia de $n \in \mathbb{N}$.

iv) Demostrar que f *es suprayectiva.*

v) Hallar la descomposición canónica de f.

Solución:

i) Reflexiva.
$x \sim x$, *ya que* $E(+\sqrt{x}) = E(+\sqrt{x})$.
Simétrica.
Si $x \sim y$, *entonces* $E(+\sqrt{x}) = E(+\sqrt{y})$, *de donde* $E(+\sqrt{y}) = E(+\sqrt{x})$ *y por tanto* $y \sim x$.
Transitiva.
Si $x \sim y$,*e* $y \sim z$, *entonces* $E(+\sqrt{x}) = E(+\sqrt{y})$ *y* $E(+\sqrt{y}) = E(+\sqrt{z})$, *de donde* $E(+\sqrt{x}) = E(+\sqrt{z})$ *y por tanto* $x \sim z$.
ii) $[1] = \{x \in \mathbb{N}; x \sim 1\} = \{x \in \mathbb{N}; E(+\sqrt{x}) = 1\} = \{1, 2, 3\}$
$[2] = [1]$
$[5] = \{x \in \mathbb{N}; x \sim 5\} = \{x \in \mathbb{N}; E(+\sqrt{x}) = 2\} = \{4, 5, 6, 7, 8\}$
iii) Sea $n \in \mathbb{N}$ *y denotemos* $m = E(+\sqrt{n})$. *Veamos que* $[n] = \{x \in \mathbb{N}; x \in [m^2, (m+1)^2[\}$. *Si* $x \in [n]$, *entonces* $E(+\sqrt{x}) = E(+\sqrt{n}) = m$, *Por tanto* $m \leq \sqrt{x} < m + 1$, *de donde* $m^2 \leq x < (m+1)^2$, *esto es,* $x \in [m^2, (m+1)^2[$.
Recíprocamente, si $x \in [m^2, (m+1)^2[$, *entonces* $m^2 \leq x < (m+1)^2$. *Por tanto* $m \leq \sqrt{x} < m + 1$, *de donde* $E(\sqrt{x}) = m = E(\sqrt{n})$ *y así* $x \in [n]$.
iv) Sea $n \in \mathbb{N}$. *Ya que* $f(n^2) = E(+\sqrt{n^2}) = E(n) = n$, f *es suprayectiva.*
v) Ya que f *es suprayectiva,* $\mathrm{im}(f) = \mathbb{N}$. $\overline{f} : \mathbb{N}/\sim \to \mathbb{N}$ *viene dada por* $\overline{f}([n]) = E(+\sqrt{n})$ *y* $p_\sim : \mathbb{N} \to \mathbb{N}/sim$ *mediante* $p_\sim(n) = [n]$. *Además tenemos* $f = \overline{f} p_{sim}$.

Ejercicio 1.21

Sea $X = \{0, 1, 2, 3\}$, $Y = \{a, b, c\}$ *y* $f : X \to Y$ *la aplicación dada por:* $f(0) = c$; $f(1) = f(2) = a$; $f(3) = b$. *Considerar la aplicación* $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$ *que a cada subconjunto* $B \subseteq Y$ *le hace corresponder su imagen inversa por* f.

i) ¿Es f^* *inyectiva, suprayectiva o biyectiva?*

ii) Calcular la relación $\sim_{f^*}$ *en* $\mathcal{P}(Y)$ *asociada a* f^* *y el conjunto cociente* $\mathcal{P}(Y)/\sim_{f^*}$.

iii) Hallar la descomposición canónica de f^*.

Solución:

Tenemos que f es suprayectiva, pero no es inyectiva. i) ¿f^* es inyectiva? Supongamos que $f^*(B) = f^*(B')$, para $B, B' \in \mathcal{Y}$. Veamos que $B = B'$. Sea $b \in B$, entonces existe $x \in X$ tal que $b = f(x)$. Así $x \in f^*(B) = f^*(B')$, de donde $b = f(x) \in B'$, de donde $B \subseteq B'$. Por simetría, $B' \subseteq B$. Así $B = B'$. Por tanto f^* es inyectiva.
¿f^* es suprayectiva? Si fuera suprayectiva, sería biyectiva y por tanto $\text{card}(\mathcal{P}(Y)) = 2^3 = 2^4 = \text{card}(\mathcal{P}(X))$, lo que es imposible.
¿f^* es biyectiva? Por lo anterior no es biyectiva.
ii) Como f^* es inyectiva, $B \sim_{f^*} B'$ si y sólo si $B = B'$.
Tenemos que $\mathcal{P}(Y) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a,b\}, \{a,c\}, \{b,c\}, Y\}$ y $\mathcal{P}(Y)/\sim_{f^*} = \{\{B\}; B \in \mathcal{Y}\}$
iii) $\text{im}(f^*) = \{f^*(\emptyset), f^*(\{a\}), f^*(\{b\}), f^*(\{c\}), f^*(\{a,b\}), f^*(\{a,c\}), f^*(\{b,c\}), f^*(Y)\} = \{\emptyset, \{1,2\}, \{3\}, \{0\}, \{1,2,3\}, \{0,1,2\}, \{0,3\}, X\}$.
Por consiguiente, $p_\sim : \mathcal{P}(Y) \to \mathcal{P}(Y)/\sim$ está dada por $p_\sim(B) = \{B\}$ para todo $B \in \mathcal{P}(Y)$ y $\overline{f} : \mathcal{P}(Y)/\sim \to \text{im}(f^*)$ dada por $\overline{f}(\{B\}) = f^*(B)$. Finalmente la inclusión $i : \text{im}(f^*) \to \mathcal{P}(X)$.
Además $f = i\overline{f}p_\sim$.

Ejercicio 1.22

Sean X e Y dos conjuntos tales que $Y \subseteq X$. En el conjunto $\mathcal{P}(X)$ se define la siguiente relación binaria: $A \sim B \Leftrightarrow A \cap Y = B \cap Y$. Demostrar que dicha relación es de equivalencia y describir el conjunto cociente.

Solución:

Reflexiva: Si $A \sim A$, ya que $A \cap Y = A \cap Y$.
Simétrica: Si $A \sim B$, entonces $A \cap Y = B \cap Y$, de donde $B \cap Y = A \cap Y$, y por tanto $B \sim A$.
Transitiva: Si $A \sim B$ y $B \sim C$, entonces $A \cap Y = B \cap Y$ y $B \cap Y = C \cap Y$, de donde $A \cap Y = C \cap Y$, y por tanto $A \sim C$.
Definamos la siguiente aplicación $f : \mathcal{P}(X)/\sim \mathcal{P}(Y)$ dada por $f([A]) = A \cap Y$. Veamos que es biyectiva.
Es aplicación: Si $[A] = [B]$, entonces $A \sim B$, de donde $A \cap Y = B \cap Y$.
Es inyectiva: Si $A \cap Y = B \cap Y$, entonces $A \sim B$, de donde $[A] = [B]$.
Es suprayectiva: Sea $C \in \mathcal{P}(Y)$, entonces $C \in \mathcal{P}(X)$ y $[C] \in \mathcal{P}(X)/\sim$ es tal que $f([C]) = C \cap Y = C$.

Ejercicio 1.23

i) Dar un ejemplo de una relación binaria que sea reflexiva y simétrica pero que no sea transitiva.

ii) Calcular cuantas relaciones reflexivas se pueden definir en un conjunto de 4 elementos.

iii) Calcular cuantas relaciones de equivalencia distintas se pueden definir en un conjunto de 3 elementos y construir todos los conjuntos cocientes.

iv) Demostrar que un conjunto de 4 elementos admite exactamente 15 conjuntos cociente.

Solución:

i) $A = \{a, b, c\}$ *y* $\mathcal{R} = \{(a,a), (b,b), (c,c), (a,b), (b,a), (b,c), (c,b)\}$.
ii) Una relación reflexiva $\mathcal{R}$ *es un subconjunto de* $X \times X$ *que contiene a* $\Delta = \{(a,a); a \in X\}$. *En general, si* $\text{card}(X) = n$, *entonces* $\text{card}(X \times X) = n^2$. *Se trata pues de calcular el cardinal de* 2^{n^2-n}.
iii) Las relaciones de equivalencia se corresponden a las particiones del conjunto $X = \{a, b, c\}$.
Luego tenemos del tipo:
3+0) X *y* $\emptyset$, *esto es,* $\mathcal{R} = X \times X$.
2+1) $\{a, b\}$ *y* $\{c\}$, *esto es,* $\mathcal{R} = \{(a,a), (b,b), (a,b), (b,a), (c,c)\}$.
$\{a, c\}$ *y* $\{b\}$, *esto es,* $\mathcal{R} = \{(a,a), (c,c), (a,c), (c,a), (b,b)\}$.
$\{b, c\}$ *y* $\{a\}$, *esto es,* $\mathcal{R} = \{(b,b), (c,c), (b,c), (c,b), (a,a)\}$.
1+1+1) $\{a\}$, $\{b\}$ *y* $\{c\}$, *esto es,* $\mathcal{R} = \{(a,a), (b,b), (c,c)\}$.
iv) Las relaciones de equivalencia se corresponden a las particiones del conjunto $X = \{a, b, c\}$ *o conjuntos cocientes, luego procedemos como en iii)*
4+0) Hay 1.
3+1) Hay $\binom{4}{1} = 4$.
2+2) Hay $\binom{4}{2}/2 = 6/2$, *pues al elegir 2 los otros 2 quedan automáticamente elegidos, pero hemos de evitar repeticiones.*
2+1+1) Hay $\binom{4}{2} = 6$, *pues al elegir 2 los otros 2 quedan automáticamente elegidos.*
1+1+1+1) Hay 1

Ejercicio 1.24

Sea $f : X \to Y$ *una aplicación y sea* $\mathcal{R}$ *una relación de equivalencia en* Y. *Estudiar si la siguiente relación binaria* $\mathcal{S}$ *en* X

$$x_1 \mathcal{S} x_2 \Leftrightarrow f(x_1) \mathcal{R} f(x_2)$$

es una relación de equivalencia.

Solución:

Reflexiva.) $x\mathcal{S}x$ *ya que* $f(x)\mathcal{R}f(x)$.
Simétrica.) Si $x_1\mathcal{S}x_2$, *entonces* $f(x_1)\mathcal{R}f(x_2)$, *de donde* $f(x_2)\mathcal{R}f(x_1)$ *y por tanto* $x_2\mathcal{S}x_1$.
Transitiva.) Si $x_1\mathcal{S}x_2$ *y* $x_2\mathcal{S}x_3$, *entonces* $f(x_1)\mathcal{R}f(x_2)$ *y* $f(x_2)\mathcal{R}f(x_3)$, *de donde* $f(x_1)\mathcal{R}f(x_3)$ *y por tanto* $x_1\mathcal{S}x_3$.

Ejercicio 1.25

Una relación binaria $\mathcal{R}$ *en un conjunto* X *se dice que es circular si satisface la siguiente propiedad:* $x_1\mathcal{R}x_2 \wedge x_2\mathcal{R}x_3 \Rightarrow x_3\mathcal{R}x_1$. *Demostrar que una relación binaria en* X *es de equivalencia si y solo si es reflexiva y circular.*

Solución:

$\Rightarrow$*) Solo hemos de probar la circular.*
Si $x_1\mathcal{R}x_2 \wedge x_2\mathcal{R}x_3$, *entonces* $x_1\mathcal{R}x_3$ *(por la transitiva) y así* $x_3\mathcal{R}x_1$ *(por la reflexiva).*
$\Leftarrow$*) Simétrica.) Si* $x_1\mathcal{R}x_2$, *como* $x_2\mathcal{R}x_1$ *(por la reflexiva), entonces* $x_2\mathcal{R}x_1$ *(por la circular)*

Transitiva.) Si $x_1\mathcal{R}x_2$ y $x_2\mathcal{R}x_3$, entonces $x_3\mathcal{R}x_1$ (por la circular), de donde $x_1\mathcal{R}x_3$ (por la simétrica).

Ejercicio 1.26

Sea $X = Y = \{a, b, c, d\}$ y sea $f : X \to Y$ la aplicación dada por el grafo $\{(a, a), (b, a), (c, d), (d, c)\}$. Considérense las aplicaciones inducidas $f_* : \mathcal{P}(X) \to \mathcal{P}(Y)$ y $f^* : \mathcal{P}(Y) \to \mathcal{P}(X)$ y determínense entonces los conjuntos cociente de $\mathcal{P}(X)$ y $\mathcal{P}(Y)$ bajo las relaciones de equivalencia inducidas por f_* y f^*.

Solución:

A	$\emptyset$	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	$\{a,b\}$	$\{a,c\}$	$\{a,d\}$
$f_*(A)$	$\emptyset$	$\{a\}$	$\{a\}$	$\{d\}$	$\{c\}$	$\{a\}$	$\{a,d\}$	$\{a,c\}$

A	$\{b,c\}$	$\{b,d\}$	$\{c,d\}$	$\{a,b,c\}$	$\{a,b,d\}$	$\{a,c,d\}$	$\{b,c,d\}$	$\{a,b,c,d\}$
$f_*(A)$	$\{a,d\}$	$\{a,c\}$	$\{c,d\}$	$\{a,d\}$	$\{a,c\}$	$\{a,c,d\}$	$\{a,c,d\}$	$\{a,c,d\}$

B	$\emptyset$	$\{a\}$	$\{b\}$	$\{c\}$	$\{d\}$	$\{a,b\}$	$\{a,c\}$	$\{a,d\}$
$f^*(B)$	$\emptyset$	$\{a.b\}$	$\emptyset$	$\{d\}$	$\{c\}$	$\{a,b\}$	$\{a,b,d\}$	$\{a,b,c\}$

B	$\{b,c\}$	$\{b,d\}$	$\{c,d\}$	$\{a,b,c\}$	$\{a,b,d\}$	$\{a,c,d\}$	$\{b,c,d\}$	$\{a,b,c,d\}$
$f^*(B)$	$\{d\}$	$\{c\}$	$\{c,d\}$	$\{a,b,d\}$	$\{a,b,c\}$	$\{a,b,c,d\}$	$\{c,d\}$	$\{a,b,c,d\}$

El resto ya es fácil.

Ejercicio 1.27

Sean $f : X \to Y$ y $g : X \to Z$ dos aplicaciones tales que f es suprayectiva y $\mathcal{R}_f \subseteq \mathcal{R}_g$. Demostrar que existe una aplicación $h : Y \to Z$ tal que $g = hf$.

Solución:

Sea $y \in Y$, como f es suprayectiva existe $x \in X$ tal que $y = f(x)$. Entonces $g(x) \in Z$. Definamos $h : Y \to Z$ mediante $h(y) = g(x)$.
Veamos que en efecto es una aplicación. Supongamos que $y = y'$, entonces existen $x, x' \in X$ tales que $f(x) = y = y' = f(x')$. Por tanto $x\mathcal{R}_f x'$ y así $x\mathcal{R}_g x'$, de donde $g(x) = g(x')$, esto es, $h(y) = h(y')$.

Ejercicio 1.28

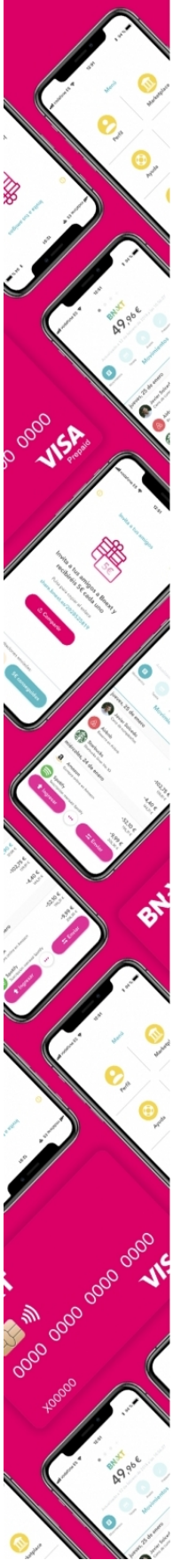
Si X e Y son dos conjuntos y $\mathcal{R}$ y $\mathcal{S}$ son relaciones de equivalencia en X e Y respectivamente, definir en el conjunto $X \times Y$ una relación de equivalencia $\mathcal{T}$ tal que exista una biyección $(X \times Y)/\mathcal{T} \cong (X/\mathcal{R}) \times (Y/\mathcal{S})$.

Solución:

Definimos

$$(x_1, y_1)\mathcal{T}(x_2, y_2) \Leftrightarrow (x_1\mathcal{R}x_2) \wedge (y_1\mathcal{S}y_2).$$

Reflexiva.) $(x_1, y_1)\mathcal{T}(x_1, y_1)$, ya que $(x_1\mathcal{R}x_1) \wedge (y_1\mathcal{S}y_1)$.



Simétrica.) *Si* $(x_1, y_1)\mathcal{T}(x_2, y_2)$, *entonces* $(x_1\mathcal{R}x_2) \wedge (y_1\mathcal{S}y_2)$, *de donde* $(x_2\mathcal{R}x_1) \wedge (y_2\mathcal{S}y_1)$ *y por tanto* $(x_2, y_2)\mathcal{T}(x_1, y_1)$.
Transitiva.) *Si* $(x_1, y_1)\mathcal{T}(x_2, y_2)$ *y* $(x_2, y_2)\mathcal{T}(x_3, y_3)$, *entonces* $(x_1\mathcal{R}x_2) \wedge (y_1\mathcal{S}y_2)$ *y* $(x_2\mathcal{R}x_3) \wedge (y_2\mathcal{S}y_3)$, *de donde* $(x_1\mathcal{R}x_3) \wedge (y_1\mathcal{S}y_3)$ *y por tanto* $(x_1, y_1)\mathcal{T}(x_3, y_3)$.
Finalmente.

$$X \times Y/\mathcal{T} = \{[(x, y)]; (x, y) \in X \times Y\} = \{([x], [y]); x \in X, y \in Y\} = X/\mathcal{R} \times Y/\mathcal{S}.$$

Ejercicio 1.29

Dibujar un diagrama para cada uno de los siguientes subconjuntos de $\mathbb{N}$ *parcialmente ordenados por divisibilidad y encontrar los elementos notables que existan:*

i) $\{1, 2, 3, 6, 12\}$

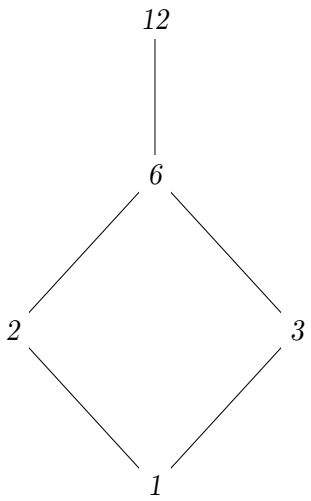
ii) $\{1, 2, 3, 12, 18, 36\}$

iii) $\{1, 2, 3, 5, 12, 60\}$

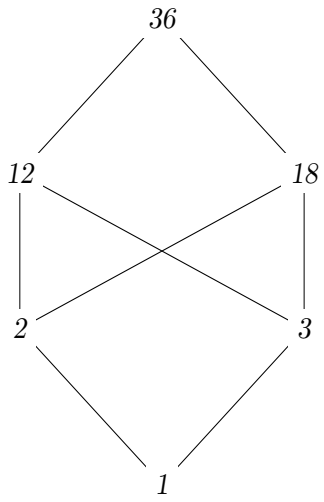
iv) $\{1, 2, 3, 8, 9, 72\}$.

Solución:

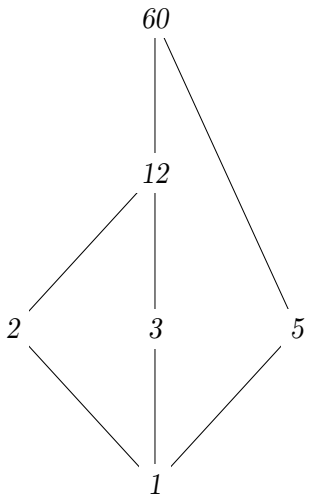
i)



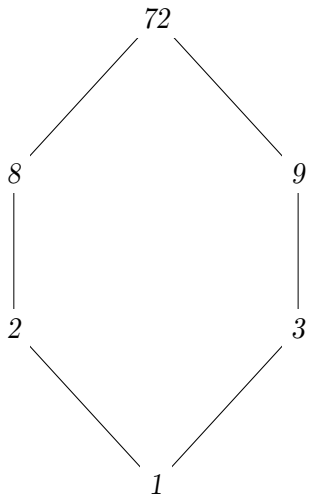
Mínimo: 1
Máximo: 12
ii)



Mínimo: 1
Máximo: 36
iii)



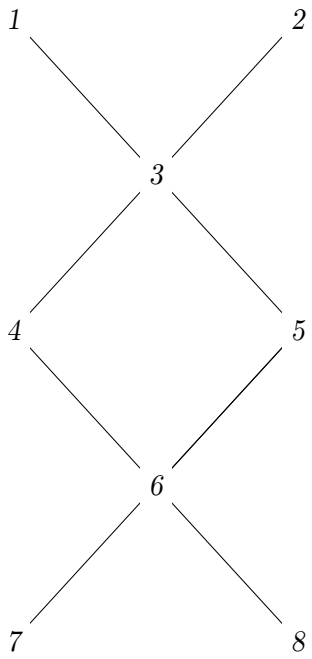
Mínimo: 1
Máximo: 60
iv)



Mínimo: 1
Máximo: 72

Ejercicio 1.30

Sea $X = \{1, 2, 3, 4, 5, 6, 7, 8\}$ *ordenado por el diagrama*



y sea $A = \{4, 5, 6\}$. *Encontrar todos los elementos notables en* X *y* A.

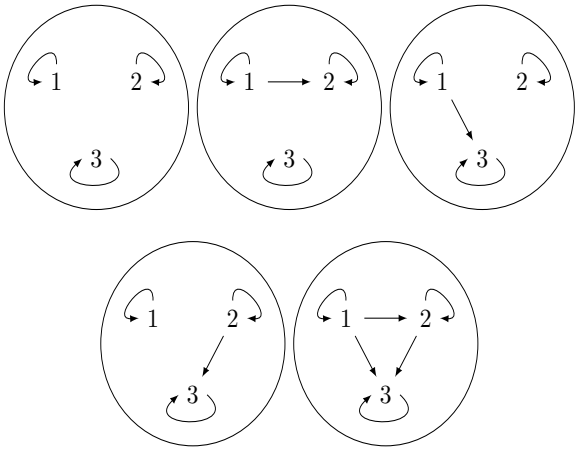
Solución:

Cotas superiores de A: $1, 2, 3$
Cotas inferiores de A: $6, 7, 8$
Supremo de A: 3
Ínfimo de A: 6

Ejercicio 1.31

Encontrar todos los órdenes parciales que se pueden definir en un conjunto de 3 elementos.

Solución:



Ejercicio 1.32

Dada una aplicación $f : X \to Y$ se define en $\mathcal{P}(Y)$ la relación binaria: $B\mathcal{R}B' \Leftrightarrow f_*(f^*(B)) \subseteq B'$ para $B, B' \in \mathcal{P}(Y)$. Estudiar si $\mathcal{R}$ es una relación de orden en $\mathcal{P}(Y)$.

Solución:

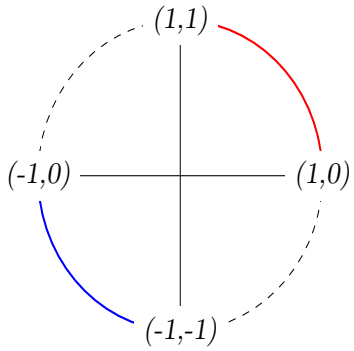
Reflexiva.) Sea $B \in \mathcal{P}(Y)$. Por el Ejercicio 1.11, $f_*(f^*(B)) \subseteq B$, de donde $B\mathcal{R}B$.
Antisimétrica.) Si $B\mathcal{R}B'$ y $B'\mathcal{R}B$, entonces $f_*(f^*(B)) \subseteq B'$ y $f_*(f^*(B')) \subseteq B$. Por tanto $f^*(f_*(f^*(B'))) \subseteq f^*(B)$. Pero por el Ejercicio 1.11, $f^*(B') \subseteq f^*(f_*(f^*(B'))) \subseteq f^*(B)$. Análogamente se prueba que $f^*(B) \subseteq f^*(B')$. Así $f^*(B) = f^*(B')$
Transitiva.) Si $B\mathcal{R}B'$ y $B'\mathcal{R}B''$, entonces $f_*(f^*(B)) \subseteq B'$ y $f_*(f^*(B')) \subseteq B''$. Por tanto $f^*(B) \subseteq f^*(B')$, de donde $f_*(f^*(B)) \subseteq f_*(f^*(B')) \subseteq B'')$ y así $B\mathcal{R}B''$.

Ejercicio 1.33

Considérese en el plano euclídeo $\mathbb{R}^2$ la siguiente relación de orden: $(x, y) \leq (x', y') \Leftrightarrow x \leq x' \wedge y \leq y'$. Calcular los elementos maximales, minimales, supremo e ínfimo de la circunferencia $C = \{(x, y); x^2 + y^2 = 1\}$.

Solución:

Hay infinitos puntos maximales en la circunferencia unidad, que son los del primer cuadrante (en rojo) y un único supremo que es el punto (1,1). Análogamente, existen infinitos minimales que son los del tercer cuadrante (en azul) y un único ínfimo que es el punto (-1,-1).



Ejercicio 1.34

Sean X e Y conjuntos ordenados y definamos en $X \times Y$ la siguiente relación binaria: $(x, y) \leq (x', y') \Leftrightarrow x \leq x' \wedge y \leq y'$. Demostrar que "$\leq$" es una relación de orden en $X \times Y$ pero que este orden no es total (incluso en el caso de que X e Y fueran totalmente ordenados) salvo en en el caso de que X ó Y consistan de un solo elemento.

Solución:

Reflexiva.)
$(x, y) \leq (x, y)$ *ya que* $x \leq x \wedge y \leq y$.
Antisimétrica.) Si $(x, y) \leq (x', y')$ *y* $(x', y') \leq (x, y)$ *entonces* $x \leq x' \wedge y \leq y'$ *y* $x' \leq x \wedge y' \leq y$, *de donde* $x = x'$ *e* $y = y'$. *Por tanto* $(x, y) = (x', y')$.
Transitiva.) Si $(x, y) \leq (x', y')$ *y* $(x', y') \leq (x'', y'')$ *entonces* $x \leq x' \wedge y \leq y'$ *y* $x' \leq x'' \wedge y' \leq y''$, *de donde* $x \leq x''$ *e* $y \leq y''$. *Por tanto* $(x, y) \leq (x'', y'')$.
Supongamos que X e Y tienen más de un elemento. Es suficiente tomar $x, x' \in X$ con $x \not\leq x'$ e $y, y' \in Y$ con $y' \not\leq y$. Entonces $(x, y) \not\leq (x', y')$ y $(x', y') \not\leq (x, y)$.

Ejercicio 1.35: Orden lexicográfico

Sean X e Y conjuntos ordenados y definamos en $X \times Y$ la siguiente relación binaria: $(x, y) \leq (x', y') \Leftrightarrow x \leq x' \vee (x = x' \wedge y \leq y')$. Demostrar que "$\leq$" es una relación de orden en $X \times Y$ y que este orden es total si X e Y son totalmente ordenados.

Solución:

Reflexiva.)
$(x, y) \leq (x, y)$ *ya que* $x \leq x$.
Antisimétrica.) Si $(x, y) \leq (x', y')$ *y* $(x', y') \leq (x, y)$, *entonces* $x \leq x' \vee (x = x' \wedge y \leq y')$ *y* $x' \leq x \vee (x' = x \wedge y' \leq y)$. *En todos los casos concluimos que* $x = x'$ *e* $y = y'$ *y por tanto* $(x, y) = (x', y')$.
Transitiva.) Si $(x, y) \leq (x', y')$ *y* $(x', y') \leq (x'', y'')$, *entonces* $x \leq x' \vee (x = x' \wedge y \leq y')$ *y* $x' \leq x'' \vee (x' = x'' \wedge y' \leq y'')$. *En todos los casos concluimos que* $x \leq x'' \vee (x = x'' \wedge y \leq y'')$ *y por tanto* $(x, y) \leq (x'', y'')$.
Total.) Sean $(x, y), (x', y') \in X \times Y$.
Si $x = x'$ *e* $y \leq y'$, *entonces* $(x, y) \leq (x', y')$.
Si $x = x'$ *e* $y' \leq y$, *entonces* $(x', y') \leq (x, y)$.
Si $x < x'$, *entonces* $(x, y) \leq (x', y')$.
Si $x > x'$, *entonces* $(x', y') \leq (x, y)$.

Ejercicio 1.36

Sean X e Y conjuntos ordenados y consideremos en $X \times Y$ el orden lexicográfico. Demostrar que si X e Y son bien ordenados entonces $X \times Y$ también es bien ordenado.

Solución:

Hemos de probar que todo subconjunto no vacío de $X \times Y$ tiene un elemento mínimo respecto del orden lexicográfico.
Sea $\emptyset \neq A \subseteq X \times Y$. Sea $A_1 = \{a \in X; (a,b) \in A \text{ para algún } b \in Y\}$. Tenemos que $\emptyset \neq A_1 \subseteq X$. Como X es bien ordenado, existe $a_1 = \min A_1$. Análogamente, sea $A_2 = \{b \in Y; (a,b) \in A \text{ para algún } a \in X\}$. Tenemos que $\emptyset \neq A_2 \subseteq Y$. Como Y es bien ordenado, existe $a_2 = \min A_2$. Veamos que $(a_1, a_2) = \min_{lex} A$. Claramente $(a_1, a_2) \in A$. Sea $(x, y) \in A$. Si $a_1 < x$, entonces $(a_1, a_2) \leq_{lex} (x, y)$. Si $a_1 = x$, como $y \in A_2$, $a_2 \leq y$ y por tanto $(a_1, a_2) \leq_{lex} (x, y)$

Ejercicio 1.37

Sea $<$ una relación binaria sobre un conjunto X que es transitiva y irreflexiva (esto último significa que $x < x$ no se verifica para ningún $x \in X$). Demostrar que la relación $x \leq y$ definida por $x < y \vee x = y$ es un orden en X.

Solución:

Reflexiva.) Sea $x \in X$, ya que $x = x$, tenemos que $x < x \vee x = x$, luego $x \leq x$.
Antisimétrica.) Si $x \leq y$ e $y \leq x$, entonces $x < y \vee x = y$ e $y < x \vee y = x$. En todos los casos obtenemos $x = y$.
Transitiva.) Si $x \leq y$ e $y \leq z$, entonces $x < y \vee x = y$ e $y < z \vee y = z$. En todos los casos obtenemos $x < z \vee x = z$. Por tanto $x \leq z$.

Capítulo

2

Aritmética entera.

Ejercicios

Ejercicio 2.1

Demostrar, utilizando inducción:

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

ii) $\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

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

iv) $\sum_{i=1}^{n} i^5 + \sum_{i=1}^{n} i^7 = 2(\frac{n(n+1)}{2})^4$

v) $\sum_{i=1}^{n} (2i-1) = n^2$,

vi) $2^n \leq n!$ *para todo* $n \geq 4$.

Solución:

i) Para $n = 1$,

$$1 = \frac{1 \cdot 2}{2}.$$

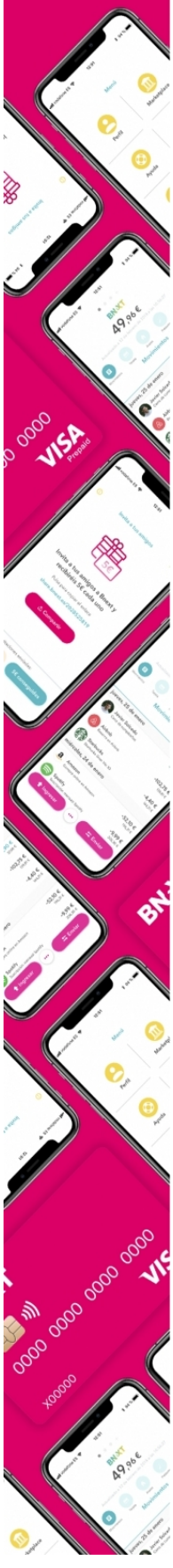
Hipótesis de inducción:

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

Hay que probar:

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

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



ii) Para $n = 1$,

$$\sum_{i=1}^{1} i^2 = 1 = \frac{2 \cdot 3}{6}.$$

Hipótesis de inducción:

$$\sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}.$$

Hay que probar:

$$\sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2n+3)}{6}.$$

$$\sum_{i=1}^{n+1} i^2 = \sum_{i=1}^{n} i^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{n(n+1)(2n+1) + 6(n+1)^2}{6}$$
$$= \frac{(n+1)[2n^2 + n + 6n + 6]}{6} = \frac{(n+1)(2n^2+7n+6}{6} = \frac{(n+1)(n+2)(2n+3)}{6}.$$

iii) Para $n = 1$,

$$\sum_{i=1}^{1} i^3 = 1 = (\frac{1 \cdot 2}{2})^2.$$

Hipótesis de inducción:

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

Hay que probar:

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

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

iv) Para $n = 1$,

$$\sum_{i=1}^{1} i^5 + \sum_{i=1}^{1} i^7 = 1 + 1 = 2 = 2(\frac{2}{2})^4.$$

Hipótesis de inducción:

$$\sum_{i=1}^{n} i^5 + \sum_{i=1}^{n} i^7 = 2(\frac{n(n+1)}{2})^4.$$

Hay que probar:

$$\sum_{i=1}^{n+1} i^5 + \sum_{i=1}^{n+1} i^7 = 2(\frac{(n+1)(n+2)}{2})^4.$$

$$\sum_{i=1}^{n+1} i^5 + \sum_{i=1}^{n+1} i^7 = (n+1)^5 + (n+1)^7 + 2(\frac{n(n+1)}{2})^4 = \frac{8(n+1)^5 + 8(n+1)^7 + n^4(n+1)^4}{8}$$
$$= \frac{(n+1)^4[n^4 + 8(n+1) + 8(n+1)^3]}{8} = \frac{(n+1)^4(n+2)^4}{8} = 2(\frac{(n+1)(n+2)}{2})^4.$$

v*) Para* $n = 1$,

$$\sum_{i=1}^{1}(2i-1) = 1 = 1^2.$$

Hipótesis de inducción:

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

Hay que probar:

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

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

v*i) Para* $n = 4$,

$$2^4 = 16 \leq 24 = 4!.$$

Hipótesis de inducción:

$$2^n \leq n!.$$

Hay que probar:

$$2^{(n+1)} \leq (n+1)!.$$

$$2^{(n+1)} = 2 \cdot 2^n \leq n!(n+1) = (n+1)!$$

Ejercicio 2.2

Demostrar que para todo $n \geq 1$, se verifica:

i) $\overline{A_1 \cup \cdots \cup A_n} = \overline{A_1} \cap \cdots \cap \overline{A_n}$

ii) $\overline{A_1 \cap \cdots \cap A_n} = \overline{A_1} \cup \cdots \cup \overline{A_n}$

Solución:

i)) Para $n = 1$,

$$\overline{A_1} = \overline{A_1}$$

Hipótesis de inducción:

$$\overline{A_1 \cup \cdots \cup A_n} = \overline{A_1} \cap \cdots \cap \overline{A_n}$$

Hay que probar:

$$\overline{A_1 \cup \cdots \cup A_n \cup A_{n+1}} = \overline{A_1} \cap \cdots \cap \overline{A_n} \cap \overline{A_{n+1}}$$

$$\overline{A_1 \cup \cdots \cup A_n \cup A_{n+1}} = \overline{A_1 \cup \cdots \cup A_n} \cap \overline{A_{n+1}} = \overline{A_1} \cap \cdots \cap \overline{A_n} \cap \overline{A_{n+1}}$$

ii) Análogo al anterior

Ejercicio 2.3

Denotamos

$$\binom{n}{i} = \frac{n!}{m!(n-m)!}.$$

Probar que $\binom{n}{i} + \binom{n}{i-1} = \binom{n+1}{i}$.
Usando esta igualdad, probar por inducción que

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Solución:

i)

$$\binom{n}{i} + \binom{n}{i-1} = \frac{n!}{i!(n-i)!} + \frac{n!}{(i-1)!(n-i+1)!} = \frac{(n+1-i)n! + in!}{i!(n+1-i)!} = \frac{(n+1)!}{i!(n+1-i)!} = \binom{n+1}{i}.$$

ii) Para $n = 1$,

$$(a+b)^1 = a + b = \binom{1}{0} a + \binom{1}{1} b.$$

Hipótesis de inducción:

$$(a+b)^n = \sum_{i=0}^{n} \binom{n}{i} a^{n-i} b^i.$$

Hay que probar:

$$(a+b)^{n+1} = \sum_{i=0}^{n+1} \binom{n+1}{i} a^{n+1-i} b^i.$$

$$(a+b)^{n+1} = (a+b)^n(a+b) = (\binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{n-1}ab^{n-1} + \binom{n}{n}b^n)(a+b) =$$
$$\binom{n}{0}a^{n+1} + \binom{n}{1}a^n b + \cdots + \binom{n}{n-1}a^2 b^{n-1} + \binom{n}{n}ab^n +$$
$$\binom{n}{0}a^n b + \binom{n}{1}a^{n-1}b^2 + \cdots + \binom{n}{n-1}ab^n + \binom{n}{n}b^{n+1} =$$
$$\binom{n}{0}a^{n+1} + (\binom{n}{1} + \binom{n}{0})a^n b + \cdots + (\binom{n}{n} + \binom{n}{n-1})ab^n + \binom{n}{n}b^{n+1} =$$
$$\binom{n+1}{0}a^{n+1} + \binom{n+1}{1}a^n b + \cdots + \binom{n+1}{n}ab^n + \binom{n+1}{n+1}b^{n+1}.$$

Ejercicio 2.4

Demostrar por inducción que para todo número par k, el resto de dividir 2^k entre 3 es 1.

Solución:

Si $k = 2n$, entonces $2^k = 2^{2n} = 4^n$. Para $n = 1$,

$$2^k = 4, 4 = 1 \cdot 3 + 1.$$

Hipótesis de inducción:

$$2^k = 4^n = 3 \cdot q + 1.$$

Hay que probar:

$$2^{k+1} = 4^{n+1} = 3 \cdot q' + 1.$$

$$2^{k+1} = 4^{n+1} = 4(3q+1) = 12q + 4 = 3(4q+1) + 1.$$

Ejercicio 2.5

Demostrar que para todo n, entero no negativo, $4^{2n} - 2^n$ es divisible por 7.

Solución:

Para $n = 0$, $4^0 - 2^0 = 1 - 1 = 0$ *y* 0 *es divisible por 7.*
Para $n = 1$, $4^2 - 2^1 = 16 - 2 = 14$ *y* 0 *es divisible por 7.*
Hipótesis de inducción: $4^{2n} - 2^n = 7q$.
Hay que probar: $4^{2(n+1)} - 2^{(n+1)} = 7q'$.

$$4^{2(n+1)} - 2^{(n+1)} = 16 \cdot 4^{2n} - 2 \cdot 2^n = 16(7q + 2^n) - 2 \cdot 2^n = 16 \cdot 7q + 14 \cdot 2^n = 7(16q + 2 \cdot 2^n)$$

Ejercicio 2.6

Demuestra que para todo n, entero no negativo, se tiene que $2^{3n} - 14^n$ *es divisible por 6.*

Solución:

Para $n = 0$, $2^0 - 14^0 = 1 - 1 = 0$ *y* 0 *es divisible por 6.*
Para $n = 1$, $2^3 - 14^1 = 8 - 14 = -6$ *y* -6 *es divisible por 6.*
Hipótesis de inducción: $2^{3n} - 14^n = 6q$.
Hay que probar: $2^{3(n+1)} - 14^{n+1} = 6q'$.

$$2^{3(n+1)} - 14^{n+1} = 8 \cdot 2^{3n} - 14 \cdot 14^n = 8(6q + 14^n - 14 \cdot 14^n = 8 \cdot 6q + 14^n(8 - 14) = 6(8q - 14^n).$$

Ejercicio 2.7

Para cada una de las siguientes parejas de enteros (a, b)*, calcula el máximo común divisor* $d = m.c.d(a, b)$ *y enteros* s, t *que satisfagan la relación de Bezout, esto es, tales que* $d = sa + tb$

i) $a = -99$, $b = 17$,

ii) $a = 6643$, $b = 2873$,

iii) $a = -7655$, $b = 1001$,

iv) $a = 24230$, $b = 586$.

Solución:

i)

i	q	r	s	t
0	-	-99	1	0
1	-6	17	0	1
2	5	3	1	6
3	1	2	-5	-29
4	2	1	6	35

Solución: $(d, s, t) = (1, 6, 35)$.
ii)

i	q	r	s	t
0	-	6643	1	0
1	2	2873	0	1
2	3	897	1	-2
3	4	182	-3	7
4	1	169	13	-30
5	13	13	-16	37

Solución: $(d, s, t) = (13, -16, 37)$.
iii)

i	q	r	s	t
0	-	-7655	1	0
1	-8	1001	0	1
2	2	353	1	8
3	1	295	-2	-15
4	5	58	3	23
5	11	5	-17	-130
6	1	3	190	1453
7	1	2	-207	-1583
8	2	1	397	3036

Solución: $(d, s, t) = (1, 397, 3036)$.
iv)

i	q	r	s	t
0	-	24230	1	0
1	41	586	0	1
2	2	204	1	-41
3	1	178	-2	83
4	6	26	3	-124
5	1	22	-20	827
6	5	4	23	-951
7	2	2	-135	5582

Solución: $(d, s, t) = (2, -135, 5582)$.

Ejercicio 2.8

Demuestra que para todo $n > 0$

(i) $3^{2n} - 2^n$ *es divisible por 7,*

(ii) $3^{2n+1} + 2^{n+2}$ *es divisible por 7,*

(iii) $3^{2n+2} + 2^{6n+1}$ *es divisible por 11,*

(iv) $3 \cdot 5^{2n+1} + 2^{3n+1}$ *es divisible por 17.*

Solución:

(i) $3^{2n} = (3^2)^n = 9^n$. *Como* $9 \equiv 2 \pmod 7$, *tenemos que* $9^n \equiv 2^n \pmod 7$.
Así $3^{2n} - 2^n \equiv 2^n - 2^n \equiv 0 \pmod{}7$).
(ii) $3^{2n+1} = (3^2)^n \cdot 3 = 3 \cdot 9^n$. *Como* $9 \equiv 2 \pmod 7$, *tenemos que* $3 \cdot 9^n \equiv 3 \cdot 2^n \pmod 7$.
Por otro lado, $2^{n+2} = 2 * 2 \cdot 2^n = 4 \cdot 2^n$.
Así $3^{2n+1} + 2^{n+2} \equiv 3 \cdot 2^n + 4 \cdot 2^n \equiv 7 \cdot 2^n \equiv 0 \pmod 7$.
(iii) $3^{2n+2} = 3^2 \cdot (3^2)^n = 9 \cdot 9^n$.
Por otro lado $2^{6n+1} = 2 \cdot (2^6)^n = 2 \cdot 64^n$. *Como* $64 \equiv 9 \pmod{11}$, *tenemos que* $2^{6n+1} \equiv 2 \cdot 9^n \pmod{11}$.
Así $3^{2n+2} + 2^{6n+1} \equiv 9 \cdot 9^n + 2 \cdot 9^n \equiv 0 \pmod{11}$.
(iv) $3 \cdot 5^{2n+1} = 3 \cdot 5 \cdot (5^2)^n = 15 \cdot 25^n$. *Como* $25 \equiv 8 \mod 17$, *tenemos que* $15 \cdot 25^n \equiv 15 \cdot 8^n \pmod{17}$.
Por otro lado $2^{3n+1} = 2 \cdot (2^3)^n = 2 \cdot 8^n$.
Así $3 \cdot 5^{2n+1} + 2^{3n+1} \equiv 15 \cdot 8^n + 2 \cdot 8^n \equiv 0 \pmod{17}$.

Ejercicio 2.9

Demostrar que si a y b son enteros primos relativos y n es un entero divisible por a y por b entonces lo es por ab.

Solución:

Ya que $a \mid n$ *y* $b \mid n$, *tenemos que* $m.c.m(a,b) \mid n$. *Pero como* $m.c.d(a,b) = 1$, *entonces* $m.c.m(a,b) = ab$.
Así $ab \mid n$.

Ejercicio 2.10

Demuestra que si $3 \mid a^2 + b^2$, *entonces* $3 \mid a$ *y* $3 \mid b$.

Solución:

Si $3 \nmid a$ *o* $3 \nmid b$, *entonces, como* $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = \overline{1}$, *tenemos que* $a^2 \equiv 1 \pmod 3$ *o* $b^2 \equiv 1 \pmod 3$.
Por tanto $\overline{a}^2 + \overline{b}^2 \in \{\overline{1}, \overline{2}\}$.

Ejercicio 2.11

Demuestra que si $5 \mid a^2 + b^2 + c^2$, *entonces* $5 \mid a$ *o* $5 \mid b$ *o* $5 \mid c$.

Solución:

Si $5 \nmid a$ *y* $5 \nmid b$ *y* $5 \mid c$, *entonces, como* $\overline{0}^2 = \overline{0}$, $\overline{1}^2 = \overline{1}$, $\overline{2}^2 = -\overline{1}$, $\overline{3}^2 = -\overline{1}$, $\overline{4}^2 = \overline{1}$. *Por tanto* $\overline{a}^2 + \overline{b}^2 + \overline{c}^2 \in \{-\overline{1}, \overline{1}\}$.

Ejercicio 2.12

Sean a,b,c enteros no nulos. Demostrar que $m.c.d(a,b) = 1$ *y* $m.c.d(a,c) = 1$ *si, y sólo si,* $m.c.d(a, m.c.m(b,c)) = 1$.

Solución:

Sea $m = m.c.m(b, c)$. $\Rightarrow$) *Sea* $m.c.d(a, m) = d$. *Entonces* $d \mid a$ *y* $d \mid m$. *Por tanto, si* $m.c.d(a, b) = 1$, *existen* u, v *tales que* $1 = au + bv$. *Así* $c = acu + bcv$. *Ya que* $d \mid ac$ *y* $d \mid bc$, *resulta que* $d \mid c$. *Como* $d \mid a$, *tenemos que* $d \mid m.c.d(a, c) = 1$. *Así* $d = 1$.
$\Leftarrow$) *Si* $m.c.d(a, m) = 1$, *entonces existen* u, v *tales que* $1 = au + mv$. *Como* $b \mid m$, *entonces* $m = bh$ *y* $1 = au + bhv$. *Por tanto* $m.c.d(a, b) = 1$. *Análogamente, como* $c \mid m$, *entonces* $m = ck$ *y* $1 = au + ckv$. *Por tanto* $m.c.d(a, c) = 1$.

Ejercicio 2.13

Para n *natural calcula:* $m.c.d(n, n^2)$, $m.c.d(n, n + 1)$ *y* $m.c.d(n, n + 2)$.

Solución:

(i) Si $d = m.c.d(n, n^2)$, *entonces* $d \mid n$. *Como* $n \mid n$ *y* $n \mid n^2$, *entonces* $n \mid d$. *Por tanto* $d = n$.
(ii) Si $d = m.c.d(n, n + 1)$, *entonces* $d \mid n$ *y* $d \mid n + 1$, *de donde* $d \mid (n + 1) - n = 1$. *Por tanto* $d = 1$.
(iii) Tenemos que, por el algoritmo de Euclides, $m.c.d(n, n + 2) = m.c.d(2, n)$, *de donde* $m.c.d(n, n + 2) = 1$ *si* n *es impar y* $m.c.d(n, n + 2) = 2$ *si* n *es par.*

Ejercicio 2.14

Resolver las ecuaciones diofánticas

i) $60x + 36y = 12$,

ii) $35x + 6y = 8$,

iii) $12x + 18y = 11$.

Solución:

i)

$$x = -1 + 3k \qquad y = 2 - 5k$$

ii)

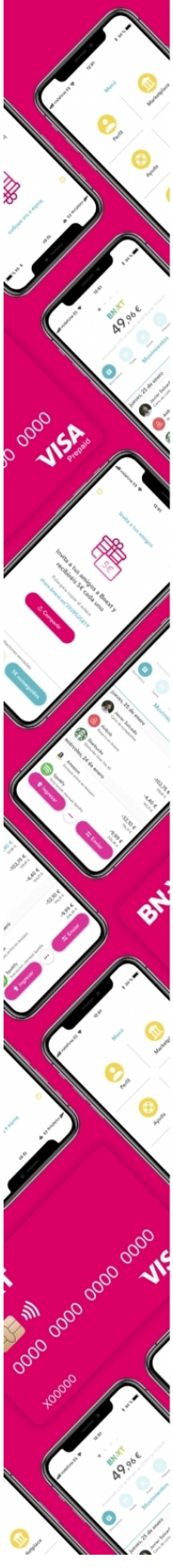
$$x = -8 + 6k \qquad y = 48 - 35k$$

iii)

$$x = -2 + 3k \qquad y = 1 - 2k$$

Ejercicio 2.15

Se dispone de 4050 euros para gastar en bolígrafos de 10 euros y en plumas de 46 euros. Calcular cuantos bolígrafos y plumas se pueden comprar si se quiere el menor número posible de bolígrafos.



Solución:

Consideremos la ecuación diofántica $10x + 46y = 4050$, *o equivalentemente* $5x + 23y = 2025$. *La solución general es:*

$$x = 23t_0 - 18225 \qquad y = -5t_0 + 4050$$

Por tanto, de $23t_0 - 18225 \geq 0$, *obtenemos que* $t_0 \geq 792$. *Sea pues* $t_0 = 793$, *entonces* $x = 14$ *e* $y = 85$.

Ejercicio 2.16

Factorizar en primos cada uno de los siguientes números y, usando estas factorizaciones, calcular el máximo común divisor y el mínimo común múltiplo de cada una de las parejas que puedas formar con ellos: 6643, 2873, 4148, 252.

Solución:

Ya que $6643 = 7 \cdot 13 \cdot 73$
$2873 = 13^3 \cdot 17$
$4148 = 2^2 \cdot 17 \cdot 61$
$252 = 2^2 \cdot 3^2 \cdot 7$
tenemos por ejemplo $m.c.d(6643, 252) = 7$ *y* $m.c.m(6643, 252) = 7 \cdot 13 \cdot 73 \cdot 2^2 \cdot 3^2$.

Ejercicio 2.17

Demostrar que entre $-|b|$ *y* $|b|$ *no hay múltiplos de* b *salvo el cero.*

Solución:

Sea a *un múltiplo de* b, *esto es,* $a = bq$. *Entonces* $|a| = |qb| = |q||b|$ *y* $|b| \geq |a|$.

Ejercicio 2.18

¿Cuántos primos hay entre 27270 y 27280? ¿y entre 4900 y 4905?.

Solución:

Ya que un número entero $n > 1$ *es primo o tiene un divisor primo* $\leq \sqrt{n}$, *si* $27270 < x < 27280$, *entonces* $\sqrt{27270} < \sqrt{x} < \sqrt{27280}$.
En el intervalo $(27270, 27280) = \{27271, 27272, 27273, 27274, 27275, 27276, 27277, 27278, 27279\}$, *claramente no son primos, por las de divisibilidad del 2,3,5, los números* $27272, 27273, 27274, 27275, 27276, 27278, 27279$. *Nos quedan por tanto* 27271 *y* 27277.
27271*) Para averiguar si es primo, ya que un número entero* $n > 1$ *es primo o tiene un divisor primo* $\leq \sqrt{n}$, *debemos dividir por todos los primos* $\leq \sqrt{27271} = 165$. *Demasiado aburrido para hacer a mano.*
La segunda parte es igual de aburrida.

Ejercicio 2.19

Tres agricultores dividieron equitativamente el arroz que habían cultivado en común. Para venderlo fueron a mercados diferentes, donde se usaban diferentes medidas de peso, además todos ellos usaron carretas en las que podían transportar un máximo de 1000 libras. En el primer mercado la medida era de 11 libras, en el segundo de 14 y en el tercero de 15 libras. Cada agricultor vendió todo lo que pudo en medidas enteras y cuando volvieron al hogar, el primero llevaba 5 libras de arroz, el segundo 6 y el tercero 4. ¿Cuánto arroz habían cultivado entre los tres?

Solución:

Consideremos el sistema de congruencias:

$$\begin{aligned} x \equiv & 5 \pmod{11} \\ x \equiv & 6 \pmod{14} \\ x \equiv & 4 \pmod{15} \end{aligned}$$

cuya solución es:

i	a	m	c	d	b
1	*5*	*11*	*210*	*1*	*1050*
2	*6*	*14*	*165*	*9*	*720*
3	*4*	*15*	*154*	*4*	*874*

Por tanto $3 * x = 2622$.

Ejercicio 2.20

En un centro comercial hay tres salas de cine con capacidades de 35,65 y 91 espectadores. Se sabe que el pasado sábado, y en exclusiva para los alumnos de Matemáticas de la UGR, estas tres salas estrenaban a las 20 horas un documental sobre el futuro de las Matemáticas. La asistencia fue muy amplia, entre 300 y 400 alumnos, y al final de la sesión se planteó la pregunta, entre ellos, de cuántos en realidad habían asistido. Sabiendo que en todas las salas las palomitas las daban gratis y que, si todos los asistentes se hubieran intentado acomodar en salas como la pequeña 8 de ellos no hubieran podido hacerlo, que si 3 de los asistentes hubieran decidido no entrar entonces los restantes habrían cabido exactamente en la sala mediana y que, si 22 veces el número de asistentes se hubieran intentado acomodar en salas como la de mayor aforo uno de ellos se tendría que haber quedado fuera ¿podrías calcular tú, razonadamente, cuántos alumnos asistieron a la sesión?

Solución:

Consideremos el sistema de congruencias:

$$\begin{aligned} x \equiv & 8 \pmod{35} \\ x - 3 \equiv & 0 \pmod{65} \\ 22x \equiv & 1 \pmod{91} \end{aligned}$$

$x \equiv 8 \pmod{35}$
$x \equiv 3 \pmod{65}$
$x \equiv 29 \pmod{91}$

Ya que los módulos no son primos entre sí, utilizaremos el sistema equivalente de congruencias:

$x \equiv 8 \pmod{5}$
$x \equiv 3 \pmod{13}$
$x \equiv 29 \pmod{7}$

cuya solución es:

i	a	m	c	d	b
1	8	5	91	1	273
2	3	13	35	3	133
3	29	7	65	4	393

Por tanto $x = 393$.

Ejercicio 2.21

Una expedición de seguidores de un club de fútbol llega en 5 aviones iguales completamente llenos al aeropuerto de la ciudad del equipo rival con el que van a disputar la semifinal de la Copa de Europa. Se sabe que si a los integrantes de 2 aviones se les transportara al estadio en minibuses de 15 pasajeros quedarían 3 de ellos sin ser transportados; que si a los integrantes de 3 aviones se les llevase en minibuses de 14 pasajeros uno de ellos se quedaría en el aeropuerto y que si a todos los expedicionarios se les transportase en minibuses de 8 pasajeros quedarían 3 asientos libres en el último de ellos. El equipo rival viste camisetas a rayas y, además, se sabe que ha reservado para los expedicionarios un máximo de 2000 entradas. Si todos los aficionados que han viajado van a poder ver el partido ¿Cuántas personas componen la expedición?

Solución:

$2x \equiv 3 \pmod{15}$
$3x \equiv 1 \pmod{14}$
$5x \equiv 3 \pmod{8}$

esto es,

$x \equiv 9 \pmod{15}$
$x \equiv 5 \pmod{14}$
$x \equiv 7 \pmod{8}$

equivalente a

$$x \equiv 9 \mod 15$$
$$x \equiv 5 \mod 7$$
$$x \equiv 7 \mod 8$$

i	a	m	c	d	b
1	*9*	*15*	*56*	*11*	*504*
2	*5*	*7*	*120*	*1*	*264*
3	*7*	*8*	*105*	*1*	*159*

*Solución: 5*159.*

Ejercicio 2.22

Demostrar que cualquier producto de números de la forma $4n+1$ es otra vez de esa forma. Deducir que hay infinitos primos de la forma $4n-1$.

Solución:

$\prod_{i=1}^{1}(4n_i+1) = (n_1+1)$.
Supongamos que $\prod_{i=1}^{r}(4n_i+1) = 4m+1$. *Tenemos que*

$$\prod_{i=1}^{r+1}(4n_i+1) = (\prod_{i=1}^{r}(4n_i+1))(n_{r+1}+1) = (4m+1)(n_{r+1}+1) = 4(mn_{r+1}+m+n_{r+1})+1.$$

Todo número impar m es de la forma $4n+1$ o $4n-1$. En efecto, al dividir m entre 4, el resto debe verificar que $0 \leq r \leq 4$. Pero, ya que m es impar, no puede ser ni 0 ni 2. Luego $m \equiv 1 \pmod 4$ o $m \equiv -1 \mod 4$.
Supongamos que solo existieran un número finito de primos de la forma $4n-1$. Llamémoslos $p_1 = 4n_1 - 1, \ldots p_r = 4n_r - 1$. Consideremos $m = 4(p_1 \cdots p_r) - 1$. Factoricemos $m = q_1 \cdots, q_s$. Algún q_j debe ser de la forma $4n-1$, pues si todos los q_j fuesen de la forma $4n+1$, entonces m sería de la forma $4n+1$, lo que es una contradicción. Pero, ya que ningún p_i divide a m, $q_j \neq p_i$, para $i = 1, \ldots, r$.

Ejercicio 2.23

Un grupo de 12 ladrones decidieron robar un cofre lleno de monedas de oro, que según un informe fidedigno contenía entre 2000 y 3000 monedas. El día del robo, uno de ellos resultó apresado, los 11 restantes decidieron repartir las monedas a partes iguales. Al hacer el reparto resultó que sobraron 8 monedas que decidieron darían a María, la mujer del ladrón apresado. María, no contenta con el reparto, delató a los dos ladrones que lo habían propuesto, después de lo cual quedaron 9 ladrones en libertad que volvieron a repartirse el botín. En este caso solo sobraron 2 monedas, que en su momento darían a Maria. Indignada María con el comportamiento de los compinches de su marido, decidió acabar con todos ellos y quedarse con todo el botín. Para ello, colocó una bomba en el lugar de reunión de la banda, desafortunadamente para María, la bomba hizo explosión cuando solo se encontraban 4 ladrones en el local. Los que quedaron, volvieron a decidir repartir el botín a partes iguales y dar a María la única moneda que sobraba del reparto. Esto indignó aún más a María, que

mediante intrigas consiguió que disputaran los ladrones entre ellos, muriendo 3 en la disputa. Los dos que quedaron con vida repartieron el botín a partes iguales y no sobró moneda alguna. ¿Qué cantidad de monedas tenía el cofre?

Solución:

Tenemos el siguiente sistema de congruencias:

$$\begin{cases} x \equiv 8 \pmod{11} \\ x \equiv 2 \pmod{9} \\ x \equiv 1 \pmod{5} \\ x \equiv 0 \pmod{2} \end{cases}$$

La solución es $866 + 990k'''$*, de donde* $x = 866 + 990 \cdot 2 = 2846$.

i	a	m	c	d	b
1	8	11	90	6	360
2	2	9	110	5	470
3	1	5	198	2	866
4	0	2	495	1	866

Ejercicio 2.24

Encontrar todas las soluciones del sistema de congruencias:

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv -2 \pmod{4} \\ x &\equiv 1 \pmod{7} \end{aligned}$$

Solución:

El sistema es equivalente a

$$\begin{cases} x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{4} \\ x \equiv 1 \pmod{7} \end{cases}$$

Sea $x = 3 + 45$*, entonces sustituyendo en la segunda* $k \equiv 2 \pmod{4}$*, de donde* $k = 3 + 4k'$*, esto es,* $x = 18 + 20k'$*. Sustituyendo en la tercera* $k' \equiv 3 \pmod{7}$*, esto es,* $k' = 3 + 7k''$ *y por tanto* $x = 78 + 140k''$*. Así la solución es 78.*

i	a	m	c	d	b
1	3	5	28	2	28
2	2	4	35	3	98
3	1	7	20	6	78

Ejercicio 2.25

Antonio,Pepe y Juan son tres campesinos que principalmente se dedican al cultivo de la aceituna. Este año la producción de los olivos de Antonio fue tres veces la de los de Juan y la de Pepe cinco veces la de los de Juan. Los molinos a los que estos campesinos llevan la aceituna, usan recipientes de 25 litros el de Juan, 7 litros el de Antonio y 16 litros el de Pepe. Al envasar el aceite producido por los olivos de Juan sobraron 21 litros, al envasar el producido por Antonio sobraron 3 litros y al envasar el producido por Pepe sobraron 11 litros. Sabiendo que la producción de Juan está entre 1000 y 2000 litros ¿cuál fue la producción de cada uno de ellos?.

Solución:

Tenemos el siguiente sistema de congruencias:

$$\begin{cases} x \equiv 21 \pmod{25} \\ 3x \equiv 3 \pmod{7} \\ 5x \equiv 11 \pmod{16} \end{cases}$$

que es equivalente a

$$\begin{cases} x \equiv 21 \pmod{25} \\ x \equiv 1 \pmod{7} \\ x \equiv 15 \pmod{16} \end{cases}$$

i	a	m	c	d	b
1	21	25	112	23	896
2	1	7	400	1	1296
3	15	16	175	15	1471

La solución es $x = 1471$, esto es, Juan produjo 1471, Antonio produjo $3 \cdot 1471$ y Pepe $5 \cdot 1471$.

Ejercicio 2.26

Calcular la menor capacidad posible de un depósito de agua sabiendo que a un depósito de doble capacidad le ha faltado un litro para poder ser llenado con garrafas de 5 litros, mientras que a uno de quíntuple capacidad también le ha faltado un litro tanto si se llenaba con garrafas de 7 litros como de 11 litros.

Solución:

Tenemos el sistema

$$\begin{cases} 2x+1 \equiv 0 \pmod{5} \\ 5x+1 \equiv 0 \pmod{7} \end{cases}$$

El sistema es equivalente a

$$\begin{cases} x \equiv 2 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$$

La solución es 32.

i	a	m	c	d	b
1	2	5	7	3	7
2	4	7	5	3	32

Ejercicio 2.27

Calcular el resto de dividir 279^{323} *entre 17. Análogamente, si se divide* 320^{207} *entre 13.*

Solución:

$279^{323} \equiv 7^{323} \pmod{17}$. *Además ya que* $\varphi(17) = 16$, *por el teorema de Euler* $7^{16} \equiv 1 \pmod{17}$. *Así* $279^{323} \equiv 7^{323} \equiv 7^{20\cdot 16+3} \equiv 7^3 \equiv 3 \pmod{17}$.
$320^{207} \equiv 8^{207} \pmod{13}$. *Además ya que* $\varphi(13) = 12$, *por el teorema de Euler* $8^{12} \equiv 1 \pmod{13}$. *Así* $320^{207} \equiv 8^{207} \equiv 8^{12\cdot 7+3} \equiv 8^3 \equiv 5 \pmod{13}$.

Ejercicio 2.28

Demostrar las reglas del 2,3,5 y 11 para la división.

Solución:

Sea $x = a_0 + a_1 10 + a_2 10^2 + \cdots a_n 10^n$.
2)
Tenemos que $1 \equiv 1 \pmod{10}$ *y* $10^k \equiv 0 \pmod{2}$, *de donde*

$$x \equiv x_0 \pmod{2}$$

Así $2 \mid x$ *si y sólo si* $2 \mid x_0$.
3)
Tenemos que $1 \equiv 1 \pmod{10}$ *y* $10^k \equiv 1 \pmod{3}$, *de donde*

$$x \equiv x_0 + x_1 + \cdots + x_n \pmod{3}$$

Así $3 \mid x$ *si y sólo si* $3 \mid (x_0 + x_1 + \cdots + x_n)$.
5)
Tenemos que $1 \equiv 1 \pmod{10}$ *y* $10^k \equiv 0 \pmod{5}$, *de donde*

$$x \equiv x_0 \pmod{5}$$

Así $5 \mid x$ *si y sólo si* $5 \mid x_0$.
11)
Tenemos que $1 \equiv 1 \pmod{10}$ *y* $10^k \equiv (-1)^k \pmod{11}$, *de donde*

$$x \equiv x_0 - x_1 + \cdots + (-1)^n x_n \pmod{11}$$

Así $11 \mid x$ *si y sólo si* $11 \mid (x_0 - x_1 + \cdots + (-1)^n x_n)$.

Ejercicio 2.29

Calcular las dos últimas cifras de $(3^3)^{94}$.

Solución:

$(3^3)^{94} = 3^{282}$. *Como* $\varphi(100) = 40$, $3^{40} \equiv 1 \pmod{100}$. *Así* $(3^3)^{94} = 3^{282} \equiv 3^{40\cdot 7+2} \equiv 3^2 \equiv 9 \pmod{100}$.

Ejercicio 2.30

En un garaje se aparcan coches(de cuatro ruedas)y camiones (de seis ruedas). ¿Cuál es el mayor número de camiones que se puede aparcar si el total de neumáticos en el garaje ha de ser 778? ¿Y si lo que queremos es aparcar el mayor número de coches?

Solución:

$[3k - 389, -2k + 389]$ *Ya que* $X = 3k - 389 > 0$ *e* $Y = -2k + 389 > 0$

Ejercicio 2.31

Calcular la menor solución positiva del sistema de congruencias

$$\begin{aligned} 3x &\equiv 1 \pmod 4 \\ 2x &\equiv 2 \pmod 5 \\ x &\equiv -1 \pmod 3 \end{aligned}$$

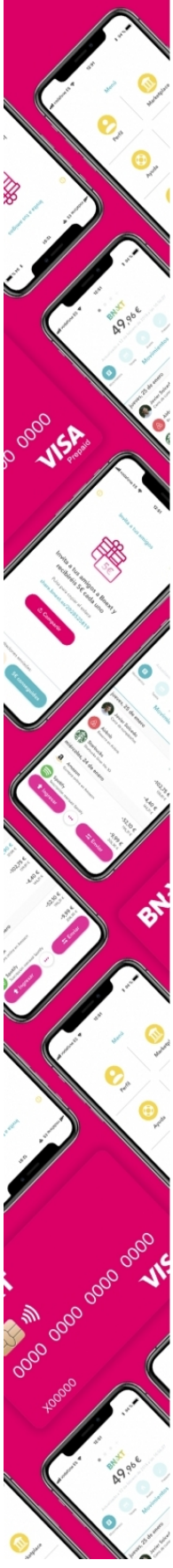
Solución:

El sistema es equivalente a

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 5 \\ x \equiv 2 \pmod 3 \end{cases}$$

Sea $x = 3 + 4k$, *entonces sustituyendo en la segunda* $k \equiv 2 \pmod 5$, *de donde* $k = 2 + k'$, *esto es,* $x = 11 + 20k'$. *Sustituyendo en la tercera* $k' \equiv 0 \pmod 3$, *esto es,* $k' = 3k''$ *y por tanto* $x = 11 + 60k''$. *Así la solución es 11.*

i	a	m	c	d	b
1	3	4	15	3	15
2	1	5	12	3	51
3	2	3	20	2	11



Ejercicio 2.32

Discutir y resolver el siguiente sistema de congruencias:

$$\begin{aligned} 3x &\equiv -1 \pmod 7 \\ x &\equiv -2 \pmod 5 \\ x &\equiv 1 \pmod 6 \end{aligned}$$

Solución:

El sistema es equivalente a

$$\begin{cases} x \equiv 2 \pmod 7 \\ x \equiv 3 \pmod 5 \\ x \equiv 1 \pmod 6 \end{cases}$$

Sea $x = 2 + 7k$, entonces sustituyendo en la segunda $k \equiv 3 \pmod 5$, de donde $k = 3 + 5k'$, esto es, $x = 23 + 35k'$. Sustituyendo en la tercera $k' \equiv 4 \pmod 6$, esto es, $k' = 4 + 6k''$ y por tanto $x = 163 + 210k''$. Así la solución es 163.

i	a	m	c	d	b
1	2	7	30	4	30
2	3	5	42	3	198
3	1	6	35	5	163

Ejercicio 2.33

Calcular la última cifra del número 87^{95}.

Solución:

Tenemos que $\varphi(10) = 4$ y por el teorema de Euler, $87^4 \equiv 1 \pmod{10}$. Así $87^{95} \equiv 87^3 \equiv 3658503 \equiv 3 \pmod{10}$. La última cifra es por tanto 3.

Ejercicio 2.34

Encuentra el menor entero par positivo que al dividirlo entre cinco dé resto tres, y que sumándole siete sea un múltiplo de trece.

Solución:

Tenemos el siguiente sistema de congruencias:

$$\begin{cases} 2x \equiv 3 \pmod 5 \\ 2x + 7 \equiv 0 \pmod{13} \end{cases}$$

que podemos escribir como

$$\begin{cases} x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod{13} \end{cases}$$

Sea $x = 4 + 5k$, entonces $4 + 5k \equiv 3 \pmod{13}$, de donde $k \equiv 5 \pmod{13}$ y así $k = 5 + 13h$, de donde $x = 4 + 5(5 + 13h) = 29 + 65h$. Por tanto la solución es 58.

Ejercicio 2.35

Razona que si $n > 3$ no es un múltiplo de 3, entonces la clase de -1 es un múltiplo de la clase de 3 módulo n.

Solución:

De la división euclídea $n = 3q + r$, deducimos que $r \in \{1, 2\}$, ya que n no es múltiplo de 3.
Si $n = 3q + 1$, entonces, tomando clases módulo n, $[0] = [3][q] + [1]$, esto es, $[3][q] = [-1]$ y $[3] \mid [-1]$.
Pero si $n = 3q + 2$, por ejemplo $n = 5$, tenemos que $[3]$ no divide a $[-1] = [4]$

Ejercicio 2.36

He encontrado un par de enteros a y $n > 3$, primos relativos, tales que al dividir $a^n - 1$ por n obtengo de resto 3. ¿Puedes asegurar que n no es primo?

Solución:

Si n es primo, entonces por el teorema de Fermat, $a^{n-1} \equiv 1 \pmod{n}$. Pero $a^{n-1} \equiv 3 \pmod{n}$, de donde $3 \equiv 1 \pmod{n}$, esto es, $n \mid 2$, lo que es imposible ya que $n > 3$.

Ejercicio 2.37

Demuestra que si c es múltiplo de 8 y a y b son primos relativos con 60, entonces $a^{b^c} \equiv a \pmod{60}$.

Solución:

Ya que $\varphi(60) = 16$. Por el teorema de Euler, $b^{\varphi(16)} \equiv 1 \pmod{16}$, esto es, $b^8 \equiv 1 \pmod{16}$, pues $\varphi(16) = 8$. Por tanto $b^c \equiv 1 \pmod{16}$, pues c es múltiplo de 8. Así $a^{b^c} \equiv a^1 \pmod{60}$.

Capítulo

3

Dominios euclídeos.

Ejercicios

Ejercicio 3.1

Sea X un conjunto no vacío y $R = \mathcal{P}(X)$, el conjunto de partes de X. Si se consideran en R las operaciones:

$$A + B = (A \cap \overline{B}) \cup (\overline{A} \cap B)$$

$$A \times B = A \cap B$$

demostrar que $(R, +, \times)$ es un anillo con elemento 1 igual a X.

Solución:

Veamos las propiedades de la suma: i) asociativa

$$\begin{aligned}
&A+(B+C) = (A \cap \overline{B+C}) \cup (\overline{A} \cap (B+C)) = (A \cap \overline{((B \cap \overline{C}) \cup (\overline{B} \cap C))}) \cup (\overline{A} \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C))) \\
&= (A \cap (\overline{(B \cap \overline{C})} \cap \overline{(\overline{B} \cap C)})) \cup (\overline{A} \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C))) \\
&= (A \cap ((\overline{B} \cup C) \cap (B \cup \overline{C}))) \cup (\overline{A} \cap ((B \cap \overline{C}) \cup (\overline{B} \cap C)) \\
&= (((A \cap \overline{B}) \cup (A \cap C)) \cap (B \cup \overline{C}))) \cup (((\overline{A} \cap B \cap \overline{C})) \cup (\overline{A} \cap \overline{B} \cap C)) \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad =
\end{aligned}$$

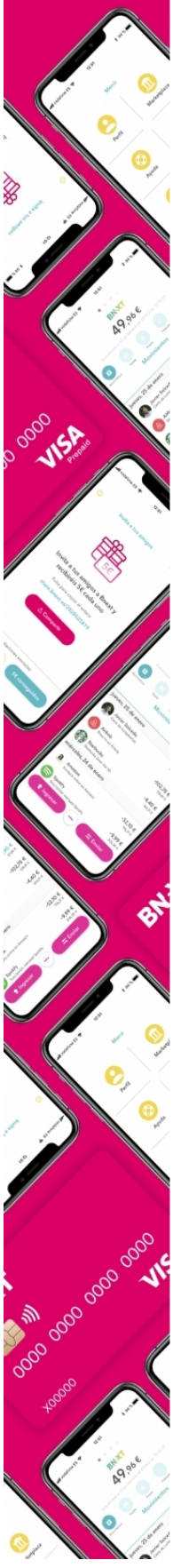
Ejercicio 3.2

Sea A un grupo abeliano y consideremos el producto cartesiano $R = \mathbb{Z} \times A$. Si en R definimos las siguientes operaciones:

$$(n, a) + (m, b) = (n + m, a + b)$$

$$(n, a)(m, b) = (nm, ma + nb)$$

demostrar que $(R, +, \cdot)$ es un anillo conmutativo con elemento 1 igual a $(1, 0)$.



Solución:

Veamos las propiedades de la suma: i) asociativa

$$\begin{aligned}((n,a)+(m,b))+(p,c) &= ((n+m),a+b)+(p,c) = ((n+m)+p,(a+b)+c)\\ &= (n+(m+p),a+(b+c)) = (n,a)+(m+p,b+c) = (n,a)+((m,b)+(p,c)).\end{aligned}$$

ii) conmutativa

$$(n,a)+(m,b) = (n+m,a+b) = (m+n,b+a) = (m,b)+(n,a).$$

iii) elemento cero

$$(n,a)+(0,0) = (n+0,a+0) = (n,a).$$

iv) elemento opuesto

$$(n,a)+(-n,-a) = (n+(-n),a+(-a)) = (0,0).$$

Veamos las propiedades del producto: i) asociativa

$$\begin{aligned}((n,a)(m,b))(p,c) &= ((nm),ma+nb)+(p,c) = ((nm)p,nmc+p(nb+ma))\\ &= (n(mp),n(pb+mc)+mpa)) = (n,a)(mp,pb+mc) = (n,a)((m,b)(p,c)).\end{aligned}$$

ii) conmutativa

$$(n,a)(m,b) = (nm,ma+nb) = (mn,nb+ma) = (m,b)(n,a).$$

iii) elemento uno

$$(n,a)(1,0) = (n1,1a+n0) = (n,a).$$

Veamos la propiedad distributiva:

$$\begin{aligned}&(n,a)((m,b))+(p,c) = (n,a)(m+p,b+c) = (n(m+p),(m+p)a+n(b+c))\\ &= (nm+np,ma+nb+pa+nc) = (nm,ma+nb)+(np,pa+nc) = (n,a)(m,b)+(n,a)(p,c).\end{aligned}$$

Ejercicio 3.3

En el conjunto $\mathbb{Z}$ de los enteros se definen las siguientes operaciones:

$$a \oplus b = a+b-1$$

y

$$a \otimes b = a+b-ab.$$

Demuestra que $(\mathbb{Z},\oplus,\otimes)$ es un dominio de integridad.

Solución:

Propiedades de $\oplus$*:*
Asociativa $a\oplus(b\oplus c)=a\oplus(b+c-1)=a+b+c-1-1$ *y* $(a\oplus b)\oplus c=(a+b-1)\oplus c=a+b-1+c-1$.
Conmutativa: $a\oplus b=a+b-1=b+a-1=b\oplus a$.
Elemento cero: Es 1, *ya que* $a\oplus 1=a+1-1=a$
Elemento opuesto: Es $2-a$, *ya que* $a\oplus(2-a)=a+2-a-1=1$.
Propiedades de $\otimes$*:*
Asociativa $a\otimes(b\otimes c)=a\otimes(b+c-bc)=a+b+c-bc-ab-ac+abc$ *y* $(a\otimes b)\otimes c=(a+b-ab)\otimes c=a+b-ab+c-ac-bc+abc$.
Conmutativa: $a\otimes b=a+b-ab=b+a-ba=b\otimes a$.
Elemento uno: Es 0, *ya que* $a\otimes 0=a+0-a\cdot 0=a$
Propiedad distributiva: $a\otimes(b\oplus c)=a\otimes(b+c-1)=a+b+c-1-ab-ac+a$ *y* $(a\otimes b)\oplus(a\otimes c)=(a+b-ab)\oplus(a+c-ac)=a+b-ab+a+c-ac-1$.
Luego es un anillo unitario conmutativo.
Dominio de integridad: Si $a\otimes b=1$, *entonces* $a+b-ab=1$, *es decir* $a+b(1-a)=1$. *Esta ecuación solo tiene solución si* $a=1$ *o* $b=1$. *En efecto, si* $a\neq 1$, *entonces* $b=(1-a)/(1-a)=1$ *y análogamente, si* $b\neq 1$, *entonces* $a=(1-b)/(1-b)=1$.

Ejercicio 3.4

En el conjunto $\mathbb{Z}\times\mathbb{Z}$ *de las parejas de enteros se definen las siguientes operaciones:*

$$(a,b)+(c,d)=(a+c,b+d)$$

y

$$(a,b)(c,d)=(ac,bd).$$

Demuestra que $(\mathbb{Z}\times\mathbb{Z},+,\cdot)$ *es un anillo conmutativo con unidad. Prueba que no es dominio de integridad y calcula sus unidades y sus divisores de cero.*

Solución:

No es dominio de integridad, ya que por ejemplo, $(1,0)(0,1)=(0,0)$ *y* $(1,0)\neq(0,0)$ *y* $(0,1)\neq(0,0)$.
Ya que $\mathbb{Z}^\times=\{1,-1\}$, *si* $(a,b)(x,y)=(1,1)$, *entonces* $ax=1$ *y* $by=1$, *de donde* $(\mathbb{Z}\times\mathbb{Z})^\times=\{(1,1),(1,-1),(-1,1),(-1,-1)\}$.
Ya que $\mathbb{Z}$ *es un dominio de integridad, si* $(a,b)(x,y)=(0,0)$, *entonces* $ax=0$ *y* $by=0$, *de donde* $\{(a,0);a\neq 0\}$ *y* $\{(0,b);b\neq 0\}$ *son los divisores de cero.*

Ejercicio 3.5

En un anillo A *un elemento* a *es idempotente si* $a^2=a$. *Demuestra que en un dominio de integridad los únicos idempotentes son 0 y 1.*

Solución:

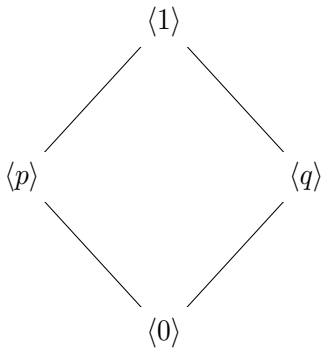
Sea $a\neq 0$ *idempotente en un dominio de integridad* A. *Entonces* $(1-a)a=a-a^2=a-a=0$, *de donde* $1-a=0$, *esto es,* $a=1$.

Ejercicio 3.6

Determinar los ideales del anillo cociente $\mathbb{Z}_n$. Describir el retículo de ideales de este anillo cuando $n = pq$ siendo p y q primos positivos distintos.

Solución:

Los ideales de $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ son de la forma $\langle \overline{m} \rangle$ con $m|n$. Así si $n = pq$, los ideales son $\langle \overline{p} \rangle$, $\langle \overline{q} \rangle$, $\langle \overline{1} \rangle$, $\langle \overline{n} \rangle = \langle \overline{0} \rangle$.



Ejercicio 3.7

Sea A un dominio de integridad y $a, b, c \in A$. Demostrar:

i) $b \mid a \Rightarrow b \mid ac$.

ii) $b \mid a$ *y* $c \mid b \Rightarrow c \mid a$.

iii) $b \mid a$ *y* $b \mid (a + c) \Rightarrow b \mid c$.

iv) $b \mid a$ *y* $b \nmid c \Rightarrow b \nmid (a + c)$.

v) Si $c \neq 0$, $bc \mid ac \Leftrightarrow b|a$.

Solución:

(i) Si $b|a$, entonces $a = bq$, de donde $ac = bqc$ y por tanto $b|ac$.
(ii) Si $b|a$ y $c|b$, entonces $a = bq$ y $b = cq'$, de donde $a = cq'q$ y por tanto $c|a$.
(iii) Si $b|a$ y $b|(a + c)$, entonces $a = bq$ y $a + c = bq'$, de donde $c = b(q' - q)$ y por tanto $b|c$.
(iv) Es equivalente a (iii)
(v) Ya que $c \neq 0$, $bc|ac$ si y solo si $ac = bcq$ si y solo si $a = bq$ si y solo si $b|a$.

Ejercicio 3.8

El conjunto $A = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\} \subseteq \mathbb{Z}_{10}$ es cerrado para la suma y el producto.

- *Demostrar que A es un cuerpo.*
- *Demostrar que A no es un subanillo de $\mathbb{Z}_{10}$.*

Solución:

i) El elemento uno es $\overline{6}$*, ya que* $\overline{6}\cdot\overline{0}=\overline{0}$, $\overline{6}\cdot\overline{2}=\overline{2}$, $\overline{6}\cdot\overline{4}=\overline{4}$, $\overline{6}\cdot\overline{6}=\overline{6}$, $\overline{6}\cdot\overline{8}=\overline{8}$.
El inverso de los elementos no nulos es, $\overline{2}^{-1}=\overline{8}$ *ya que* $\overline{2}\cdot\overline{8}=\overline{6}$, $\overline{4}^{-1}=\overline{4}$ *ya que* $\overline{4}\cdot\overline{4}=\overline{6}$, $\overline{6}^{-1}=\overline{6}$ *ya que* $\overline{6}\cdot\overline{6}=\overline{6}$, $\overline{8}^{-1}=\overline{2}$ *ya que* $\overline{8}\cdot\overline{2}=\overline{6}$.
ii) No es subanillo, ya que por ejemplo, tienen distinto elemento uno.

Ejercicio 3.9

¿Cuáles de los siguientes conjuntos son subanillos del cuerpo $\mathbb{Q}$ *de los números racionales? (Siempre que aparece* $\frac{n}{m}$ *suponemos que* $m.c.d(n,m)=1$*).*

i) $\{\frac{n}{m}; m \text{ es impar }\}$

ii) $\{\frac{n}{m}; m \text{ es par }\}$

iii) $\{\frac{n}{m}; 4 \nmid m\}$

iv) $\{\frac{n}{m}; m.c.d(m,6)=1\}$

v) ¿Es alguno de los subconjuntos anteriores un ideal de $\mathbb{Q}$*?*

Solución:

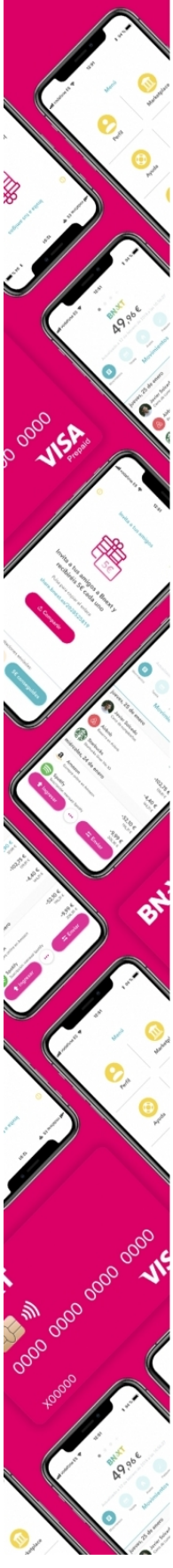
Tenemos que $\frac{n_1}{m_1}-\frac{n_2}{m_2}=\frac{n_1m_2-n_2m_1}{m_1m_2}$ *y* $\frac{n_1}{m_1}\frac{n_2}{m_2}=\frac{n_1n_2}{m_1m_2}$.
i) Sea $A=\{\frac{n}{m}; m \text{ es impar }\}$*. Si* $m_1=2k_1+1$ *y* $m_2=2k_2+1$*, entonces* $m_1m_2=2(2k_1k_2+k_1+k_2)+1$*, luego si* $\frac{n_1}{m_1},\frac{n_2}{m_2}\in A$*, entonces* $\frac{n_1}{m_1}-\frac{n_2}{m_2}\in A$ *y* $\frac{n_1}{m_1}\frac{n_2}{m_2}\in A$*. Además* $\frac{1}{1}\in A$*. Es por tanto un subanillo y no puede ser un ideal.*
ii) Sea $A=\{\frac{n}{m}; m \text{ es par }\}$*. Si* $m_1=2k_1$ *y* $m_2=2k_2$*, entonces* $m_1m_2=2(2k_1k_2)$*, luego si* $\frac{n_1}{m_1},\frac{n_2}{m_2}\in A$*, entonces* $\frac{n_1}{m_1}-\frac{n_2}{m_2}\in A$ *y* $\frac{n_1}{m_1}\frac{n_2}{m_2}\in A$*. Además* $\frac{1}{1}\notin A$*. No es por tanto un subanillo.*
Es un ideal, ya que si $\frac{a}{b}\in\mathbb{Q}$ *y* $\frac{n}{m}\in A$*, entonces* $\frac{a}{b}\frac{n}{m}=\frac{an}{bm}\in A$.
iii) Sea $A=\{\frac{n}{m}; 4 \nmid m\}$*. No es un subanillo, pues por ejemplo* $\frac{1}{2}\in A$*, pero* $\frac{1}{2}\frac{1}{2}=\frac{1}{4}\notin A$*. El mismo ejemplo nos sirve para comprobar que no es un ideal.*
iv) Sea $A=\{\frac{n}{m}; m.c.d(m,6)=1\}$*. Si* $1=s_1m+6t_1$ *y* $1=s_2m+6t_2$*, entonces* $1=(s_1ms_2)m+6(6t_1t_2+s_1t_2m+s_2t_1m)$*,luego si* $\frac{n_1}{m_1},\frac{n_2}{m_2}\in A$*, entonces* $\frac{n_1}{m_1}-\frac{n_2}{m_2}\in A$ *y* $\frac{n_1}{m_1}\frac{n_2}{m_2}\in A$*. Además* $\frac{1}{1}\in A$*. Es por tanto un subanillo y no puede ser un ideal.*

Ejercicio 3.10

Sea $\varphi: A\to A$ *un homomorfismo de anillos y sea* $B=\{a\in A;\varphi(a)=a\}$*. Demostrar que* B *es un subanillo de* A*.*

Solución:

i) Si $a,b\in B$*, entonces* $\varphi(a-b)=\varphi(a)-\varphi(b)=a+b$*, de donde* $a-b\in B$.
ii) Si $a,b\in B$*, entonces* $\varphi(ab)=\varphi(a)\varphi(b)=ab$*, de donde* $ab\in B$.
iii) Ya que $\varphi(1)=1$*, tenemos que* $1\in B$.



Ejercicio 3.11

Sea A un anillo y sea $a \in A$ un elemento invertible. Demostrar que la aplicación $\varphi_a : A \to A$ dada por $\varphi_a(x) = axa^{-1}$ es un automorfismo de A.

Solución:

Es aplicación: Si $x = y$ entonces $axa^{-1} = aya^{-1}$.
Es inyectiva: Si $axa^{-1} = aya^{-1}$, entonces $x = y$.
Es suprayectiva: Si $y \in A$, consideramos $x = a^{-1}ya$, entonces $\varphi_a(x) = axa^{-1} = aa^{-1}yaa^{-1} = y$.
Es homomorfismo: $\varphi_a(x + y) = a(x + y)a^{-1} = axa^{-1} + aya^{-1} = \varphi_a(x) + \varphi_a(y)$
$\varphi_a(xy) = a(xy)a^{-1} = axa^{-1}aya^{-1} = \varphi_a(x)\varphi_a(y)$
$\varphi_a(1) = a1a^{-1} = 1$.

Ejercicio 3.12

Sea A un dominio de integridad. Si la característica de A es cero entonces existe un homomorfismo inyectivo de $\mathbb{Z}$ en A y si la característica de A es p (con p primo) entonces entonces existe un homomorfismo inyectivo de $\mathbb{Z}_p$ en A.

Solución:

Consideremos la aplicación $\chi : \mathbb{Z} \to A$ definida por $\chi(n) = n \cdot 1_A$. Ya que

1.- $\chi(1) = 1_A$,

2.- $\chi(n + m) = (n + m) \cdot 1_A = n \cdot 1A + m \cdot 1_A = \chi(n) + \chi(m)$,

3.- $\chi(nm) = (nm) \cdot 1_A = (n \cdot 1_A)(m \cdot 1_A) = \chi(n)\chi(m)$.

tenemos que χ es un homomorfismo de anillos.
Caso $\text{car}(A) = 0$. Ya que $\chi(n) = n \cdot 1_A = 0_A$ si y solo si $n = 0$, tenemos que χ es inyectiva.
Caso $\text{car}(A) = p$. Ya que $\chi(n) = n \cdot 1_A = 0_A$ si y solo si $p|n$, tenemos que $\ker(\chi) = p\mathbb{Z}$ y por tanto $\mathbb{Z}_p \cong \text{im}(\chi) \subseteq A$.

Ejercicio 3.13

Dados dos números naturales n y m, dar condiciones para que exista un homomorfismo de anillos de $\mathbb{Z}_n$ en $\mathbb{Z}_m$.

Solución:

Sea $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m$ una correspondencia dada por $\varphi([x]_n) = [x]_m$. Para que sea aplicación necesitamos que si $[x]_n = [y]_n$ se verifique entonces que $[x]_m = [y]_m$, esto es, que si $n|x - y$ entonces $m|x - y$.
Es claro que si $m|n$ esto se verifica. Veamos el recíproco. Tomemos $x = n$, $y = 0$, entonces $n|n - 0$, de donde $m|n - 0 = n$.

Ejercicio 3.14

Describir los ideales de $\mathbb{Z}_{14}$ enumerando los elementos de cada uno de ellos.

Solución:

Los ideales de $\mathbb{Z}$ son de la forma $n\mathbb{Z}$ con $n \geq 0$. Por tanto los ideales de $\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z}$ son de la forma $m\mathbb{Z}/n\mathbb{Z}$ con $m|n$.
Ya que los divisores de 14 son $1, 2, 7, 14$, tenemos 4 ideales, a saber, $\mathbb{Z}/14\mathbb{Z} = \mathbb{Z}_{14}$, $2\mathbb{Z}/14\mathbb{Z} = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}\}$, $7\mathbb{Z}/14\mathbb{Z} = \{\overline{0}, \overline{7}\}$, $14\mathbb{Z}/14\mathbb{Z} = \{\overline{0}\}$.

Ejercicio 3.15

Calcular en $\mathbb{Z}[i]$ todos los elementos z que cumplan $N(z) \leq 5$, ¿cuáles de ellos son irreducibles?.

Solución:

Sea $z = a + bi \in \mathbb{Z}[i]$.
$N(z) = 1$) De $1 = a^2 + b^2$, deducimos que $a^2 = 1$ y $b^2 = 0$ o $a^2 = 0$ y $b^2 = 1$. Por tanto $z \in \{1, -1, i, -i\}$.
$N(z) = 2$) De $2 = a^2 + b^2$, deducimos que $a^2 = 1$ y $b^2 = 1$. Por tanto $z \in \{1+i, 1-i, -1+i, -1-i\}$.
$N(z) = 3$) De $3 = a^2 + b^2$, deducimos que no existen.
$N(z) = 4$) De $4 = a^2 + b^2$, deducimos que $a^2 = 4$ y $b^2 = 0$ o $a^2 = 0$ y $b^2 = 4$. Por tanto $z \in \{2, -2, 2i, -2i\}$.
$N(z) = 5$) De $5 = a^2 + b^2$, deducimos que $a^2 = 1$ y $b^2 = 4$ o $a^2 = 4$ y $b^2 = 1$. Por tanto $z \in \{1+2i, 1-2i, -1+2i, -1-2i\}$.
Ya que 2 y 5 son primos los elementos de norma 2 y 5 son irreducibles.

Ejercicio 3.16

Calcula $A^\times$ las unidades del anillo A en los casos $A = \mathbb{Z}[i]$ y $A = \mathbb{Z}[\sqrt{-5}]$.

Solución:

i) Sea $z = a + bi \in \mathbb{Z}[i]$ una unidad, entonces $1 = a^2 + b^2$, de donde $a^2 = 1$ y $b^2 = 1$. Por tanto las unidades son $1, -1, i, -i$.
ii) Sea $z = a + bi \in \mathbb{Z}[\sqrt{-5}]$ una unidad, entonces $1 = a^2 + 5b^2$, de donde $a^2 = 1$ y $b = 0$. Por tanto las unidades son $1, -1$.

Ejercicio 3.17

Comprobar que los elementos $2, 3, 4 + \sqrt{10}, 4 - \sqrt{10}$ son irreducibles en $\mathbb{Z}[\sqrt{10}]$ pero no son primos. Como consecuencia deducir que en $\mathbb{Z}[\sqrt{10}]$ hay dos factorizaciones en irreducibles de 6 distintas.

Solución:

En $\mathbb{Z}[\sqrt{10}]$ su norma multiplicativa es $N(a + b\sqrt{10}) = |a^2 - 10b^2|$.
Irreducibilidad:
2) $N(2) = 4$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de 2 han de tener norma 2. Ahora bien si $N(a + b\sqrt{10}) = 2$, entonces $|a^2 - 10b^2| = 2$, lo que implica que $a^2 - 10b^2 = \pm 2$. Si reducimos módulo 5, obtenemos $\overline{a}^2 = \overline{2}$ o $\overline{a}^2 = \overline{3}$. Ambos casos no tienen solución. Por tanto 2 es irreducible.
3) $N(3) = 9$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de 2 han de tener norma 3. Ahora bien si $N(a + b\sqrt{10}) = 3$, entonces $|a^2 - 10b^2| = 3$, lo que implica que

$a^2 - 10b^2 = \pm 3$. Si reducimos módulo 5, obtenemos $\overline{a}^2 = \overline{3}$ o $\overline{a}^2 = \overline{3}$. Ambos casos no tienen solución. Por tanto 3 es irreducible.
$4+\sqrt{10})$ $N(4+\sqrt{10}) = 6$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de $4+\sqrt{10}$ han de tener norma 2 o 3. Acabamos de ver que no existen elementos de norma 2 ni 3. Por tanto $4+\sqrt{10}$ es irreducible.
$4-\sqrt{10})$ $N(4-\sqrt{10}) = 6$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de $4-\sqrt{10}$ han de tener norma 2 o 3. Acabamos de ver que no existen elementos de norma 2 ni 3. Por tanto $4-\sqrt{10}$ es irreducible.
Primalidad:
Ahora $6 = 2 \cdot 3 = (4+\sqrt{10})(4-\sqrt{10})$.
2) $2|6 = (4+\sqrt{10})(4-\sqrt{10})$. Ya que, si $z \mid z'$ entonces $N(z) \mid N(z')$, tenemos que como $N(2) = 4 \nmid 6 = N(4+\sqrt{10}$, $2 \nmid 4+\sqrt{10}$ y análogamente $2 \nmid 4-\sqrt{10}$, luego 2 no es primo.
De forma análoga probamos que 3, $4+\sqrt{10}$ y $4-\sqrt{10}$ no son primos.

Ejercicio 3.18

Demostrar que los elementos $2, 7, 1+\sqrt{-13}$ y $1-\sqrt{-13}$ son irreducibles no asociados en $\mathbb{Z}[\sqrt{-13}$. Encontrar dos factorizaciones distintas en irreducibles de 14 y a partir de ella concluir que en $\mathbb{Z}[\sqrt{-13}]$ hay elementos irreducibles que no son primos.

Solución:

En $\mathbb{Z}[\sqrt{-13}]$ su norma multiplicativa es $N(a+b\sqrt{-13}) = a^2 + 13b^2$.
Irreducibilidad:
2) $N(2) = 4$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de 2 han de tener norma 2. Ahora bien si $a+b\sqrt{-13} = 2$, entonces $a^2 + 13b^2 = 2$. Si reducimos módulo 13, obtenemos $\overline{a}^2 = \overline{2}$. Ambos casos no tienen solución. Por tanto 2 es irreducible.
3) $N(7) = 49$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de 7 han de tener norma 7. Ahora bien si $a+b\sqrt{-13} = 7$, entonces $a^2 + 13b^2 = 7$. Si reducimos módulo 13, obtenemos $\overline{a}^2 = \overline{7}$. Ambos casos no tienen solución. Por tanto 7 es irreducible.
$1+\sqrt{-13})$ $N(1+\sqrt{-13}) = 14$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de $1+\sqrt{-13}$ han de tener norma 2 o 7. Acabamos de ver que no existen elementos de norma 2 ni 7. Por tanto $1+\sqrt{-13}$ es irreducible.
$1-\sqrt{-13})$ $N(1-\sqrt{-13}) = 14$. Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de $1-\sqrt{-13}$ han de tener norma 2 o 7. Acabamos de ver que no existen elementos de norma 2 ni 7. Por tanto $1-\sqrt{-13}$ es irreducible.
Primalidad:
Ahora $14 = 2 \cdot 7 = (1+\sqrt{-13})(1-\sqrt{-13})$.
2) $2|14 = (1+\sqrt{-13})(1-\sqrt{-13})$. Ya que, si $z \mid z'$ entonces $N(z) \mid N(z')$, tenemos que como $N(2) = 4 \nmid 14 = N(1+\sqrt{-13}$, $2 \nmid 1+\sqrt{-13}$ y análogamente $2 \nmid 1-\sqrt{-13}$, luego 2 no es primo.
De forma análoga probamos que 7, $1+\sqrt{-13}$ y $1-\sqrt{-13}$ no son primos.

Ejercicio 3.19

En el anillo $\mathbb{Z}[i]$ calcular el máximo común divisor y el mínimo común múltiplo de $a = 2i$ y $b = 3-7i$. Calcular además elementos s y t tales que $sa + tb = m.c.d(a, b)$.

Solución:

i	q	r	s	t
0	-	2i	1	0
1	i	3 + -7i	0	1
2	-4 + -2i	2i	1	0
3	1 -i	-1 + i	4 + 2i	1

$m.c.d = 1 - i$, $s = 4 + 2i$, $t = 1$.

Ejercicio 3.20

Calcular las unidades de $\mathbb{Z}[\sqrt{-3}]$ *y demostrar que en este anillo* $4 = 2 \cdot 2 = (1 + \sqrt{-3})(1 - \sqrt{-3})$ *son dos factorizaciones en irreducibles distintas del elemento 4. Razonar que los elementos en las factorizaciones no son primos.*

Solución:

Sea $a + b\sqrt{-3}$ *una unidad en* $\mathbb{Z}[\sqrt{-3}]$.
Entonces, $(a + b\sqrt{-3})(c + d\sqrt{-3}) = 1$ *para algún* $c + d\sqrt{-3} \in \mathbb{Z}[\sqrt{-3}]$.
Tomando normas obtenemos $(a^2 + 3b^2)(c^2 + 3d^2) = 1$, *de donde* $a^2 + 3b^2 = 1$ *(ya que la suma de cuadrados no puede ser negativa). Por tanto* $a = \pm 1$ *y* $b = 0$.
Ya que -1 y 1 son claramente unidades en $\mathbb{Z}[\sqrt{-3}]$, *concluimos que* $\mathbb{Z}[\sqrt{-3}]^\times = \{-1, 1\}$.
2 *y* $1 \pm \sqrt{-3}$ *son irreducibles no asociados.*
2 es irreducible pero no es primo. En efecto, $2 \mid (1+\sqrt{-3})(1-\sqrt{-3})$, *pero* $2 \nmid (1+\sqrt{-3})$ *y* $2 \nmid (1-\sqrt{-3})$.

Ejercicio 3.21

En el anillo $\mathbb{Z}[i]$ *calcular elementos* u *y* v *tales que* $(2 + 5i)u + (3 - 4i)v = 1 + i$.

Solución:

i	q	r	s	t
0	-	2 + 5i	1	0
1	-1 + i	3 -4i	0	1
2	2	1 -2i	1	1 -i
3	1 -2i	1	-2	-1 + 2i

$(d, s, t) = (1, -2, -1 + 2i)$.

Ejercicio 3.22

Da la solución general, si existe, de la ecuación diofántica en $\mathbb{Z}[i]$, $4x + (3 + 3i)y = -1 + 5i$.

Solución:

$x = (3k + 2) - 10i, y = (-2k + 6) + (2k + 9)i$.

Ejercicio 3.23

Factoriza $15+42i$ *y* $9-2i$ *en* $\mathbb{Z}[i]$. *Calcula* $m.c.d(15+42i, 9-2i)$.

Solución:

Ya que $15+42i = 3(1-4i)(3-2i)$ *y* $9-2i = (1-4i)(2-i)$, *tenemos que* $m.c.d = 1-4i$ *y* $m.c.m = 3(1-4i)(3-2i)(2-i)$.

Ejercicio 3.24

En $\mathbb{Z}[\sqrt{3}]$ *factoriza* $3+\sqrt{3}$ *en irreducibles y calcula* $m.c.d(3+\sqrt{3}, 2)$ *y* $m.c.d(3+\sqrt{3}, 2)$.

Solución:

Tenemos que $3+\sqrt{3} = \sqrt{3}(1+\sqrt{3})$.

Ejercicio 3.25

Demuestra que los elementos $2, 1+\sqrt{-7}, 1-\sqrt{-7}$ *de* $\mathbb{Z}[\sqrt{-7}]$ *son irreducibles pero no son primos y encuentra dos factorizaciones que no sean esencialmente idénticas de 8 en irreducibles. ¿Qué se puede concluir entonces de las propiedades aritméticas de* $\mathbb{Z}[\sqrt{-7}]$*?*

Solución:

$8 = 2\cdot 2\cdot 2 = (1+\sqrt{-7})(1-\sqrt{-7})$. *Sea* $a+b\sqrt{-7}$ *una unidad en* $\mathbb{Z}[\sqrt{-7}]$.
Entonces, $(a+b\sqrt{-7})(c+d\sqrt{-7}) = 1$ *para algún* $c+d\sqrt{-7} \in \mathbb{Z}[\sqrt{-7}]$.
Tomando normas obtenemos $(a^2+7b^2)(c^2+7d^2) = 1$, *de donde* $a^2+7b^2 = 1$ *(ya que la suma de cuadrados no puede ser negativa). Por tanto* $a = \pm 1$ *y* $b = 0$.
Ya que -1 y 1 son claramente unidades en $\mathbb{Z}[\sqrt{-7}]$, *concluimos que* $\mathbb{Z}[\sqrt{-7}]^\times = \{-1, 1\}$.
2 *y* $1 \pm \sqrt{-7}$ *son irreducibles no asociados.*

Ejercicio 3.26

En el anillo $\mathbb{Z}[i]$ *se consideran los elementos* $x = 1+3i$, $y = 3+4i$. *Factorizar* x *e* y *como producto de irreducibles y calcular su m.c.d y su m.c.m.*

Solución:

Sabemos que si $z \mid x$, *entonces* $N(z) | N(x) = 10$. *Probemos con* $N(z) = 2$. *Sea pues* $z = 1+i$. *Ya que* $\frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{(1+i)(1-i)} = \frac{4+2i}{2} = 2+i$. *Ya que* $N(2+i) = 5$, $(1+3i) = (1+i)(2+i)$ *es una factorización en irreducibles.*
Sabemos que si $z \mid y$, *entonces* $N(z) | N(y) = 25$. *Probemos con* $N(z) = 5$. *Sea pues* $z = 2+i$. *Ya que* $\frac{3+4i}{2+i} = \frac{(3+4i)(2-i)}{(2+i)(2-i)} = \frac{10+5i}{5} = 2+i$. *Ya que* $N(2+i) = 5$, $(3+4i) = (2+i)^2$ *es una factorización en irreducibles.*
Así $m.c.d(x, y) = 2+i$ *y* $m.c.m(x, y) = (2+i)^2(1+i) = -1+7i$.

Ejercicio 3.27

En el anillo $\mathbb{Z}[i]$ resolver el siguiente sistema de congruencias:

$$\begin{aligned} x &\equiv i \pmod 3 \\ x &\equiv 2 \pmod{(2+i)} \\ x &\equiv (1+i) \pmod{(3+2i)} \\ x &\equiv (3+2i) \pmod{(4+i)} \end{aligned}$$

Solución:

i	a	m	c	d	b
1	i	3	$9+32i$	i	-9 -32i
2	2	$2+i$	$30+33i$	-1	-42 -2i
3	$1+i$	$3+2i$	$21+18i$	2	33 -47i
4	$3+2i$	$4+i$	$12+21i$	-i	24 -14i

$x = 24 - 14i$.

Ejercicio 3.28

Resolver, dando la solución general, el siguiente sistema de congruencias en $\mathbb{Z}[i]$:

$$\begin{aligned} x &\equiv 1 \pmod{1+2i} \\ x &\equiv 1-i \pmod{1+3i} \\ x &\equiv 2i \pmod{3+2i} \end{aligned}$$

Solución:

i	a	m	c	d	b
1	1	$1+2i$	-3 + 11i	-1	3 -11i
2	1 -i	$1+3i$	-1 + 8i	-i	-8 + 12i
3	2i	$3+2i$	-5 + 5i	2	2 + 12i

$2 + 12i$.

Ejercicio 3.29

Calcular en $\mathbb{Z}[\sqrt{-2}]$ el m.c.d y el m.c.m de los elementos 3 y $2+\sqrt{-2}$.

Solución:

i	q	r
01	-	3
1	1	$2+\sqrt{-2}$
2	$\sqrt{-2}$	$1-\sqrt{-2}$

Por tanto m.c.d $= 1 - \sqrt{-2}$ *y* m.c.m $= 5 \cdot (2+\sqrt{-2})/(1-\sqrt{-2}) = 3\sqrt{-2}$.

Ejercicio 3.30

En el anillo $\mathbb{Z}[\sqrt{-2}]$ *resolver el siguiente sistema de congruencias*

$$\begin{aligned} x &\equiv 1+2\sqrt{-2} \pmod{2-3\sqrt{-2}} \\ x &\equiv 3 \pmod{1+\sqrt{-2}} \end{aligned}$$

Solución:

La solución general de la primera ecuación es $x = (1+\sqrt{-2}) + (2-3\sqrt{-2})t_1$. *Sustituyendo en la segunda y trasponiendo términos nos queda la ecuación*

$$(2-3\sqrt{-2})t_1 \equiv 3-(1+2\sqrt{-2}) = 2-2\sqrt{-2} \pmod{(1+\sqrt{-2})}.$$

Por el algoritmo de Euclides calculado tenemos que

$$t_1 \equiv -1\cdot(2-2\sqrt{-2}) = -2+2\sqrt{-2} \pmod{(1+\sqrt{-2})}$$

Sustituyendo en la solución de la primera obtenemos la solución general del sistema:

$$x = (1+\sqrt{-2}) + (2-3\sqrt{-2})((-2+2\sqrt{-2}) + (1+\sqrt{-2})t) = (9+11\sqrt{-2}) + (8-\sqrt{-2})t.$$

Ejercicio 3.31

En el anillo $\mathbb{Z}[\sqrt{5}]$ *comprobar que* $4 = 2\cdot 2$ *y* $4 = (1+\sqrt{5})(-1+\sqrt{5})$ *son dos factorizaciones en irreducibles no equivalentes, ¿es* $(1+\sqrt{5})$ *primo?.*

Solución:

$N(2) = 4$. *Ya que las unidades son los elementos de norma 1, los posibles divisores no unidades de 2 han de tener norma 2. Ahora bien si* $N(a+b\sqrt{5}) = 2$, *entonces* $|a^2-5b^2| = 2$, *lo que implica que* $a^2-5b^2 = \pm 2$. *Si reducimos módulo 5, obtenemos* $\overline{a}^2 = \overline{2}$ *o* $\overline{a}^2 = \overline{3}$. *Ambos casos no tienen solución. Por tanto 2 es irreducible.*
$N(1+\sqrt{5}) = |1-5| = 4$. *Por el apartado anterior es irreducible.*
$N(1-\sqrt{5}) = |1-5| = 4$. *Análogamente es irreducible.*
Como $4 = 2\cdot 2 = (1+\sqrt{5})(-1+\sqrt{5}$, *si*

Capítulo

4

Anillos de polinomios.

Ejercicios

Ejercicio 4.1

Hallar el cociente y el resto, en $\mathbb{Q}[X]$, al dividir los polinomios:

i) $X^3 - 7X - 1$ *entre* $X - 2$.

ii) $X^4 - 2X^2 - 1$ *entre* $X^2 + 3X - 1$.

iii) $X^4 + X^3 - 1$ *entre* $2X^2 + 1$.

iv) $X^3 - 3X + 2$ *entre* $X^3 - 3X^2 - X + 3$.

Solución:

i)

$$\begin{array}{rr|l} X^3 & -7X-1 & X-2 \\ \cline{3-3} -X^3+2X^2 & & X^2+2X-3 \\ \cline{1-1} 2X^2-7X & & \\ -2X^2+4X & & \\ \cline{1-1} -3X-1 & & \\ 3X-6 & & \\ \cline{1-1} -7 & & \end{array}$$

ii)

$$\begin{array}{rrr|l} X^4 & -2X^2 & -1 & X^2+3X-1 \\ \cline{4-4} -X^4-3X^3 & +X^2 & & X^2-3X+8 \\ \cline{1-2} -3X^3 & -X^2 & & \\ 3X^3+9X^2 & -3X & & \\ \cline{1-2} 8X^2 & -3X-1 & & \\ -8X^2-24X & +8 & & \\ \cline{1-2} -27X & +7 & & \end{array}$$

iii)

$$\begin{array}{rr|l} X^4+X^3 & -1 & 2X^2+1 \\ \cline{3-3} -X^4 \quad -\frac{1}{2}X^2 & & \frac{1}{2}X^2+\frac{1}{2}X-\frac{1}{4} \\ \cline{1-1} X^3-\frac{1}{2}X^2 & & \\ -X^3 \quad -\frac{1}{2}X & & \\ \cline{1-1} -\frac{1}{2}X^2-\frac{1}{2}X-1 & & \\ \frac{1}{2}X^2 \quad +\frac{1}{4} & & \\ \cline{1-1} -\frac{1}{2}X-\frac{3}{4} & & \end{array}$$

iv)

$$\begin{array}{rr|l} X^3 & -3X+2 & X^3-3X^2-X+3 \\ \cline{3-3} -X^3+3X^2 & +X-3 & 1 \\ \cline{1-2} 3X^2-2X-1 & & \end{array}$$

Ejercicio 4.2

Sean $f(X)$, $g(X)$ polinomios con coeficientes en $\mathbb{Q}$. Calcular el máximo común divisor y la identidad de Bézout.

(1) $f(X)=X^2-3X+2$, $g(X)=X^2+X+1$.

(2) $f(X)=X^2+X+1$, $g(X)=X^2-X+1$.

(3) $f(X)=X^3-3X+2$, $g(X)=X^3-3X^2-X+3$.

(4) $f(X)=X^3-3X+2$, $g(X)=X^4-5X^2+4$.

Solución:

i)

i	q	r	s	t
0	-	X^2-3X+2	*1*	*0*
1	*1*	X^2+X+1	*0*	*1*
2	$-X/4-5/16$	$-4X+1$	*1*	*-1*
3	$-64X/21+16/21$	$21/16$	$X/4+5/16$	$-X/4+11/16$

$(d,s,t)=(1,4X/21+5/21,-4X/21+11/21)$

ii)

i	q	r	s	t
0	-	X^2+X+1	*1*	*0*
1	*1*	X^2-X+1	*0*	*1*
2	$X/2-1/2$	$2X$	*1*	*-1*
3	$2X$	*1*	$-X/2+1/2$	$X/2+1/2$

$(d,s,t)=(1,-X/2+1/2,X/2+1/2)$

iii)

i	q	r	s	t
0	-	X^3-3X+2	1	0
1	1	X^3-3X^2-X+3	0	1
2	$X/3-7/9$	$3X^2-2X-1$	1	-1
3	$-27X/20-9/20$	$-20X/9+20/9$	$-X/3+7/9$	$X/3+2/9$

$(d,s,t)=(X-1,3X/20-7/20,-3X/20-1/10)$

iv)

i	q	r	s	t
0	-	X^4-5X^2+4	1	0
1	X	X^3-3X+2	0	1
2	$-X/2+1/2$	$-2X^2-2X+4$	1	$-X$

$(d,s,t)=(X^2+X-2,-1/2,X/2)$

Ejercicio 4.3

Encontrar los polinomios irreducibles de grados 2 y 3 en $\mathbb{Z}_2[X]$, $\mathbb{Z}_3[X]$ y $\mathbb{Z}_5[X]$.

Solución:

Calcularemos los polinomios mónicos irreducibles, salvo asociados. Para ello, comenzaremos calculando todos los polinomios mónicos.
$\mathbb{Z}_2[X]$). Los polinomios mónicos de grado 1 son: X, $X+1$. Todos son irreducibles.
Los polinomios mónicos de grado 2 son: X^2, X^2+1, X^2+X, X^2+X+1. Los polinomios reducibles se obtienen a partir de los polinomios irreducibles de orden 1. Por tanto son: X^2, $X(X+1)=X^2+X$ y $(X+1)^2=X^2+1$. Así los polinomios irreducibles son: X^2+X+1.
Los polinomios mónicos de grado 3 son: X^3, X^3+1, X^3+X, X^3+X+1, X^3+X^2, X^3+X^2+1, X^3+X^2+X, X^3+X^2+X+1.
Los polinomios reducibles se obtienen a partir de los polinomios irreducibles de orden 1 y 2. Por tanto son: X^3, $X^2(X+1)=X^3+X^2$, $X(X+1)^2=X^3+X$, $X(X^2+X+1)=X^3+X^2+X$, $(X+1)(X^2+X+1)=X^3+1$ y $(X+1)^3=X^3+X^2+X+1$. Así los polinomios irreducibles son: X^3+X+1 y X^3+X^2+1.
ii) Procediendo de la misma forma obtenemos: Polinomios irreducibles de grado 1 en $\mathbb{Z}_3$: X, $X+1$, $X-1$.
Polinomios irreducibles de grado 2 en $\mathbb{Z}_3$: X^2+1, X^2+X-1, X^2-X-1.
Polinomios irreducibles de grado 3 en $\mathbb{Z}_3$: X^3-X+1, X^3-X-1, X^3+X^2-1, X^3+X^2+X-1, X^3+X^2-X+1, X^3-X^2+1, X^3-X^2+X+1, X^3-X^2-X-1
iii) Procediendo de la misma forma obtenemos: Polinomios irreducibles de grado 1 en $\mathbb{Z}_5$: X, $X+1$, $X+2$, $X-1$, $X-2$.
Polinomios irreducibles de grado 2 en $\mathbb{Z}_5$: X^2+2, X^2-2, X^2+X+1, X^2+X+2, X^2+2X-2, X^2+2X-1, X^2-2X-2, X^2-2X-1, X^2-X+1, X^2-X+2
Polinomios irreducibles de grado 3 en $\mathbb{Z}_5$: X^3+X+1, X^3+X-1, X^3+2X+1, X^3+2X-1, X^3-2X+2, X^3-2X-2, X^3-X+2, X^3-X-2, X^3+X^2+1, X^3+X^2+2, X^3+X^2+X-2, X^3+X^2+X-1, X^3+X^2-2X+1, X^3+X^2-2X-1, X^3+X^2-X+1, X^3+X^2-X-2, X^3+2X^2+1, X^3+2X^2-2, X^3+2X^2+X-2, X^3+2X^2+X-1, X^3+2X^2+2X+2, X^3+2X^2+2X-2, X^3+2X^2-X+2, X^3+2X^2-X-1, X^3-2X^2+2, X^3-2X^2-1, X^3-2X^2+X+1, X^3-2X^2+X+2,

X^3-2X^2+2X+2, X^3-2X^2+2X-2, X^3-2X^2-X+1, X^3-2X^2-X-2, X^3-X^2-2, X^3-X^2-1, X^3-X^2+X+1, X^3-X^2+X+2, X^3-X^2-2X+1, X^3-X^2-2X-1, X^3-X^2-X+2, X^3-X^2-X-1

Ejercicio 4.4

Calcular, en $\mathbb{Z}_5[X]$, el máximo común divisor y la identidad de Bézout de $3X^3+4X^2+3$ y $3X^3+4X^2+3X+4$.

Solución:

$(d,s,t)=(-2,2,X+2)$.

Ejercicio 4.5

Calcular, en $\mathbb{Z}_3[X]$, el máximo común divisor y la identidad de Bézout de $X^5+2X^3+X^2+X+1$ y X^4+2X^3+X+1.

Solución:

$(d,s,t)=(X^3-X^2+1,-X^4+X^2-X,1)$

Ejercicio 4.6

Sea $f(X)=X^4-3X^3+X^2+3X-2\in\mathbb{Q}[X]$. Calcular el máximo común divisor de $f(X)$ y $f'(X)$. ¿Tiene $f(X)$ factores múltiples?

Solución:

$m.c.d(X^4-3X^3+X^2+3X-2,4X^3-9X^2+2X+3)=X-1$, *luego tiene factores múltiples.*

Ejercicio 4.7

Sea $m(X)=X^2+X\in\mathbb{Z}_3[X]$. Calcular un representante módulo $m(X)$ de $f(X)$ de grado menor o igual que el grado de $m(X)$ siendo

(1) $f(X)=X^3+2$,

(2) $f(X)=X^4+2X^2+1$

Solución:

i) El resto de la división euclídea de $f(X)$ y $m(X)$ es $X+2$.
i) El resto de la división euclídea de $f(X)$ y $m(X)$ es $-3X+1$.

Ejercicio 4.8

En $\mathbb{Z}_2[X]$ módulo X^4+X+1 calcular el inverso de $f(X)$, siendo:

(1) $f(X)=X^3+X$,

(2) $f(X) = X^2 + X + 1$,

(3) $f(X) = X$,

(4) $f(X) = X^2 + 1$.

Solución:

i) $(d, s, t) = (1, X^2 + X + 1, X^3 + X^2)$, *luego el inverso es* $X^3 + X^2$.
ii) $(d, s, t) = (1, 1, X^2 + X)$, *luego el inverso es* $X^2 + X$.
iii) $(d, s, t) = (1, 1, X^3 + 1)$, *luego el inverso es* $X^3 + 1$.
iv) $(d, s, t) = (1, X, X^3 + X + 1)$, *luego el inverso es* $X^3 + X + 1$.

Ejercicio 4.9

Resolver en $\mathbb{Z}_2[X]$

(1) $f(X) \equiv X \pmod{X^2 + X}$

(2) $f(X) \equiv 1 \pmod{X^2 + X + 1}$

Solución:

Tenemos que $f(X) = X + (X^2 + X)h$ *y sustituyendo en la segunda congruencia* $X + (X^2 + X)h \equiv 1 \pmod{X^2+X+1}$, *de donde* $(X^2+X)h \equiv 1-X \pmod{X^2+X+1}$. *Así* $h \equiv 1-X \pmod{X^2+X+1}$, *de donde* $h = (1 - X) + (X‘2 + X + 1)k$. *Sustituyendo obtenemos que* $f(X) = X + (X^2 + X)[(1 - X) + (X^2 + X + 1)k] = -X^3 + (X^2 + X)(X^2 + X + 1)k$.

Ejercicio 4.10

Calcular, si es posible, el inverso de la clase de X *en el anillo cociente* $\mathbb{Q}[X]/(X^4 + X + 1)$.

Solución:

$(d, s, t) = (1, 1, -X^3 - 1)$. *Por tanto existe inverso y es* $-X^3 - 1$.

Ejercicio 4.11

Demostrar que $\mathbb{Z}_2[X]/(X^4 + X + 1)$ *es un cuerpo y calcular el inverso de la clase de* $X^2 + 1$.

Solución:

Es irreducible y por un ejercicio anterior el inverso es $X^3 + X + 1$.

Ejercicio 4.12

Considerar el polinomio $f(X) = X^3 + 2X + 1 \in \mathbb{Z}_3[X]$. *Probar que* $f(X)$ *es irreducible. Calcular el inverso de la clase* $[X^2 + X + 2]$ *en el anillo cociente* $\mathbb{Z}_3[X]/(f(X))$.

Solución:

Es irreducible y $(d, s, t) = (1, X + 1, -X^2)$*, luego el inverso es* $-X^2$*.*

Ejercicio 4.13

Estudiar si los siguientes polinomios son reducibles o irreducibles en $\mathbb{Z}[X]$ *y en* $\mathbb{Q}[X]$*:*

i) $2X^5 - 6X^3 + 9X^2 - 15$.

ii) $X^4 + 15X^3 + 7$,

iii) $X^4 - 22X^2 + 1$,

iv) $X^3 + 17X + 36$,

v) $X^5 - X^2 + 1$,

vi) $X^4 + 10X^3 + 5X^2 - 2X - 3$.

Solución:

i) $f(X) = 2X^5 - 6X^3 + 9X^2 - 15$ *es primitivo. Por el criterio de Eisenstein para* $p = 3$*, es irreducible en* $\mathbb{Z}[X]$*. Como es primitivo es irreducible en* $\mathbb{Q}[X]$*.*
ii) $f(X) = X^4 + 15X^3 + 7$*. Hagamos reducción módulo 2,* $\varphi_2(f) = \overline{f} = X^4 + X^3 + \overline{1}$*. Este polinomio no tiene raíces en* $\mathbb{Z}_2$*. El único polinomio de grado dos es* $X^2 + X + \overline{1}$ *y no es divisor de* $\overline{f}$*, luego es irreducible en* $\mathbb{Z}_2$ *y por consiguiente* $f(X)$ *es irreducible en* $\mathbb{Z}$*.*
iii) $f(X) = X^4 - 22X^2 + 1$ *es bicuadrático. Hagamos el cambio* $Y = X^2$*. Entonces* $g(Y) = Y^2 - 22Y + 1$*. Veamos si este polinomio es irreducible. Las raíces de* $g(Y)$ *son* $\frac{22 \pm \sqrt{480}}{2} = 11 \pm 2\sqrt{30}$*. Así no tiene divisores de grado 1. Las raíces de* $f(X)$ *son* $\alpha_1 = \sqrt{11 + 2\sqrt{30}}$*,* $\alpha_2 = -\sqrt{11 + 2\sqrt{30}}$*,* $\alpha_3 = \sqrt{11 - 2\sqrt{30}}$ *y* $\alpha_4 = -\sqrt{11 - 2\sqrt{30}}$*. Si* f *factoriza como producto de dos polinomios de grado dos ....*
iv) $f(X) = X^3 + 17X + 36$ *es irreducible sobre* $\mathbb{Z}[X]$ *si y solo si tiene una raíz en* $\mathbb{Z}$*. Intentemos aplicar el teorema de Bolzano. Ya que* $f(1) = 18$ *y* $f(-2) = -42$*, existe una raíz real* γ *en el intervalo* $(-2, 1)$*. Como* $f'(X) = 3X^2 + 17 \geq 0$ *la función es creciente y la raíz no es entera.*
v) $f(X) = X^5 - X^2 + 1$*. Hagamos reducción módulo 2,* $\varphi_2(f) = \overline{f} = X^5 + X^2 + \overline{1}$*. Este polinomio no tiene raíces en* $\mathbb{Z}_2$*. El único polinomio de grado dos es* $X^2 + X + \overline{1}$ *y no es divisor de* $\overline{f}$*, luego es irreducible en* $\mathbb{Z}_2$ *y por consiguiente* $f(X)$ *es irreducible en* $\mathbb{Z}$*.*
vi) $f(X) = X^4 + 10X^3 + 5X^2 - 2X - 3$*. Hagamos reducción módulo 2.* $f_2 = X^4 + X^2 + \overline{1} = (X^2 + X + \overline{1})^2$*. Luego si* $f(X)$ *fuese reducible debería factorizar como dos polinomios de grado 2. Hagamos ahora reducción módulo 3,* $f_3 = X^4 + X^3 - X^2 + X = X(X^3 + X^2 - X + \overline{1})$*. Luego si* $f(X)$ *fuese reducible debería factorizar como un polinomio de grado 1 y un polinomio de grado 3. Luego las factorizaciones son incompatibles.*

Ejercicio 4.14

Calcular las unidades de los anillos cociente $\mathbb{Z}_5[X]/(X^2 + X + 1)$*,* $\mathbb{Z}_5[/(X^2 + 1)$ *y* $\mathbb{Z}_3[X]/(X^2 + 2)$*.*

Solución:

i) $[X], [X+1], [X+2], [X+3], [X+4]$.
ii) $[X], [X+1], [X+4]$.
iii) $[X]$.

Ejercicio 4.15

Hallar la intersección, la suma y el producto de los ideales de $\mathbb{Q}[X]$ *generados por los polinomios* X^2+X-2 *y* X^2-1.

Solución:

$m.c.m(X^2+X-2, X^2-1) = X^3+2X^2-X-2$, $m.c.d(X^2+X-2, X^2-1) = X-1$ *y* $(X^2+X-2)(X^2-1) = X^4+X^3-3X^2-X+2$.
i) $\langle X^3+2X^2-X-2\rangle$.
ii) $\langle X-1\rangle$.
iii) $\langle X^4+X^3-3X^2-X+2\rangle$.

Ejercicio 4.16

Factoriza los siguientes polinomios como producto de irreducibles en $\mathbb{Z}[X]$.

1. $X^6-X^5-10X^2+15X-5$.

2. $3X^4-5X^3-101$.

3. $2X^4+4X-1$.

Solución:

i) $(X-1)(X^5-10X+5)$.
ii) es irreducible
iii) es irreducible

Ejercicio 4.17

Calcular las raíces racionales de:

i) X^3-X^2-3X+6.

ii) $6X^3+X^2-5X-2$.

iii) $3X^3+7X^2-7X-3$.

Solución:

i) $(X+2)(X^2-3X+3)$
ii) $(X-1)(2X+1)(3X+2)$
iii) $(X-1)(X+3)(3X+1)$

Ejercicio 4.18

Sea $f(X) = X^4+15X^3+72X^2+137X+174$. *Sabiendo que* $f(-7) = -1$, *calcular las raíces racionales de* $f(X)$.

Solución:

$(X+6)(X^3+9X^2+18X+29)$.

Ejercicio 4.19

Estudiar la irreducibilidad y la descomposición en irreducibles de los siguientes polinomios de $\mathbb{Q}[X]$:

i) $X^5+X^4-2X^3-2X^2-2X+4$.

ii) $X^4+4X^3+6X^2+4X-24$.

iii) $X^5-6X^4+14X^3-16X^2-16X+48$.

iv) $X^4+8X^3+22X^2+24X+9$.

Solución:

i) $(X-1)(X+2)(X^3-2)$
ii) $(X^2+2X-4)(X^2+2X+6)$
iii) $(X-2)(X^2-2X-4)(X^2-2X+6)$
iv) $(X+1)^2(X+3)^2$

Ejercicio 4.20

Estudiar la irreducibilidad y la descomposición en irreducibles del polinomio X^4+2X-1 *en* $\mathbb{Z}_2[X]$, $\mathbb{Z}_3[X]$ *y* $\mathbb{Q}[X]$.

Solución:

i) $f(X) = X^4+1$. *Ya que* $f(1) = 0$, *tenemos que* $f(X) = (X+1)^4$.
ii) $f(X) = X^4+2X+2$. *Ya que Ya que* $f(0) = 2$, $f(1) = 2$, $f(2) = 1$ *no tiene factores lineales. Los polinomios irreducibles de grado dos sobre* $\mathbb{Z}_3$ *son* X^2+1, X^2+X+2 *y* X^2+2X+2. *por lo que es irreducible.*
iii) $f(X+1) = X^4+4X^3+6X^2+6X+2$, *luego es irreducible por Eisenstein para* $p = 2$.

Ejercicio 4.21

Estudiar la irreducibilidad y la descomposición en irreducibles del polinomio X^4+3X-1 *en* $\mathbb{Z}_2[X]$, $\mathbb{Z}_3[X]$, $\mathbb{Z}_5[X]$ *y* $\mathbb{Q}[X]$.

Solución:

i) $f(X) = X^4 + X + 1$. *luego es irreducible*
ii) $f(X) = (X+2)(X+1)(X^2+1)$
iii)

Ejercicio 4.22

Factorizar $X^5 + X + 1 \in \mathbb{Z}_2[X]$ *usando el algoritmo de Berlekamp.*

Solución:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

$Qbasis = [[1,0,0,0,0],[0,1,0,1,1]]$

$X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1)$.

Ejercicio 4.23

Factorizar $X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \in \mathbb{Z}_2[X]$ *usando el algoritmo de Berlekamp.*

Solución:

$$\begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$Qbasis = [[1,0,0,0,0,0],[0,1,1,0,1,0]]$

$X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 = (X^3 + X + 1)(X^3 + X^2 + 1)$.

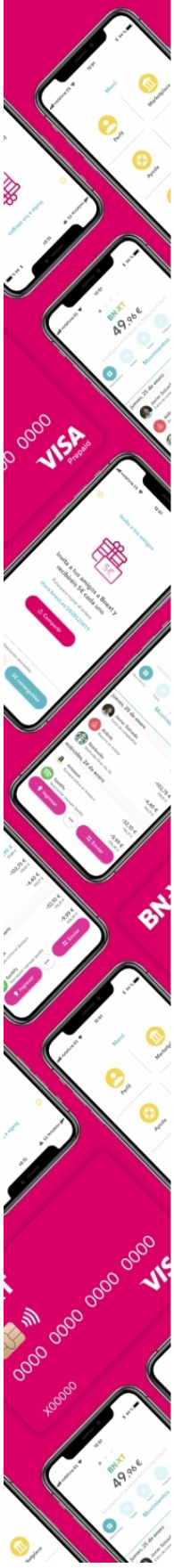
Ejercicio 4.24

Probar que $X^7 + X^3 + \overline{1} \in \mathbb{Z}_2[X]$ *es irreducible.*

Solución:

Sea $f(X) = X^7 + X^3 + \overline{1} \in \mathbb{Z}_2[X]$. *Veamos si tiene algún factor de grado 1. Ya que* $f(\overline{0}) = \overline{1}$ *y* $f(\overline{1}) = \overline{1}$, *no tiene factores de grado 1.*
El único polinomio irreducible de grado 2 en $\mathbb{Z}_2[X]$ *es* $X^2 + X + \overline{1}$. *Pero* $f(X) = (X^2 + X + \overline{1})(X^5 +$

$X^4 + X^2 + \overline{1}) + X$, luego no tiene factores de grado 2.
Los polinomios irreducibles de grado 3 en $\mathbb{Z}_2[X]$ son $X^3 + X + \overline{1}$ y $X^3 + X^2 + \overline{1}$, pero $f(X) = (X^3 + X + \overline{1})(X^4 + X^2 + X) + (X + \overline{1})$ y $f(X) = (X^3 + X^2 + \overline{1})(X^4 + X^3 + X^2) + (X^2 + \overline{1})$.
Por tanto el polinomio es irreducible.



Bibliografía

[1] Akritas, A.G., *Elements of Computer Algebra and Applications*, John Wiley and Sons, 1989.

[2] Alaca S., Williams K. *Introductory algebraic number theory*, Cambridge University Press, 2004.

[3] Clark, A., *Elementos de Algebra Abstracta*, Alhambra, 1974.

[4] Dorronsoro, J., Hernández, E.,*Números, grupos y anillos*, Addison-Wesley, 1996.

[5] Dummit, D.S., Foote, R.M., *Abstract Algebra*, Prentice Hall, 1991.

[6] Fraleigh, J. B., *Algebra Abstracta*, Addison Wesley Iberoamericana, 1987.

[7] Gallian, J., *Contemporary Abstract Algebra*, Houghton Mifflin, 1998.

[8] Goldstein, L.J., *Abstract Algebra. A first course*,Prentice Hall, 1973.

[9] Grimaldi, R.P.,*Matemáticas discretas y combinatoria*, Prentice Hall, 1997.

[10] Hibbard, A.C., Levasseur, K., Levasseur, K.C., *Exploring Abstract Algebra With Mathematica*, Springer, 1999.

[11] Scherk, J., *Algebra*, versión electrónica 2009.