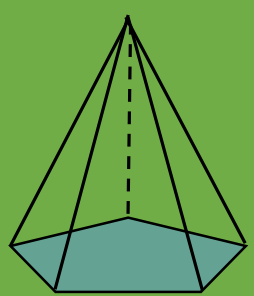
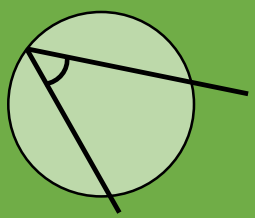
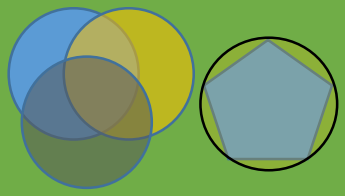
Algebra y Geometría I

$30x - 6y = 1 \quad x,y \in Z$

Lic. Toledo Christian







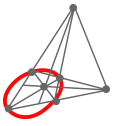
1ra Edición 2016

Toledo Christian

Álgebra y Geometría

Edición Toledo Christian

Profesorado de Matemática



Revista digital
Matemática, Educación e Internet. (http://www.tec-digital.itcr.ac.cr/revistamatematica/).

Índice general

1 — LÓGICA

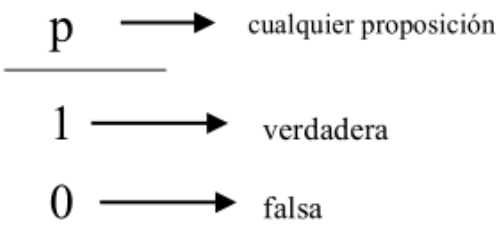
1.1 LOS SIGNOS DE LA LÓGICA PROPOSICIONAL

Definición 1.1

La lógica es la ciencia que estudia los principios y métodos para distinguir un razonamiento correcto de otro incorrecto. Pero, como la mayoría de las personas se preguntan (incluido yo) ¿ la lógica sirve para algo? esto es contestado por Leibniz de la siguiente manera:
Yo sostengo que la lógica es uno de los inventos más bellos del espíritu humano. Es como una especie de lenguaje universal, inteligible para todo el mundo. Por eso, cuando los hombres han de tomar, solos o en grupo, decisiones importantes, le serviría de gran utilidad el uso de la lógica para evitar dejarse llevar por embaucadores y vendedores de baratijas.

1.1.1 Variables proposicionales:

Para simbólizar las proposiciones simples se utilizan las letras minúsculas del alfabeto a partir de la $p(q,s,t,u,a,b,c,...)$Estas letras se denominan *variables propocionales* porque se utilizan para representar cualquier proposición del lenguaje natural.Por ejempo: la proposición simple *los gatos son mamiferos* se simbóliza con la letra p. Y la proposición comlepleja y los gatos son mamímeferos y le gustan los ratones , simbólizamos con las letras p y q. Advertimos que cualquier proposición simple obien es verdadera, o bien es falsa pero las dos a la vez. Este es el *principio de bivalencia* una proposición simple solo puede tener dos valores de verdad, o es verdadera o es falsa.



1.1.2 Símbolos auxiliares:

En lógica se utilizan paréntesis, corchetes y llaves para agrupar ordenadamente las proposiciones.
( ) , [ ] , { } .

1.1.3 Conectivas o constantes lógicas:

Se denominan conectivas a aquellos signos lógicos que sirven para unir a las proposiciones entre sí. Las conectivas que manejaremos son las siguientes:

Negador ($\sim$)

$\sim$ .... se lee *no*

$\sim p$... se lee *no p*

$\sim q$... se lee *no q*

Las expresiones siguientes: *No podremos ir de excursión a Bariloche* , *Pedro ni siquiera me escuchó*, las simbolizamos $\sim p$.

El negador es aquella conectiva que al aplicarse a una proposición cualquiera, sea simple o compleja, la convierte en falsa si es verdadera y en verdadera si es falsa.

p	$\sim p$
1	0
0	1

Conjuntor ($\wedge$):

$\wedge$ .... se lee **y**

$p \wedge q$ ... se lee **p y q**

Ejemplo 1.1

Las expresiones siguientes: *Hoy estamos alegres y nos iremos a bailar* , *Pedro es buena persona, aunque debería ducharse más*, *El sol se nubló, pero seguimos caminando*, las simbolizamos en lógica proposicional $p \wedge q$.

El conjuntor es aquella conectiva que sólo es verdadera si las dos proposiciones que une son ambas verdaderas, y que es falsa en los demás casos.

=>Tabla de verdad del conjuntor: (Las combinaciones posibles de los valores de verdad de 2 proposiciones (p,q), cada una de las cuales puede ser verdadera o falsa, son cuatro: que las dos sean verdaderas, que una sea verdadera y la otra falsa, que una sea falsa y la otra verdadera, y que las dos sean falsas. Para un número 'n' de proposiciones las combinaciones de sus valores de verdad serán 2^n .)

p	q	$p \wedge q$
1	1	**1**
1	0	**0**
0	1	**0**
0	0	**0**

p	q	r	$p \wedge q$	$(p \wedge q) \wedge r$
1	1	1	1	**1**
1	1	0	1	**0**
1	0	1	0	**0**
1	0	0	0	**0**
0	1	1	0	**0**
0	1	0	0	**0**
0	0	1	0	**0**
0	0	0	0	**0**

$\sim p \wedge q$.... se lee no p y q, y su tabla de verdad sería:

p	q	$\sim p$	$\sim p \wedge q$
1	1	0	**0**
1	0	0	**0**
0	1	1	**1**
0	0	1	**0**

$p \wedge \sim q$.... se lee p y no q, y su tabla de verdad es:

p	q	$\sim q$	$p \wedge \sim q$
1	1	0	**0**
1	0	1	**1**
0	1	0	**0**
0	0	1	**0**

$\sim p \wedge \sim q$.... se lee no p y no q , y su tabla de verdad es:

p	q	$\sim p$	$\sim q$	$\sim p \wedge \sim q$
1	1	0	0	**0**
1	0	0	1	**0**
0	1	1	0	**0**
0	0	1	1	**1**

Disyuntor ($\vee$):

$\vee$ ... se lee o

$p \vee q$ ... se lee p o q

Ejemplo 1.2

Las expresiones siguientes: *Pedro vendrá el lunes o el martes*, *O bien me quedo en casa o bien voy al cine*, *Tal vez escuche esa canción o tal vez me vaya a pasear al río* , las simbolizamos $\mathbf{p \vee q}$.

Definición 1.2

El disyuntor es aquella conectiva que sólo es falsa si las dos proposiciones que une son ambas falsas, y verdadera en los demás casos.

La tabla de verdad del disyuntor es:

p	q	$p \vee q$
1	1	**1**
1	0	**1**
0	1	**1**
0	0	**0**

$\sim p \vee q$.... se lee no p o q , y su tabla de verdad es:

p	q	$\sim p$	$\sim p \vee q$
1	1	0	**1**
1	0	0	**0**
0	1	1	**1**
0	0	1	**1**

$\sim p \vee q$.... se lee no p o q, y su tabla de verdad es:

p	q	$\sim p$	$\sim p \vee q$
1	1	0	**1**
1	0	0	**0**
0	1	1	**1**
0	0	1	**1**

$\sim (\sim p \vee q)$.... se lee*no es cierto que no* p o q, y su tabla de verdad es:

p	q	$\sim p$	$\sim p \vee q$	$\sim (\sim p \vee q)$
1	1	0	1	**0**
1	0	0	0	**1**
0	1	1	1	**0**
0	0	1	1	**0**

$\sim (p \wedge q) \vee \sim p$.... se lee *no es cierto que* p y q o no p, y su tabla de verdad es:

p	q	$p \wedge q$	$\sim (p \wedge q)$	$\sim p$	$\sim (p \wedge q) \vee \sim p$
1	1	1	0	0	**0**
1	0	0	1	0	**1**
0	1	0	1	1	**1**
0	0	0	1	1	**1**

Condicional ($\rightarrow$ ó $\Rightarrow$):
$\rightarrow$ se lee *si..., entonces...*

$p \rightarrow q$ ... se lee *si* p , *entonces* q (p es el antecedente, y q es el consecuente)

Ejemplo 1.3

Las expresiones *si llueve, las calles se mojan*, *si vienes mañana, iremos a la casa de Luis*, *Si supieras lo que me ha dicho Pedro, quedaría perplejo*, las simbólizamos como $p \rightarrow q$.

El condicional es aquella conectiva que sólo es falsa cuando, siendo el antecedente verdadero, el consecuente sea falso, y verdadera en los demás casos. Llamamos *antecedente* del condicional a la proposición que se halla a su izquierda, y *consecuente* a la que está a su derecha.

La tabla de verdad del condicional es:

p	q	$p \rightarrow q$
1	1	**1**
1	0	**0**
0	1	**1**
0	0	**1**

Ejemplos:$\sim p \rightarrow q$ ... se lee *si no p, entonces q* , y su tabla de verdad es

p	$\sim p$	q	$\sim p \rightarrow q$
0	1	1	**1**
0	1	0	**1**
1	0	1	**1**
1	0	0	**0**

Otro Ejemplo

p	q	$\sim q$	$p \rightarrow \sim q$	$\sim (p \rightarrow \sim q)$
1	1	0	0	**1**
1	0	1	1	**0**
0	1	0	1	**0**
0	0	1	1	**0**

Bicondicional($\leftrightarrow$):
$\rightarrow$ ... se lee *sólo si....*

$p \leftrightarrow q$.... se lee *p sólo si q* o *sólo si p, entonces q*

Ejemplo 1.4

Las expresiones *Sólo si llueve , me quedaré en casa, Sólo en el caso que sepas la primer pregunta bebérias responder la segunda, te contestaré sólo si tu respuesta me satisface*, las simbolizamos $p \leftrightarrow q$.

Definición 1.3
El bicondicional es aquella conectiva que sólo es verdadera si las dos proposiciones unidas por ella tienen ambas el mismo valor de verdad, es decir,son ambas verdaderas o falsas a la vez.

p	q	$p \leftrightarrow q$
1	1	**1**
1	0	**0**
0	1	**0**
0	0	**1**

Ejemplo:

$p \leftrightarrow \sim q$ se lee *Sólo si p , entonces no q* o también *p sólo si no q* y su tabla de valores es:

p	q	$\sim q$	$p \leftrightarrow \sim q$
1	1	0	**0**
1	0	0	**1**
0	1	0	**1**
0	0	1	**0**

1.1.4 Tablas de verdad de cualquier fórmulas

Para hallar la tabla de verdad de cualquier fórmula hay que dar los siguientes pasos:

1. En primer lugar, se asignan los valores 1*y*0 a las proposiciones simples que componen la fórmula, combinando de todos los modos posibles tales valores.Recordemos que para una fórmula con dos proposiciones distintas, las combinaciones posibles de sus valores de verdad son $2^2 = 4$

p	q
1	1
1	0
0	1
0	0

Para una fórmula con tres proposiciones distintas, las combinaciones posibles de sus valores de verdad son $2^3 = 8$. Con cuatro proposiciones son $2^4 = 16$. Etc.

p	q	r
1	1	1
1	1	0
1	0	1
1	0	0
0	1	1
0	1	0
0	0	1
0	0	0

p	q	r	s
1	1	1	1
1	1	1	0
1	1	0	1
1	1	0	0
1	0	1	1
1	0	1	0
1	0	0	1
1	0	0	0
0	1	1	1
0	1	1	0
0	1	0	1
0	1	0	0
0	0	1	1
0	0	1	0
0	0	0	1

El modo más fácil de combinar los valores de verdad de las proposiciones que integran cualquier fórmula, consiste en asignarle a la primera proposición por orden alfabético la mitad de 1 y la mitad de 0. A la siguiente proposición, la mitad de la mitad de 1, la mitad de la mitad de 0, hasta completar el número de las combinaciones que admita la fórmula Y a la última proposición de la fórmula siempre se le asignará 1 y 0 alternativamente hasta completar las combinaciones posibles de la fórmula.

Y en segundo lugar, se hallan los valores de verdad de las conectivas existentes en la fórmula, empezando por las menos dominantes (es decir, por las que afectan a menor parte de la fórmula) y terminando por la conectiva dominante (es decir, por aquella que afecta a toda la fórmula y cuya tabla de verdad, por tanto, será la tabla de verdad de la fórmula completa).

Tabla de verdad de la fórmula: $\sim p \rightarrow (r \wedge \sim q)$ se lee Si no p, entonces r y no q. La conectiva dominante es el $\rightarrow$.

p	q	r	$\sim q$	$r \wedge \sim q$	$\sim p$	$\sim p \rightarrow (r \wedge \sim q)$
1	1	1	0	0	0	1
1	1	0	0	0	0	1
1	0	1	1	1	0	1
1	0	0	1	0	0	1
0	1	1	0	0	1	0
0	1	0	0	0	1	0
0	0	1	1	1	1	1
0	0	0	1	0	1	0

1.1.5 ¿CÓMO FORMALIZAR EN LA LÓGICA PROPOSICIONAL CUALQUIER EXPRESIÓN DEL LENGUAJE NATURAL?

Formalizar una expresión del lenguaje natural consiste en destacar la *forma* en que se relacionan las proposiciones de esa expresión, prescindiendo del contenido o significado de éstas. Dicho de otro modo: consiste en *traducir* al lenguaje artificial de la lógica las expresiones del lenguaje natural.

Ejemplo 1.5

1. La comida no le supo bien: $\sim p$
2. Mañana es sábado y nos iremos a la playa: $p \wedge q$
3. Aunque tú no me quieras, yo te amo: $\sim p \wedge q$.
4. O bien te lo comes o no verás la tele: $p \vee \sim q$
5. O lo recoges todo o no vas de excursión y no te regalo el vestido: $p \vee (\sim q \wedge \sim r)$
6. Si vienes, no te lo olvides en casa: $p \rightarrow \sim q$.
7. Si no estuvo aquí el asesino, entonces no llegó a verlo o lo supo demasiado tarde: $\sim p \rightarrow (\sim q \vee r)$

8. No por mucho madrugar amanece más temprano: $\sim (p \rightarrow q)$
9. Sólo si baja la Bolsa 15 puntos, deberás vender el 10 % de las acciones de la empresa y no comunicarlo al Consejo: $p \leftrightarrow (q \wedge \sim r)$.
10. Sólo en el caso de que no sepas hacer el dibujo y haya dos preguntas en la 2da casilla del examen, deberás contestar únicamente a la primera de ellas: $(\sim p \wedge q) \leftrightarrow r$
11. Si Pedro sabe hablar inglés, entonces no habla francés, aunque si no supiese hablar inglés, tampoco hablaría francés: $(p \rightarrow \sim q) \wedge (\sim p \rightarrow \sim q)$
12. Si llegas después de las 10, te encontrarás con la puerta cerrada y no podrás cenar: $p \rightarrow (q \wedge \sim r)$
13. Juan abrirá la puerta y saldrá a la calle, sólo en el caso de que, si viene María con el coche, no venga con ella Pedro: $(p \wedge q) \leftrightarrow (r \rightarrow \sim s)$
14. No es verdad que si Antonio estudia, entonces María no trabaje: $\sim (p \rightarrow \sim q)$
15. Sólo si tú no lo has matado, te dejaremos libre: $\sim p \leftrightarrow q$
16. Si no crees que lo que te digo ni lo que te dice Juan, nunca sabrás lo que pasó: $(\sim p \wedge \sim q) \rightarrow \sim r$
17. No es cierto que Fernando esté en Madrid y Juan no esté en Ávila: $\sim (p \wedge \sim q)$
18. Si eres licenciado, no puede ser cierto que no sepas leer ni escribir: $p \rightarrow \sim (\sim q \wedge \sim r)$
19. Sólo si conoces Oviedo, podrás disfrutar a fondo leyendo La Regenta y no perderte entre sus tumultuosas páginas: $p \leftrightarrow (q \wedge \sim r)$

1.1.6 TAUTOLOGÍA, CONTRADICCIÓN E INDETERMINACIÓN

Al hacer la tabla de verdad de cualquier fórmula nos podemos encontrar con tres casos: que la tabla de verdad de la fórmula sólo tenga 1, que sólo tenga 0, y que tenga 1 y 0.

TAUTOLOGÍA:

Definición 1.4
Es una fórmula siempre válida, sean cuales sean los valores de verdad de las proposiciones que la integran. Es decir, es una fórmula cuya tabla de verdad final sólo tiene unos (1).

CONTRADICCIÓN:

Definición 1.5
Es una fórmula no válida nunca, sean cuales sean los valores de verdad de las proposiciones que la integran. Es decir, es una fórmula cuya tabla de verdad final sólo tiene ceros (0).

INDETERMINACIÓN O CONTINGENCIA:

Definición 1.6
Es una fórmula que puede ser válida o no, en función de los valores de verdad de las proposiciones que la integran. Es decir, es una fórmula cuya tabla de verdad final tiene unos (1) y ceros (0) no importa en qué proporción.

Ejemplo 1.6

CONTRADICCIÓN $p \wedge \sim p$ Se lee p y no p

p	$\sim p$	$p \wedge \sim p$
1	0	**0**
0	1	**0**

Cuadro 1.1: ejemplo de *Contradicción*

Ejemplo 1.7

$(p \rightarrow q) \wedge \sim (p \rightarrow q)$ Se lee Si, entonces q, y no es cierto que si p, entonces q.

$(p$	$\rightarrow$	$q)$	$\wedge$	$\sim$	$(p$	$\rightarrow$	$q)$
1	1	1	**0**	0	1	1	1
1	0	0	**0**	1	1	0	0
0	1	1	**0**	0	0	1	1
0	1	0	**0**	0	0	1	0

Cuadro 1.2: ejemplo de *Contradicción*

Ejemplo 1.8

TAUTOLOGÍA $p \vee \sim p$ Se lee p o no q

p	$\sim p$	$p \vee \sim p$
1	0	**1**
0	1	**1**

Cuadro 1.3: ejemplo de *Tautología*

Ejemplo 1.9

$p \rightarrow (p \vee q)$ Se lee Si p, entonces p o q.

p	$\rightarrow$	$(p$	$\vee$	$q)$
1	**1**	1	1	1
1	**1**	1	1	0
0	**1**	0	1	1
0	**1**	0	0	0

Cuadro 1.4: ejemplo de *Tautología*

Ejemplo 1.10

INDETERMINACIÓN $p \rightarrow \sim (p \vee q)$ Se lee: *Si p, entonces no es cierto que p o q.*

p	$\rightarrow$	$\sim$	$(p$	$\vee$	$q)$
1	**0**	0	1	1	1
1	**0**	0	1	1	0
0	**1**	0	0	1	1
0	**1**	1	0	0	0

Cuadro 1.5: ejemplo de *Indeterminación*

1.1.7 LEYES DE LA LÓGICA PROPOSICIONAL

Las fórmulas que son tautologías constituyen esquemas válidos de inferencia o razonamientos formalmente válidos, y son llamadas por ello leyes lógicas.

PRINCIPIOS

A las llamadas leyes lógicas hay que anteponerles tres Principios básicos y fundamentales del pensar humano:los principios de la Lógica.

1. Principio de identidad:$p \rightarrow p$
2. Principio de no contradicción: $\sim (p \wedge \sim p)$
3. Principio de tercio excluso (tertium non datur): $p \vee \sim p$

LEYES

1. Ley de la Doble Negación: $\sim\sim p \leftrightarrow p$
2. Leyes de la Simplificación: $(p \wedge q) \rightarrow p$
3. Leyes de la idempotencia: $(p \wedge p) \rightarrow p$, $(p \vee p) \rightarrow p$
4. Ley de la adición: $p \rightarrow (p \vee q)$
5. Leyes del silogismo disyuntivo: $[(p \wedge q) \wedge \sim q] \rightarrow p$ $[(p \wedge q) \wedge \sim p] \rightarrow q$

6. Leyes de De Morgan: $\sim (p \wedge q) \rightarrow (\sim p \vee \sim q), (p \vee q) \rightarrow (\sim p \wedge \sim q)$
7. Ley del Modus Ponendo Ponens: $[(p \rightarrow q) \wedge p] \rightarrow q$
8. Ley del Modus Tollendo Tollens: $[(p \rightarrow q) \wedge \sim q] \rightarrow \sim p$
9. Ley de la Transitividad del Condicional: $[(p \rightarrow q) \wedge (q \rightarrow r)] \rightarrow (p \rightarrow r)$
10. Leyes del Bicondicional:

$$(p \leftrightarrow q) \rightarrow (p \rightarrow q)$$

$$(p \leftrightarrow q) \rightarrow (q \rightarrow p)$$

$$(p \leftrightarrow q) \leftrightarrow [(p \rightarrow q) \wedge (q \rightarrow p)]$$

11. Leyes Conmutativas:
    - Del conjuntor: $(p \wedge q) \leftrightarrow (q \wedge p)$
    - Del disyuntor: $(p \vee q) \leftrightarrow (q \vee p)$
    - Del bicondicional: $(p \leftrightarrow q) \leftrightarrow (q \leftrightarrow p)$
12. Leyes asociativas:
    - $[(p \wedge q) \wedge r] \leftrightarrow [p \wedge (q \wedge r)]$
    - $[(p \vee q) \vee r] \leftrightarrow [p \vee (q \vee r)]$

1.2 Práctico 1

Ejercicios 1.1 Simboliza las siguientes proposiciones.

1.1 No vi la película, pero leí la novela.

1.2 Ni vi la película ni leí la novela.

1.3 No es cierto que viese la película y leyese la novela.

1.4 Vi la película aunque no leí la novela.

1.5 No me gusta trasnochar ni madrugar.

1.6 O tu estás equivocado o es falsa la noticia que has leído.

1.7 Si no estuvieras loca, no habrías venido aquí.

1.8 Llueve y o bien nieva o sopla el viento

1.9 O está lloviendo y nevando o está soplando el viento.

1.10 Si hay verdadera democracia, entonces no hay detenciones arbitrarias ni otras violaciones de los derechos civiles.

1.11 Roberto hará el doctorado cuando y solamente cuando obtenga la licenciatura.

1.12 Si viene en tren, llegará antes de las seis. Si viene en coche, llegará antes de las seis. Luego, tanto si viene en tren como si viene en coche, llegará antes de las seis.

1.13 Si un triángulo tiene tres ángulos, un cuadrado tiene cuatro ángulos rectos,Un triángulo tiene tres ángulos y su suma vale dos ángulos rectos. Si los rombos tienen cuatro ángulos rectos, los cuadrados no tienen cuatro ángulos rectos. Por tanto los rombos no tienen cuatro ángulos rectos.
p: un triángulo tiene tres ángulos
q: un cuadrado tiene cuatro ángulos rectos
r: su suma vale dos ángulos rectos
s: los rombos tienen cuatro ángulos rectos

1.14 Si no es cierto que se puede ser rico y dichoso a la vez, entonces la vida está llena de frustraciones y no es un camino de rosas.Si se es feliz, no se puede tener todo. Por consiguiente, la vida está llena de frustraciones.
p: se puede ser rico
q: se puede ser dichoso
r: la vida está llena de frustraciones
s: es un camino de rosas

1.15 La vida no tiene cosas así de fuertes o yo te puedo contar cómo es una llama por dentro. Si yo te puedo contar cómo es una llama por dentro, entonces pienso entregarte mi tiempo y pienso entregarte mi fe. No es cierto que piense entregarte mi tiempo y piense entregarte mi fe. Por lo tanto, la vida no tiene cosas así de fuertes.
p: tener la vida cosas así de fuertes.
q: contar cómo es una llama por dentro
r: entregarte mi tiempo
s: entregarte mi fe

2 — TEORÍA DE CONJUNTOS

2.0.1 NOCIONES PRIMITIVAS

Consideraremos tres nociones primitivas: Conjunto, Elemento y Pertenencia.

Conjunto

Podemos entender al conjunto como, colección, grupo de objetos o cosas. Por ejemplo, el conjunto formado por los *objetos* 1, a, casa. Denotaremos a los conjuntos con letras mayúsculas A, B, etc., así, A es el conjunto formado por los elementos: 1, a, casa.

Elemento

Un elemento es cualquier objeto o cosa en el conjunto. Los denotamos con letras minúsculas y al elemento genérico lo denotamos x.

Pertenencia

Denotado por el símbolo $\in$, relaciona las dos nociones primitivas anteriores. Si el elemento 1 está en el conjunto, anotamos: $1 \in A$ y se lee: *el elemento 1 pertenece al conjunto A* o simplemente *1 está en A*. Si el elemento x no pertenece al conjunto A, escribimos: $x \notin A$.

Conjuntos por extensión y por comprensión

Un conjunto está descrito por extensión cuando exhibimos a todos sus elementos encerrados en un paréntesis de llave, así por ejemplo, $A = \{2,3,4\}$. Un conjunto está descrito por comprensión cuando declaramos una propiedad que la cumplen sólo y sólo los elementos del conjunto, por ejemplo, el conjunto $A = \{2,3,4\}$ escrito por comprensión es: $A = \{x/x \in \mathbb{N}/1 < x < 5\}$.

Naturalmente también podemos anotarlo: $A = \{x/x \in N/2 \leq x \leq 4\}$, $A = \{x/x \in N/1 \leq x \leq 5\}$.

Definición 2.1

Sean A y B conjuntos, decimos que A es subconjunto de B, lo que denotamos $A \subseteq B$ si y sólo si *todos los elementos de A son también elementos de B*, es decir,

$$A \subseteq B \Leftrightarrow [\forall x : x \in A \Rightarrow x \in B] .$$

Ejemplo 2.1

Demuestre que $A \subseteq A \forall A$ (propiedad refleja)

Solución. Como $\forall A : x \in A \Rightarrow x \in A$, concluimos que $A \subseteq A$.

Ejemplo 2.2

Demuestre que $[A \subseteq B \wedge B \subseteq C] \Rightarrow A \subseteq C \forall A, B, C$ (transitividad).

Solución. $[A \subseteq B \wedge B \subseteq C] \Rightarrow [\forall x : x \in A \Rightarrow x \in B] \wedge [\forall x : x \in B \Rightarrow x \in C]$

$\Rightarrow \forall x : x \in A \Rightarrow x \in B \Rightarrow x \in C$. de donde $A \subseteq C$.

Observación. A no es subconjunto de B , lo que denotamos $A \subseteq B$ si y sólo si existe algún elemento en A que no está en B , es decir:

A no está incluido en $B \Leftrightarrow \exists x : x \in A \wedge x \notin B$.

Definición 2.2

Decimos que los conjuntos A y B son iguales, lo que denotamos $A = B$ si y sólo si *todos los elementos de A son elementos de B y todos los elementos de B son elementos de A*, es decir:

$$A = B \Leftrightarrow [\forall x : x \in A \Rightarrow x \in B] \wedge [\forall x : x \in B \Rightarrow x \in A] \Leftrightarrow A \subseteq B \wedge B \in A.$$

2.0.2 ALGUNOS CONJUNTOS IMPORTANTES

Conjunto Vacío

Sea A un conjunto, entonces $\{x/x \in A \wedge x \in A\}$ es un conjunto que no tiene elementos, lo denotamos $\emptyset A$ y es el conjunto *vacío de A*.

Proposición 2.1

$\emptyset_A \subseteq A, \forall A$

.
Demostración. La realizaremos por reducción al absurdo. Supongamos que $\emptyset A$ no es subconjunto de A, entonces $\exists x : x \in \emptyset_A \wedge x \notin A$, esto constituye una contradicción ya que el conjunto $\emptyset$ A no tiene elementos, entonces debe ocurrir que $\emptyset A \subseteq A$.

Observación. Note el uso de $[p \Rightarrow (q \wedge (\sim q))] \Rightarrow \sim p$ donde p : $\emptyset Ano \subset A$.

Proposición 2.2
$\emptyset_A = \emptyset_B, \forall A, B$

.
Demostración. Se debe demostrar que **1)** $\emptyset_A \subseteq \emptyset_B$ y **2)** $\emptyset_B \subseteq \emptyset_A$.

1) Así es, ya que si no es cierto, es decir, si $\emptyset_A$ no es subconjunto de $\emptyset_B$, debe existir al menos un elemento que pertenezca a $\emptyset_A$ y que no está en $\emptyset_B$; esto es una contradicción, por lo que $\emptyset_A \subseteq B$.

2) De manera análoga, $\emptyset_B \subseteq A$.

Por **1)** y **2)** concluimos que $\emptyset_A = \emptyset_B$.

Observación. Como todos los *vacíos* son iguales, denotamos simplemente $\emptyset$.
Conjunto Unitario

Es aquel conjunto que tiene un único elemento. Se lee como, el unitario del elemento.

Ejemplo 2.3
$A = \{x/x \in \mathbb{N}, 3 < x < 5\} = \{4\}$ se lee *el unitario del 4*.

Conjunto Universal U
Se puede demostrar que no existe un conjunto universo que contenga a todos los conjuntos (Paradoja de Russel), en cambio existe un conjunto universo de referencia, denotado U. Así por ejemplo, para los conjuntos $A = \{2,3,4\}, B = \{2,4,6,9\}$, el conjunto universal podría ser $U = \{1,2,3,4,5,6,7,8,9\}$.

2.0.3 Operaciones con conjuntos

Unión de Conjuntos

Sean A y B conjuntos en U, definimos la unión de A con B, denotada $A \cup B$ que se lee A *unión* B como el conjunto tal que

$$A \cup B = \{x/x \in A \vee x \in B\}$$

Observación.

1. En un diagrama de **Venn-Euler** tenemos

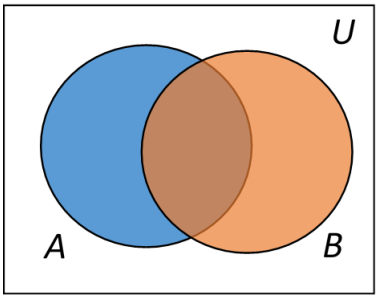


Figura 2.1: $A \cup B$

2. $x \in P \cup Q \Rightarrow x \in P \vee x \in Q$. $x \in M \vee x \in \mathbb{N} \Rightarrow x \in M \cup N$

2.0.4 Propiedades

1. $A \cup A = A, \forall A \in U$ (idempotencia)
2. $A \cup B = B \cup A, \forall A, B \in U$ (conmutatividad).
3. $(A \cup B) \cup C = A \cup (B \cup C), \forall A, B, C \in U$ (Asociatividad).
4. $A \cup \emptyset = A, A \cup U = U, \forall A \in U$.
5. $A \subseteq B \Rightarrow A \cup B = B$.

Demostración.

Propiedad 2). Se debe demostrar que: **a)** $A \cup B \subseteq B \cup A$ y **b)** $B \cup A \subseteq A \cup B$.

1. Sean $x \in A \cup B \Rightarrow$, debemos demostrar que $x \in B \cup A$

   $x \in A \cup B \Rightarrow x \in A \vee x \in B \Rightarrow x \in A \Rightarrow x \in B \cup A$

   de donde

   $$A \cup B \subseteq A \cup B.$$

2. Sea $x \in B \cup A$, debemos demostrar que $x \in A \cup B$

   $x \in B \cup A \Rightarrow x \in B \vee x \in A \Rightarrow x \in A \vee x \in B \Rightarrow x \in A \cup B$
   de donde

   $$B \cup A \subseteq A \cup B.$$

   Por **a)** y **b)** concluimos que $A \cup B = B \cup A$.

   Notemos el uso de la Tautología $p \Leftrightarrow q \vee p$.

Demostración

Propiedad 5) Se debe demostrar que **a)** $A \cup B \subseteq B$ y que **b)** $B \subseteq A \cup B$.

- Sea $x \in A \cup B$, debemos demostrar que $x \in B$, $x \in A \cup B \Rightarrow x \in A \vee x \in B$.

  Si $x \in A \Rightarrow x \subseteq B$ (por hipótesis $A \subseteq B$). Si $x \in B \Rightarrow x \in B$; esto indica que en todo caso $x \in B$, de donde

  $$A \cup B \subseteq B.$$

- Sea $x \in B \Rightarrow x \in A \vee x \in B \Rightarrow x \in A \cup B$, así $B \subseteq A \cup B$.

Por **a)** y **b)** $A \subseteq B \Rightarrow A \cup B = B$.

En la parte **b)** de la demostración usamos la tautología $p \Rightarrow q \vee p$.

2.0.5 Intersección de Conjuntos

Sean A y B conjuntos en U, definimos la intersección de A con B, denotada $A \cap B$, que se lee A *intersección* B como el conjunto tal que $A \cap B = \{x / x \in A \wedge x \in B\}$.

Observación

- En un diagrama de Venn-Euler tenemos $A \cap B$.

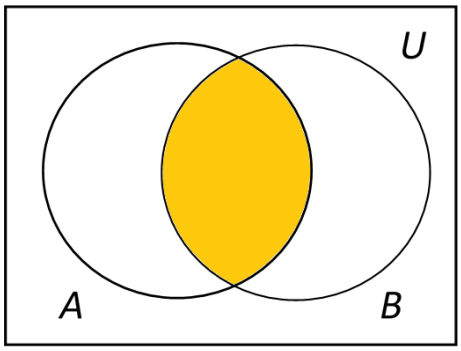


Figura 2.2: intersección $A \cap B$

- $x \in P \cap Q \Rightarrow x \in P \wedge x \in Q$.

  $x \in M \wedge x \in N \Rightarrow x \in M \cap N$.

Propiedades

1. $A \cap A = A$, $\forall A \in U$ (Idempotencia).
2. $A \cap B = B \cap A$, $\forall A, B \in U$ (Conmutatividad).
3. $(A \cap B) \cap C = A \cap (B \cap C)$, $\forall A, B, C \in U$ (Asociatividad).
4. $A \cap \emptyset = \emptyset, A \cap U = A$, $\forall A \in U$.
5. $A \subseteq B \Rightarrow A \cap B = A$.

Demostración.

3) Por demostrar que **a)** $(A\cap B)\cap C\subseteq A\cap(B\cap C)$ y **b)** $A\cap(B\cap C)\subseteq(A\cap B)\cap C$.

a) Sea $x\in(A\cap B)\cap C$, debemos demostrar que $x\in A\cap(B\cap C)$,

$x\in(A\cap B)\cap C\Rightarrow x\in(A\cap B)\wedge x\in C$
$\Rightarrow(x\in A\wedge x\in B)\wedge x\in C$
$\Rightarrow x\in A\wedge(x\in B\wedge x\in C)$
$\Rightarrow(x\in A\wedge x\in B)\wedge x\in C$
$\Rightarrow x\in(A\cap B)\wedge x\in C$
$\Rightarrow x\in(A\cap B)\cap C$.

Concluimos que $(A\cap B)\cap C\subseteq A\cap(B\cap C)$.

b) Sea $x\in A\cap(B\cap C)$, se debe demostrar que $x\in(A\cap B)\cap C$,

$x\in A\cap(B\cap C)\Rightarrow x\in A\wedge x\in(B\cap C)$
$\Rightarrow x\in A\wedge(x\in B\Rightarrow x\in C)$
$\Rightarrow(x\in A\wedge x\in B)\wedge x\in C$
$\Rightarrow x\in A\cap B\wedge x\in C$
$\Rightarrow x\in(A\cap B)\cap C$.

Concluimos que $A\cap(B\cap C)\subseteq(A\cap B)\cap C$.

Por **a)** y **b)** se deduce que $A\cap(B\cap C)=(A\cap B)\cap C$.

Propiedad 4) Debe cumplirse que $A\cap\emptyset=\emptyset$ ya que si no es así, es decir, si $A\cap\emptyset=\emptyset$ entonces existe al menos un elemento en $A\cap\emptyset$. Esto constituye una contradicción dado que el conjunto vacío no tiene elementos.

2.0.6 Diferencia de Conjuntos

Sean A y B conjuntos en U, definimos la diferencia de A con B, denotada $A-B$, que se lee A *menos* B como el conjunto tal que

$$A-B=\{x/x\in A\wedge x\notin B\}$$

Observación.

- En un diagrama de Venn-Euler tenemos

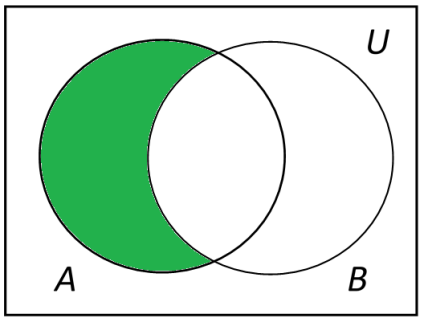


Figura 2.3: Diferencia $A-B$

- $x\in P-Q\Rightarrow x\in P\wedge x\notin Q$.

  $x\in M\wedge x\notin N\Rightarrow x\in M-N$

- En general, la diferencia no es idempotente, es decir, $A-A\neq A$. En general, la diferencia no es conmutativa, es decir, $A-B=B-A$.

2.0.7 Complemento de un Conjunto

Sea A un conjunto en U, definimos el complemento de A, denotado A^c , que se lee *complemento de* A, como el conjunto tal que

$$A^c=\{x/x\notin A\wedge x\in U\}.$$

Observación. En un diagrama de Venn-Euler tenemos

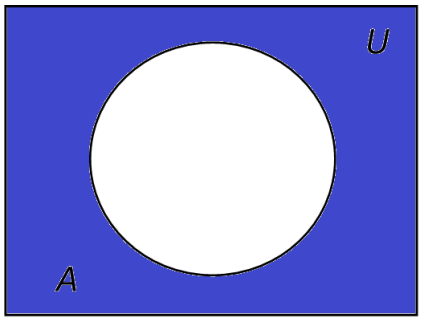


Figura 2.4: Complemento de A

Propiedades

1. $(A^c)^c = A, \forall A \in U$.
2. $U^c = \emptyset$.
3. $\emptyset^c = U$.
4. $A \subseteq B \Rightarrow B^c \subseteq A^c$.

Demostración.

1) Debemos demostrar, **a)** $(A^c)^c \subseteq A$, **b)** $A \subseteq (A^c)^c$,
a) Sea $x \in (A^c)^c$, por demostrar que $x \in A$, $x \in (A^c)^c \Rightarrow x \notin A^c \Rightarrow x \in A$,

asi, $(A^c)^c \subseteq A$.

b) Sea $x \in A$, por demostrar que $x \in (A^c)^c$, $x \in A \Rightarrow x \notin A^c \Rightarrow x \in (A^c)^c$,

asi, $A \subseteq (A^c)^c$.

Por **a)** y **b)** concluimos que $(A^c)^c = A$.

2) y **3)** son inmediatas.

4) Sea $x \in B^c$, debemos demostrar que $x \in A^c$ si $A \subseteq B$. $x \in B^c \Rightarrow x \notin B$, como $A \subseteq B$ entonces $x \notin A$de donde $x \in A^c$.

2.0.8 Propiedades Combinadas

1.
$$A - B = A \cap B^c$$

$$A \cap A^c = \emptyset$$

$$A \cup A^c = U$$

2. **Distributividades**

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

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

3. **Leyes de De Morgan**

$$(A \cup B)^c = A^c \cap B^c$$

$$(A \cap B)^c = A^c \cup B^c$$

Ejemplo 2.4

Ejemplo Usando propiedades de las operaciones de conjuntos demuestre $[(A \cap B^c)^c - (A \cup B)^c] \cup (A \cap B) = B$.

Solución.

$$[(A \cap B^c)^c - (A \cup B)^c] \cup (A \cap B) = [(A \cap B^c)^c \cap (A \cup B)] \cup (A \cap B)$$

$$= [(A^c \cup B) \cap (A \cup B)] \cup (A \cap B)$$

$$= [(A^c \cap A) \cup B] \cup (A?B)$$

$$= (\emptyset \cup B) \cup (A \cap B)$$

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

,
ya que $A \cap B \subseteq B$.

2.0.9 Cardinalidad

La Teoría de Conjuntos es la base teórica para explicar algunos fenómenos, en particular los aleatorios y allgúnos interesa contar la cantidad de elementos en un subconjunto determinado. Aceptaremos la siguiente afirmación, *si A y B son conjuntos disjuntos entonces la cantidad de elementos que tiene la unión de tales conjuntos es igual a la suma de la cantidad de elementos de los conjuntos*.

Simbólicamente, si denotamos por $n(M)$ la cantidad de elementos del conjunto M entonces $A \cap B = \emptyset$ entonces,

$$n(A \cup B) = n(A) + n(B)$$

.

Observación

Se puede demostrar (lo que queda propuesto) que: $\forall A, B \in U$,

1. $n(A \cup B) = n(A) + n(B) - n(A \cap B)$,
2. $n(A \cap B^C) = n(A) - n(A \cap B)$.

Ejemplo 2.5

En una escuela, 150 alumnos han rendido 3 exámenes. De ellos, 60 aprobaron el primero, 70 el segundo y 50 alumnos el tercer examen; 30 aprobaron los dos primeros,25 el primero y el tercero, 15 el segundo y el tercero, adem´ as, 10 alumnos aprobaron los 3 exámenes. ¿Cuántos alumnos
a) aprobaron ningún examen?, b) aprobaron sólo el primer examen?, c) aprobaron sólo dos exámenes?, d) aprobaron sólo un examen?.

Solución. Consideremos los siguientes conjuntos, A = {alumnos que aprueban el primer examen}, B = {alumnos que aprueban el segundo examen}, C = {alumnos que aprueban el tercer examen},

entonces los datos se pueden expresar como sigue:

$n(A) = 60$, $n(B) = 70$, $n(C) = 50$, $n(A \cap B) = 30$, $n(A \cap C) = 25$,

$n(B \cap C) = 15$, $n(A \cap B \cap C) = 10$,

además, $n(U) = 150$, con U = alumnos que rindieron examen.

a) Se pide $n(A^c \cap B^c \cap C^c)$ como

$$n(A^c \cap B^c \cap C^c) = n\left[(A \cup B \cup C)^c\right]$$

$$= n(U) - n(A \cup B \cup C)$$

y además

$$n(A \cup B \cup C) = n(A) + n(B) + n(C) - n(A \cap B) - n(A \cap C) - n(B \cap C) + n(A \cap B \cap C)$$
$$= 60 + 70 + 50 - 30 - 25 - 15 + 10 = 120,$$

entonces

$$n(A^c \cap B^c \cap C^c) = 150 - 120 = 30.$$

b) Se pide $n(A \cap B^c \cap C^c)$,

$$n(A \cap B^c \cap C^c) = n\left[A \cap (B \cup C)^c\right]$$
$$= n(A) - n[A \cap (B \cup C)]$$
$$= n(A) - n\left[(A \cap B) \cup (A \cap C)\right]$$
$$= n(A) - [n(A \cap B) + n(A \cap C) - n(A \cap B \cap C)] = 60 - (30 + 25 - 10) = 15.$$

c) Se pide $n\left[(A\cap B\cap C^c)\cup(A\cap C\cap B^c)\cup(B\cap C\cap A^c)\right]$,

$$\begin{aligned}&n\left[(A\cap B\cap C^c)\cup(A\cap C\cap B^c)\cup(B\cap C\cap A^c)\right]\\&=n\left[(A\cap B\cap C^c)\cup(A\cap C\cap B^c)\cup(B\cap C\cap A^c)\right]\\&=n(A\cap B\cap C^c)+n(A\cap C\cap B^c)+n(B\cap C\cap A^c)\\&\quad -n(\emptyset)-n(\emptyset)-n(\emptyset)+n(\emptyset).\end{aligned}$$

Como

$$n(A\cap B\cap C^c)=n(A\cap B)-n(A\cap B\cap C)=30-10=20,$$

análogamente obtenemos $n(A\cap C\cap B^c)=15$, $n(B\cap C\cap A^c)=5$, de donde

$$n\left[(A\cap B\cap C^c)\cup(A\cap C\cap B^c)\cup(B\cap C\cap A^c)\right]=20+15+5=40.$$

d) Se pide $n(A\cup B\cup C)$.

e) Se pide $n\left[(A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c)\cup(C\cap A^c\cap B^c)\right]$,

$$n\left[(A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c)\cup(C\cap A^c\cap B^c)\right]$$

$$=n(A\cap B^c\cap C^c)+n(B\cap A^c\cap C^c)+n(C\cap A^c\cap B^c)=-n(\emptyset)-n(\emptyset)-n(\emptyset)+n(\emptyset).$$

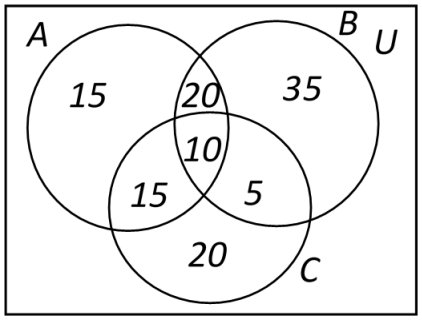
Como $n(A\cap B^c\cap C^c)=15$, (problema b)) y procediendo análogamente obtenemos

$n(B\cap A^c\cap C^c)=35$ y $n(C\cap A^c\cap B^c)=20$,

de donde

$$n\left[(A\cap B^c\cap C^c)\cup(B\cap A^c\cap C^c)\cup(C\cap A^c\cap B^c)\right]=15+35+20=70.$$

Observación. Usando un diagrama de Venn-Euler podemos solucionar el problema planteado



El diagrama se construyó, iniciando el *llenado* desde el centro, es decir, desde $n(A\cap B\cap C)$. Notemos que se puede leer inmediatamente que $n(B\cap A^c\cap B^c)=35$.

2.1 Práctico 2

Ejercicios 2.1

2.50 Sean $U=\{1,2,3,4,5,6,7,a,b,c,d,e,f,g,h\}$, $A=\{3,5,7,c,d\}$, $B=\{2,3,4,5,b,c,e\}$, $C=\{2,6,7,a,b,g\}$.

Determine

a) $(A\cup B^c)\cap(C-A)^c$.
b) $(A\cap C)\cup(B-A^c)^c$.
c) Las operaciones para obtener
   I. $\{6,2,b\}$
   II. $\{7\}$
   III. $\{3,4,5,c,d,e\}$

2.51 Demuestre

a) $A-B=A\cap B^c$.
b) $A\cap(B\cup C)=(A\cap B)\cup(A\cap C)$.
c) $(A\cap B)^c=A^c\cup B^c$.

2.52 Usando Algebra de Conjuntos, verifique si

1. $(A-B)\cup(A-B^c)=A$.
2. $B\cap[(B^c\cup A^c)\cup(A\cup B)^c]=B-A$.
3. $[(A\cap B)\cup(A^c\cap B)\cup(A^c\cap B^c)]=A^c\cup B$.
4. $A-\{A-[(A-B)\cup A]\}=A$.
5. $[A-(A\cap B)]\cap[B-(A\cap B)]=\emptyset$.
6. $A-B=A-(A\cap B)$
7. $(A\cup B)-C=(A-C)\cup(B-C)$
8. $(A\cap B)-C=(A-C)\cap(B-C)$
9. $(A-B)-C=A-(B\cup C)$
10. $A-(B-C)=(A-B)\cup(A\cap C)$
11. $(A-B)-C\subset A-(B-C)$

12. $A \cup (B - C) = (A \cup B) - (C - A)$

2.53 En un universo de 30 elementos se consideran dos conjuntos, A y B tales que $n(A \cap B) = 10$, $n(B) = 18$,$n(B^c \cap A) = 5$.

Determine

a) $n(B - A)$.

b) $n(A)$.

c) $n(A^C \cap B^C)$.

2.54 Demuestre que

a) $n(A \Delta B) = n(A) + n(B) - 2n(A \cap B)$.
b) $n((A \Delta B) \cup C) = n(A) + n(B) + n(C) - n(A \cap C) - n(B \cap C) - 2n(A \cap B) + 2n(A \cap B \cap C)$.

2.55 En un universo U se consideran tres conjuntos A, B, C tales que $A \cap C = \emptyset$, $n(A \cap B) = 5$, $n(A^c) = 25$, $n(C) = 13$, $n(B - A) = 15$, $n(B \cap C) = 9$, $n(A \cup B \cup C) = 27$

Determine

a) $n(B)$.

b) $n(A)$.

c) $n(U)$.

2.56 En un universo de 45 elementos se consideran tres conjuntos A , B , C tales que $A \cap C = \emptyset$, $B \cap C = \emptyset$,$n(A \cap B) = 4$, $n(C - B) = 10$ $n[(A \cup B \cup C)^c] = 16$, $n(B - C) = 12$.

Calcule

a) $n(A)$.

b) $n(B)$.

c) $n(B - A)$.

d) $n[(B - A) - C]$.

2.57 Una encuesta acerca de las preferencias de 180 personas sobre tres marcas A, B, C arrojó los siguientes resultados $n[(B \cap C) - A] = 25$, $n(A \cap B) = 15$, $n[((A \cap B) - C)^c] = 175$,

$n(A-B)=50$, $n[C-(A\cup B)]=35$, $n[(A\cap C)-B]=20$, $n[(A\cup B\cup C)^c]=40$.

Determine el número de personas que

a) compran sólo B.

b) compran sólo dos marcas.

c) no compran de las marcas consultadas.

2.58 Se encuestó a 100 personas sobre sus preferencias televisivas en relación a los canales A y B. Los resultados fueron: 65 no ven el canal A, 45 no ven el canal B y 50 de ellos ven el canal A o B pero no ambos. Determine la cantidad de encuestados que ven ambos canales.

3 — INDUCCIÓN MATEMÁTICA

3.1 INTRODUCCIÓN

El método deductivo, muy usado en matemática, obedece a la siguiente idea: A partir de un cierto conjuntos de axiomas aceptados sin demostración y de reglas lógicas no contradictorias, se deducen otros enunciados llamados teoremas combinando los axiomas y respetando en cada etapa las reglas lógicas. Otro método para demostrar resultados generales que dependen en algún sentido de los números naturales es conocido con el nombre de *Inducción Matemética*. Esta dependencia de los números naturales significa: se sabe que una determinada afirmación es verdadera para algunos casos particulares y surge la pregunta. ¿ Dicha afirmación sigue siendo verdadera para los infinitos números naturales restante ?. Existen muchas afirmaciones que sólo son válidas para un número finito de casos y en consecuencia son falsas para un número infinitos de situaciones. Sin embargo, podemos encontrar proposiciones (afirmaciones) que son verdaderas sólo a partir de un cierto número natural n_0 , de ser asi, la técnica que se desarrollaremos se llama Inducción Incompleta. Para demostrar que una proposición $p(n)$, $\forall n \in M \subseteq N$, es verdadera es necesario comprobar la validez de ella para todos los elementos del conjunto M. En el caso en que $M = N$, diremos que es una Inducción Completa. Si se requiere demostrar la falsedad de una cierta proposición $p(n)$, $\forall n \in M \subseteq N$, es suficiente indicar un elemento particular $m \in M$ de manera que $p(m)$ sea falsa. (Construcción de un contra ejemplo).

Ejemplo 3.1

Encontrar los valores de $n \in N$,tal que : $n^2 - 3n - 1 < 0$

Es fácil probar que esta desigualdad es verdadera para $n = 1, 2, 3$. Sin embargo, para $n = 4$ no se cumple ya que $4^2 - 34 - 1 = 3 > 0$. Nótese que este ejemplo sencillo muestra que una proposición puede ser verdadera para los primeros números naturales, sin embargo, es **falsa** , para números naturales más grandes.

Otros ejemplos:

Ejemplo 3.2

$\forall n \in \mathbb{N}$, $(2n-1)(2n+1)(2n+3)$, es divisible por 5.

Es fácil probar que esta proposición es verdadera para $n = 1,2,3$. Sin embargo, para $n = 4$ no se cumple dado que $(24-1)(24+1)(24+3) = 693$. no es divisible por 5

Ejemplo 3.3

Ejemplo dado por Leonhard Euler (1707-1783)
Consideremos el polinomio cuadrático $p(n) = n^2 + n + 41$ y determinemos su valor para ciertos $n \in \mathbb{N}$.

n :	1	2	3	4	5	6	7	8
n^2+n+41:	43	47	53	61	71	83	97	113

Nótese que todos los números que se obtienen son primos. Se podría esperar que este polinomio cuadrático continua generando números primos. Desafortunadamente no es asi, para $n = 40$, se tiene $1681 = 41^2$, que no es un número primo, luego la proposición que $\forall n \in N$, $n^2 + n + 41$ es un número primo resulta falsa.

3.2 Principio de inducción Matemática

Una proposición $p(n)$ es verdadera para todos los valores de la variable n si se cumplen las siguientes condiciones :

1. Paso:
   La proposición $p(n)$ es verdadera para $n = 1$, o bien, $p(1)$ es verdadera.
2. Paso:
   Hipótesis de Inducción . Se supone que $p(k)$ es verdadera , donde k es un número natural cualesquiera.
3. Paso:
   Tésis de Inducción. Se demuestra que $p(k+1)$ es verdadera, o bien, $p(k)$ verdadera $\Rightarrow p(k+1)$ verdadera. La técnica de Inducción Matemática consiste en los tres pasos anteriores. Si se necesita demostrar la validez de una proposición $p(n)$ para todos los valores naturales n, entonces es suficiente que se cumplan: Paso 1, Paso 2 y Paso 3 .

Comentario

Intuitivamente la idea anterior se conoce con el nombre de **Efecto Dominó**. Si imaginamos una fila infinita de fichas de dominó: dispuestas verticalmente y suficientemente próximas una cualquiera de la siguiente , entonces si el volteamiento de la primera ficha provoca el volteamiento de la segunda ficha, por el Principio de Inducción Matemática la fila completa es volteada.

Existen dos variantes útiles sobre el Principio de Inducción Matemática que deben ser considerados . En la primera variante, la proposición por demostrar involucra los naturales no menores a un natural fijo n_0 , en este caso el Principio de Inducción quedaria como sigue:

Si $p(n)$ es verdadera para n_0 y si $p(m+1)$ es verdadera para todo natural $m \geq n_0$

para la cual $p(m)$ es verdadera, entonces $p(n)$ es verdadera para todo natural $n \geq n_0$

La segunda variante se aplica de preferencia en el caso cuando $p(m+1)$ no puede ser fácilmente deducible de $p(m)$, pero su validez depende de $p(k)$ para cualquier $k < m$. Si $p(1)$ es verdadera y si $p(m+1)$ es verdadera para todo m?1 para la cual todas las proposiciones $p(1)$,$p(2)$,$p(3)$,...,$p(m)$ son verdaderas , entonces $p(n)$ es verdadera para $n \geq 1$. Para ilustrar el uso de estas variantes, consideremos los siguientes ejemplos.

Ejemplo 3.4

Determine para que valores de $n \in N$ es verdadera la desigualdad $2^n > n^2 + 4n + 5$,Al examinar los valores de $n = 1,2,3,4,5,6$ nos damos cuenta que la desigualdad es incorrecta, pero si es verdadera para $n = 7$, por lo que podemos intentar demostrar por el método de Induccion Incompleta que para todos los valores de $n \geq 7$, la desigualdad es verdadera.

1. Paso:
   Si $n = 7$, obtenemos $2^7 = 128 > 7^2 + 47 + 5 = 82$,

   o sea, cuando $n = 7$ la desigualdad es correcta.
2. Paso:
   (Hipótesis Inductiva) Se supone que la desigualdad es verdadera para un cierto valor de $n = k$, o sea, $2^k > k^2 + 4k + 5$.
3. Paso:
   Finalmente a partir de la hipótesis inductiva, se desea probar la Tesis dada por $2^{(k+1)} > (k+1)^2 + 4(k+1) + 5$.

Al multiplicar la desigualdad dada en la hipótesis inductica por 2, obtenemos $2^{(k+1)} > 2k^2 + 8k + 10$

Transformando el segundo miembro de esta desigualdad obtenemos $2^{(k+1)} > (k+1)^2 + 4(k+1) + 5 + k^2 + 2k$

Teniendo en cuenta que $k^2 + 2k > 0$ para todo $k \geq 7$, podemos deducir que $2^{(k+1)} > (k+1)^2 + 4(k+1) + 5$, obteniendo lo que se requeria demostrar (Tesis).

Ejemplo 3.5

Demostrar que la suma de los n primeros números naturales es igual a $\frac{n(n+1)}{2}$.

Demostración:

Queremos probar que $\forall n \in N : 1+2+3+4+...+n = \frac{n(n+1)}{2}$ Sea $p(n) : 1+2+3+4+...+n = \frac{n(n+1)}{2}$, debemos probar que $p(n)$ satisface las propiedades (1), (2) y (3).

Paso 1): $p(1) : 1 = \frac{1(1+1)}{2}$, lo cual es verdadero.

Paso 2): Se supone que la igualdad es verdadera para un cierto valor de k, es decir,

$$1+2+3+4+...+k = \frac{k(k+1)}{2}$$

Paso 3) Sea $k \in N$, debemos probar que $p(k) \Rightarrow p(k+1)$ es verdadero. Notese que si $p(k)$ es falsa la implicación es verdadera, de modo que hay que hacer la demostración suponiendo que $p(k)$ es verdadera. Como $p(k+1) : 1+2+3+...+k+(k+1) = \frac{(k+1)((k+1)+1)}{2}$, $p(k+1)$ debe formarse de $p(k)$ sumando $k+1$ a ambos mienbros de la igualdad (de la Hipótesis inductiva):

$$1+2+3+...+k+(k+1) = \frac{k(k+1)}{2} + (k+1) = (k+1)\left(\frac{k}{2}+1\right) = \frac{(k+1)(k+2)}{2}.$$

Hemos confirmado nuestras sospechas, lo que es, hemos deducido que $p(k+1)$ es verdadera, suponiendo que $p(k)$ lo es. Así, hemos demostrado que $\forall n \in N : 1+2+3+4+...+n = n\frac{(n+1)}{2}$ es verdadera.

Ejemplo 3.6

Probar que $\forall n \in N : 1\cdot 3+2\cdot 4+3\cdot 5+...+n(n+2) = \frac{n(n+1)(2n+7)}{6}$

Solución: Sea $p(n) : 1\cdot 3+2\cdot 4+3\cdot 5+...+n(n+2) = \frac{n(n+1)(2n+7)}{6}$

Entonces $p(1) : 1\cdot 3 = \frac{1(1+1)(2\cdot 1+7)}{6} = 2\cdot\frac{9}{6} = 3$, lo que prueba que $p(1)$ es verdadera.

Hipótesis inductiva:

$1\cdot 3+2\cdot 4+3\cdot 5+ ... + k(k+2) = \frac{k(k+1)(2k+7)}{6}$. (Suponemos que $p(n)$ es verdadera)

Tesis: $1\cdot 3+2\cdot 4+3\cdot 5+ ... +k(k+2)+(k+1)(k+3) = \frac{(k+1)(k+2)(2k+9)}{6}$.(Queremos probar que $p(k+1)$ es verdadera) Tenemos:

$$1\cdot 3+2\cdot 4+3\cdot 5+...+k(k+2)+(k+1)(k+3)=\frac{k(k+1)(2k+7)}{6}+(k+1)(k+3)=$$

$$=\frac{(k+1)}{6}(k(2k+7)+6(k+3))=$$

$$=\frac{(k+1)(2k^2+13k+18)}{6}=\frac{(k+1)(2k+9)(k+2)}{6}$$

lo que prueba que p(k +1) es verdadera. Luego, la formula $1\cdot 3+2\cdot 4+3\cdot 5+\ ...+n(n+2)$

$=\frac{n(n+1)(2n+7)}{6}$es verdadera para todo $n\in N$.

Ejemplo 3.7

Determinar si el producto de 3 números impares consecutivos es siempre divisible por 6.

Solución: Sea $p(n):(2n-1)(2n+1)(2n+3)=6q$ donde q es algún número natural . Queremos determinar si p(n) se cumple para todo $n\in N$.

$p(1):1\cdot 3\cdot 5=15=6q\Rightarrow q=\frac{5}{2}\notin\mathbb{N}$. Luego $p(1)$ es falso. Se puede continuar analizando $p(2)$,$p(3)$,$p(4)$,... y vemos que todos no cumplen la condición que sea divisible por 6. Es facil ver que $(2n-1)(2n+1)(2n+3)=8n^3+12n^2-2n-3=2(4n^3+6n^2-n-1)-1$ luego este número es de la forma $2j-1$ que es un número impar y por lo tanto no es divisible por 6.

3.3 Práctico 3

Ejercicios 3.1

3.1 Determine si la suma de tres números enteros consecutivos es siempre divisible por 6.

3.2 Consideremos un ejemplo con desigualdades. Determine todos los números naturales para los cuales: $1 \cdot 2 \cdot 3 \cdot 4 \cdots n > 2^n$

3.3 Demostrar por inducción, que si n es un número impar, $7^n + 1$ es divisible por 8.

3.4 Pruebe que la fórmula

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

es válida para todo natural n.

3.5 Pruebe que para todo número natural $n > 1$, el último dígito del número $2^{2^n} + 1$ es 7.

3.6 Demuestre que para todo natural $n \geq 2$,

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

3.7 Demuestre que para todo natural n, $n^5 - n$ es divisible por 5.

Demuestre por inducción las siguientes igualdades:

3.8

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

3.9

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

3.10

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

4 — Teoría de Números

4.1 Números Enteros

$\mathbb{Z} = N \cup 0 \cup (-\mathbb{N})$

Definición 4.1 Valor Absoluto (| |)

$$|a| = \begin{cases} a & si \quad a \geq 0 \\ -a & si \quad a < 0 \end{cases}$$

4.1.1 Propiedades

1. $|a| \geq 0$
2. $|a| = |-a|$
3. $-|a| \leq a \leq |a|$
4. $|a| + a \geq 0$
5. $|a| - a \geq 0$
6. $|a+b| \leq |a| + |b|$
7. $|a \cdot b| = |a| \cdot |b|$
8. $|a-b| \geq |a| - |b|$

Demostración 8:

$|a| = |(a-b)+b|$ por el inverso aditivo y asociativa.
$|a| \leq |a-b| + |b|$ prop. 6

$\Rightarrow |a| \leq |a-b| + |b|$

$\Rightarrow |a| - |b| \leq |a - b|$

$|a - b| \geq |a| - |b|$

axioma 4.1

I. $a \cdot 0 = 0$
II. $0.b = 0 \Leftrightarrow a = 0 \vee b = 0$
III. $a \cdot b = a \cdot c \wedge a \neq 0 \Rightarrow b = c$
IV. $a \cdot b = 1 \Rightarrow a = b = 1 \veebar a = b = -1$

4.2 Divisibilidad

Definición 4.2

Divisibilidad: Sean $a \in \mathbb{Z} \neq 0 \wedge b \in \mathbb{Z}$, decimos $a|b$ sii $\exists k \in \mathbb{Z} / b = a \cdot k$.

Ejemplo: $3|0$? si , pues $\exists 0 \in \mathbb{Z} / 0 = 3 \cdot 0$

Observación

Sólo si $a|b$ escribimos $\frac{a}{b} = k$

Teorema 4.1 (Divisibildad)

Sean $a, b, d, p, q \in \mathbb{Z}$.

1. $a \neq 0 \Rightarrow a|a$ (propiedad reflexiva)
2. $a|b \wedge b|a \Rightarrow |a| = |b|$
3. $a|b \wedge b|c \Rightarrow a|c$
4. Si $d|a$ y $d|b$ entonces $d|(ax + by)$ para cualquier $x, y \in \mathbb{Z}$
5. Si $d|(p+q)$ y $d|p \implies d|q$.
6. Si $a, b \in \mathbb{Z}^+$ y $b|a \implies a \geq b$
7. Si $a|b$, entonces $a|mb$, con $m \in \mathbb{Z}$.
8. Si $a, b \in \mathbb{Z}$, $a|b$ y $b|a \implies |a| = |b|$
9. Si $a \neq 0 \Rightarrow a|a \cdot c$
10. $a \neq 0 \Rightarrow a|a^n$
11. $a|b \Rightarrow a|b^n$
12. $a|b \Rightarrow a \cdot c|b \cdot c$

Demostración 1:

Si $a|a \Rightarrow \exists 1 \in \mathbb{Z} \qquad a = a \cdot 1$

Demostración 2:

$$\left.\begin{array}{ll} a|b \Rightarrow & b = a\cdot k (k\in\mathbb{Z}) \\ b|a \Rightarrow & a = b.k' (k'\in\mathbb{Z}) \end{array}\right\}$$
$\Rightarrow b = b\cdot(k'\cdot k)$

$k'\cdot k = 1$ si no $b \neq b$

$k'\cdot k = 1$ entonces $k = k' = 1 \wedge k = k' = -1$

si $k = 1$ Entonces $b = a\cdot k \Rightarrow b = a$
Si $k = -1$ entonces $b = -a \Rightarrow |b| = |a|$

Demostración 3:

$a|b \Rightarrow b|a\cdot k \qquad (k\in\mathbb{Z})$ (I)

$b|c \Rightarrow c = b\cdot k' \qquad (k'\in\mathbb{Z})$ (II)

Reemplazamos I en II, resulta: $c = a\cdot(k\cdot k')$ Asociativa

luego si $l = k\cdot k' \wedge l\in\mathbb{Z}$ por ley de cierre de multiplicación.

$\Rightarrow c = a\cdot l \Rightarrow a|c$ por def. de divisibilidad.

Proposición 4.1

La relación de divisibilidad no depende del signo.

$a|b \Leftrightarrow a|-b \Leftrightarrow -a|-b \Leftrightarrow a||b| \Leftrightarrow |a||b|$

4.2.1 Conjunto de divisores

Definición 4.3

$$D(b) = \{a\in\mathbb{Z}_{\neq 0}/a|b\}$$

$D^+(b) = D(b)\cap\mathbb{N}$ $\qquad$ $D^-(b) = D(b)\cap(-\mathbb{N})$

Proposición 4.2

$b\neq 0 \qquad \{-1,1,b,-b\}$

Proposición 4.3

Si $b \neq 0$ el mínimo de divisores positivos está acotado por su valor absoluto.

$b \neq 0 \qquad \#(D^+(b)) \leq |b|$

Corolario 4.1

I. $a|b, b \neq 0 \Rightarrow \{|a| \leq |b| \ , \ a \leq |b|\}$
II. $b \neq 0, \#(D^+(b)) < \infty$ (finito)
III. $b = 0, \#(D^+(b)) = \infty$

4.2.2 Conjuntos de Múltiplos

Definición 4.4 Conjuntos de Múltiplos

$M(a) = \{a \cdot q / q \in \mathbb{Z}\}$

$M^+(a) = M(a) \cap \mathbb{N}$ y $M^-(a) = M(a) \cap (-\mathbb{N})$

Demostración 4:

Si $d|a$ y $d|b$ entonces $d|(ax+by)$ para cualquier $x, y \in \mathbb{Z}$
$d|a \Rightarrow a = k \cdot d \ (k \in \mathbb{Z}) \quad \wedge \quad d|b \Rightarrow b = k' \cdot d$

$a \cdot x = k \cdot d \cdot x = (kx)d \quad$ y $\quad b \cdot y = k' \cdot d \cdot y = (k'y)d$,

ahora llamareamos $k'' = kx \quad$ y $\quad k''' = k'y$, luego

$a \cdot x = k \cdot d \cdot x = d(kx) \quad$ y $\quad b \cdot y = k' \cdot d \cdot y = d(k'y)$,

$a \cdot x = dk'' \quad$ y $\quad b \cdot y = dk'''$,

$ax + by = d \cdot k'' + d \cdot k''' \Rightarrow ax + by = d(k'' + k''')$

entonces por definicion de div.

y por lo tanto: $d|(ax+by)$

Apartir del teorema anterior definimos:

Definición 4.5

Combinación lineal de enteros: Sean x, a , $b \in \mathbb{Z}$ Decimos que x es una combinación lineal entera (CLE) a y b sii $\exists \lambda, \mu \in \mathbb{Z}$ / $\boxed{x = \lambda a + \mu b}$

Ejemplo 4.1

Hallar todos los n naturales tal que $n^4 + 2$ sea divisible por $n + 2$

Solución:

Aplicamos el método de Ruffini

	1	0	0	0	2
-2	↓	-2	4	-8	16
	1	-2	4	-8	18

Es decir, $\dfrac{n^4+2}{n+2} = n^3 - 2n^2 + 4n - 8 + \dfrac{18}{n+2}$

De donde $\dfrac{18}{n+2}$ debe ser entero y $n+2 \geq 3$ (pues $n \geq 1$) de los cual se obtiene que $n+2 \in \{3,6,9,18\}$ y por lo tanto, $n \in \{1,4,7,14\}$. Verificamos:

si $n = 1 \Rightarrow 1+2 | 1^4+2 \Rightarrow 3|3$

si $n = 4 \Rightarrow 4+2 | 4^4+2 \Rightarrow 6|18$

Etc...

Ejemplo 4.2

Determinar todos los $n \in \mathbb{Z}$ tales que : $3n-11 | 3n-1$.

Solución:

$3n-11 | 3n-11 \quad \wedge \quad 3n-11 | 3n-1$. por prop. reflexiva

$$3n-11 | (3n-11) - (3n-1)$$

por prop. 4

$$3n-11 | -11+1$$

Entonces,

$$3n-11|-10$$

Luego los divisores de 10 son $\rightarrow D(10)=\{\pm1,\pm2,\pm5,\pm10\}$

ahora podemos encontrar n para cada caso.

si $3n-11=1\Rightarrow n=\frac{12}{3}=4\Rightarrow \boxed{n=4}$

si $3n-11=-1\Rightarrow n=\frac{10}{3}\notin\mathbb{Z}$

si $3n-11=2\Rightarrow n=\frac{13}{3}\notin\mathbb{Z}$

si $3n-11=-2\Rightarrow n=\frac{9}{3}=3\Rightarrow \boxed{n=3}$

si $3n-11=5\Rightarrow n=\frac{16}{3}\notin\mathbb{Z}$

si $3n-11=-5\Rightarrow n=\frac{6}{3}=2\Rightarrow \boxed{n=2}$

si $3n-11=10\Rightarrow n=\frac{21}{3}=7\Rightarrow \boxed{n=7}$

si $3n-11=-10\Rightarrow n=\frac{1}{3}\notin\mathbb{Z}$

Entonces $n\in\{4,3,2,7\}$

Podemos comprobar: si $n=4\Rightarrow 3\cdot4-11|3\cdot4-1\Rightarrow 1|11$ correcto !

4.3 División Entera

Definición 4.6

Sean $a\in\mathbb{Z}\wedge b\in\mathbb{Z}-\{0\}$ $\quad\exists q,r!\in\mathbb{Z}$

$$a=b\cdot q+r \qquad 0\leq r<|b|$$

Ejemplo: $a=-15$ $\quad b=7$

$-15=7.(-2)+(-1)$ no !
$-15=7\cdot(-3)+6$ Si !

Teorema 4.2 Unicidad

$a = b \cdot q + r \qquad 0 \leq r \leq b \qquad \wedge \qquad a = b \cdot q' + r' \qquad 0 \leq r' \leq b$

Entonces $q = q' \qquad r = r'$

Demostración: **Unicidad**

$$a = a \; b \cdot q + r = b \cdot q' + r'$$
$$b \cdot q - b \cdot q' = r' - r \qquad \text{Suma de inversos aditivos}$$
$$b \cdot (q - q') = r - r' \qquad \text{factor común}$$

Luego como $(q - q') \in \mathbb{Z} \qquad \Rightarrow \qquad b | r' - r \qquad$ por def. de división

A partir de la prop. $a|b \wedge b \neq 0 \Rightarrow |a| \leq |b|$ decimos, $|b| < |r - r'|$

Primero probemos que $|r - r'| < b$

Esto es equivalente a demostrar $-b < r' - r < b$

Primero: $-b < r' - r$

$r < b \qquad$ hipótesis
$-b < -r \qquad$ multiplicamos por (-1).

$$\begin{array}{rcll} 0 & \leq & r' & \text{(por hip)} \\ -r & \leq & -r & \\ \hline -r & \leq & r' - r & \end{array}$$

Entonces $-b < -r < r' - r$ y por transitividad en la relación de orden.

Luego $\boxed{-b < r' - r}$ quedó probado

Ahora probemos $r' - r < b$
$0 \leq r$ entonces

$$\begin{array}{rcl} -r & \leq & 0 \\ -r' & \leq & -r' \\ \hline -r' - r & \leq & -r' \end{array}$$

$-r' - r \leq r'$ y Además $\qquad r' < b \qquad$ por Hip.

Resulta $r' - r < b \qquad$ por prop. transitiva

Por lo tanto: $|r'-r| < b$
ahora $b|r'-r \qquad |b| \leq |r'-r|$ pensar que $r'-r \neq 0$ es Absurdo ya que no es cierto que $b \leq 0$
por lo tanto $\boxed{r = r'}$

Retomamos la fórmula

$$b \cdot (q-q') = r - r' = 0 \qquad \Rightarrow \boxed{q = q'}$$

4.4 Números Primos

Definición 4.7
Si un número natural $p > 1$ sólo tiene como divisores a 1 y p, entonces se dice que es primo.
La sucesión de los primeros números primos comienza así:$2,3,5,7,11,13,17,23,\cdots$

Los números $n > 1$ que no son primos se llaman compuestos. El 1 es especial: no es ni primo ni compuesto, es simplemente la unidad. La importancia de los números primos consiste en que cualquier número natural $n > 1$ es primo o puede expresarse como producto de primos. En símbolos, $n = {p_1}^{a_1} {p_2}^{a_2} {p_3}^{a_3} \ldots p_k^{a_k}$
donde $p_1 < p_2 < \ < p_k$ son números primos y los exponentes $a_1, a_2, \ldots, a_k$ son números naturales. Más aún, esta descomposición es única excepto por el orden de los factores. De esta manera los números primos son como los bloques fundamentales que permiten generar, multiplicativamente, a todos los números naturales (del mismo modo que el 1 los genera aditivamente). Este resultado es tan importante que se conoce como Teorema Fundamental de la Aritmética, y fue probado por Euclides ($\approx$ 325 - 265 a.C.), quien dedicó el Libro IX de sus famosos Elementos a la Teoría de números. Euclides probó también (Proposición 20 del Libro IX) que existen infinitos números primos o, para ser más fieles a su manera de pensar, que los números primos son más que cualquier cantidad finita. En efecto, dado cualquier conjunto finito de números primos diferentes
$p_1, p_2, \ldots, p_k$ considere el número $N = p_1 p_2 p_{k+1}$. Como N no es divisible por ningún p_i , en su descomposición en factores primos debe aparecer por lo menos un primo q tal que $q \notin p_1, p_2, \ldots, p_k$. Por lo tanto, ningún conjunto finito de números primos los contiene a todos. Si $n = p_1 p_2 p_k$ entonces sus divisores son todos los números de la forma

$$ {p_1}^{b_1} {p_2}^{b_2} {p_3}^{b_3} \ldots p_k^{b_k} $$

donde $0 \leq b_i \leq a_i$. Por ejemplo los divisores de $24 = 2^3 \cdot 3^1$ son $2^0 \cdot 3^0 = 1 \quad , 2^1 \cdot 3^0 = 2 \quad , 2^2 \cdot 3^0 = 4, \quad 2^3 \cdot 3^0 = 8, \quad 2^0 \cdot 3^1 = 3, \quad 2^1 \cdot 3^1 = 6, \quad 2^2 \cdot 3^1 = 12$ y $2^3 \cdot 3^1 = 24$. Una consecuencia de lo anterior es que el número de divisores de n (incluyendo al 1 y al propio n) es

$$\boxed{(a_1+1)(a_2+1)(a_k+1)}.$$

En efecto, para formar un divisor el exponente de$p_1$puede escogerse de a_1+1 maneras, a saber 0,1,2,...,a_1 . De la misma manera, el exponente dep_2 puede escogerse de a_2+1 maneras y así sucesivamente hasta el exponente de p_k que puede escogerse de a_k+1 maneras.
Otra consecuencia del Teorema Fundamental es que un número natural es un cuadrado perfecto si y sólo si todos sus factores primos diferentes aparecen elevados a exponentes pares. Más en general, un número natural es una potencia k-sima si y sólo si todos sus factores primos diferentes aparecen elevados a exponentes múltiplos de k.

4.5 Máximo común divisor

Definición 4.8
El máximo común divisor de dos números naturales a y b es el mayor de sus divisores comunes y se denota $mcd(a,b)$. El mcd tiene las siguientes

4.5.1 Propiedades:

1. $mcd(a,1)=1$,
2. $mcd(a,b)=mcd(b,a)$,
3. $mcd(a,b)=a$si y sólo si $a|b$,
4. Si $a>b$, entonces $mcd(a,b)=mcd(a-b,b)$,
5. Si $a=qb+r$, entonces $mcd(a,b)=mcd(b,r)$.
6. Si se conoce la descomposición en producto de factores primos de a y de b, entonces es muy fácil calcular $mcd(a,b)$: es igual al producto de los factores

primos comunes elevados al menor de los exponentes con que aparecen en las descomposiciones de a y b. De aquí se deduce que $mcd(a,b)$ no sólo es el mayor divisor común sino que además cualquier otro divisor común de a y b divide a mcd(a,b). por ejemplo $406=2\cdot 7\cdot 29$ y $147=3\cdot 7^2$, por lo tanto $mcd(406,147)=7$. El $mcd(a,b)$ también se puede obtener aplicando el algoritmo de Euclides:

escribamos $a=bq+r \quad$ con $0\leq r<b$. Si $r=0$ entonces $b|a$ y $\quad mcd(a,b)=b$. Si $r\neq 0$, entonces $mcd(a,b)=mcd(bq+r,b)=mcd(r,b)$ y el problema se reduce a calcular $mcd(b,r)$. Prosiguiendo de esta manera eventualmente se obtiene el resultado.

Ejemplo 4.3
Hallar mcd(3127,2491) mediante el algoritmo de Euclides.

Solución

$$3127=2491+636$$

$$2491=3\cdot 636+583$$

$$636=583+53$$

$$583=5\cdot 53$$

y por lo tanto $mcd(3127,2491) = 53$. es interesante hacer los cálculos por descomposición en producto de factores primos y comparar el trabajo realizado.
Del algoritmo de Euclides se sigue que mcd(a,b) se puede expresar en la forma $sa+tb$ para ciertos enteros s y t (esto se conoce como **Teorema de bezout**). Por ejemplo, aprovechando los cálculos que acabamos de hacer se tiene

$$mcd(3127,2491) = 53 = 636 - 583 = 636 - (2491 - 3 \cdot 636)$$
$$= 4 \cdot 636 - 2491 = 4(3127 - 2491)?2491 = 4 \cdot 3127 - 5 \cdot 2491$$

.
Una consecuencia importante de esta manera de expresar el máximo común divisor es el **Lema de Euclides**.

Lema 4.1 Si $a|bc$ y $mcd(a,b) = 1$ entonces $a|c$.

*Demostración:*Para ciertos enteros sy t se tiene $1 = mcd(a,b) = sa+tb$. Multiplicando por c resulta $c = sac+tbc$ y como $a|sac$y$a|tbc$ se tiene que $a|sac+tbc = c$.

4.6 Números coprimos

Definición 4.9
Dos números a y b se dicen coprimos, primos relativos o primos entre sí si no tienen más divisor común que 1, es decir si $mcd(a,b) = 1$. Observe que en este caso $mcm(a,b) = ab$. Si $mcd(a,b) = d$ entonces $mcd(a/d,b/d) = 1$, es decir que a/d y b/d son coprimos.

4.7 Mínimo común múltiplo

El mínimo común múltiplo de a y b es el menor de sus múltiplos comunes y se denota $mcm(a,b)$. El $mcm(a,b)$ es igual al producto de los factores primos comunes y no comunes elevados al mayor de los exponentes con que aparecen en a y b. De aquí se deduce que $mcm(a,b)$ no sólo es el menor múltiplo común sino que además divide a cualquier otro múltiplo común de a y b. El $mcd(a,b)$ y el $mcm(a,b)$ satisfacen la siguiente relación:

$$mcd(a,b) \cdot mcm(a,b) = a \cdot b$$

. Si un número natural es divisible entre el producto ab de otros dos, entonces es divisible entre cada uno de ellos. El recíproco no es cierto: 12 es divisible entre 4 y entre 6 pero no es divisible entre 4·6 = 24. Lo que siempre se puede afirmar es que si n es múltiplo de a y de b entonces n es múltiplo de $mcm(a,b)$.

4.8 Practico 4 (parte 1)

Problema 4.1 Los números desde el 1 hasta el 2009 se escriben consecutivamente en la pizarra. En una primera pasada se borran el primer número escrito, el tercero, el quinto y así sucesivamente hasta borrar el 2009. En una segunda pasada se aplica el mismo procedimiento a los números que quedaron, borrando el primero de ellos, el tercero, el quinto y así sucesivamente. Esto se repite mientras queden números en la pizarra. ¿En qué pasada se elimina el 1728? ¿Cuál es el último número borrado y en qué pasada se elimina?

Problema 4.2 Pruebe que $n(n+1)(n+2)$ es múltiplo de 6 para cualquier entero n.

Problema 4.3 Pruebe que $n(n+1)(n+2)(n+3)$ es múltiplo de 24 para cualquier entero n.

Problema 4.4 Probar que el número $1+k^2+k^4$ es compuesto para cualquier número k entero mayor que 1.

Problema 4.5 Pruebe que para cualquier número natural n el número n^3+2n es múltiplo de 3.

Problema 4.6 Pruebe que $17|2m+3n$ si y sólo si $17|9m+5n$ (m y n enteros).

Problema 4.7 Caracterice los números naturales que tienen una cantidad impar de divisores.

Problema 4.8 Dado un número, una extraña calculadora sólo puede hacer lo siguiente: multiplicarlo por 2 o por 3, o calcular su segunda o tercera potencia. Si comenzamos con el número 15, ¿cuál de los siguientes resultados se puede obtener al usar la calculadora cinco veces consecutivas?
(a) $2^6 3^6 5^4$; **(b)** $2^8 3^5 5^6$; **(c)** $2^8 3^4 5^2$; **(d)** $2^3 3^3 5^3$; **(e)** $23^2 5^6$.

Problema 4.9 Halle el menor número natural A tal que $10A$ es un cuadrado perfecto y $6A$ es un cubo perfecto.

Problema 4.10 Un número primo se dice que es extraño si tiene un solo dígito, o si tiene dos o más dígitos pero los dos números que se obtienen omitiendo el primero o el último dígito son también primos extraños. ¿Cuántos primos extraños hay?

Problema 4.11 Sea n un entero positivo. Pruebe que si 2^n-1 es primo entonces n es primo.

Problema 4.12 Sea n un entero positivo. Pruebe que si 2^n+1 es primo entonces n es una potencia de 2.

Problema 4.13 En cada lado de un pentágono se escribe un número natural, de manera tal que números adyacentes nunca tienen un factor común mayor que 1, pero números no adyacentes siempre tienen un factor común mayor que 1. Hay muchas posibilidades de hacer esto, pero uno de los números siguientes no aparecerá nunca en los lados del pentágono. ¿Cuál es?

(a) 15 ; **(b)** 18 ; **(c)** 19 ; **(d)** 21 ; **(e)** 22.

Problema 4.14 Todos los divisores del entero positivo N, diferentes de N y 1, se escriben en orden creciente. ¿Cuántos números naturales N son tales que el mayor de los divisores escritos es 45 veces más grande que el menor?

Problema 4.15 Si $56a = 65b$, pruebe que $a+b$ es compuesto.

Problema 4.16 Pruebe que para cualquier número natural n existen n números naturales consecutivos que son compuestos.

Problema 4.17 Halle el menor entero positivo n tal que cada dígito de $15n$ sea 0 ó 2.

Problema 4.18 Halle todas las soluciones enteras de la ecuación $xy-3x-2y=15$.

Problema 4.19 Halle todos los enteros positivos que son menores que 1000 y cumplen con la siguiente condición: el cubo de la suma de sus dígitos es igual al cuadrado de dicho entero.

Problema 4.20 Sea B un entero mayor que 10 tal que cada uno de sus dígitos pertenece al conjunto $\{1,3,7,9\}$. Demuestre que B tiene un factor primo mayor o igual que 11.

Problema 4.21 Un entero positivo al ser dividido entre 4 deja resto 1 y al ser dividido entre 5 deja resto 3. ¿Qué resto deja al ser dividido entre 20?

Problema 4.22 Si dividimos 336 entre el número natural n el resto es 2. Entonces el resto que se obtiene al dividir 2007 entre n es: **(a)** 100 ; **(b)** 3 ; **(c)** 2; **(d)** 1; **(e)** 0.

Problema 4.23 Cinco números enteros se escriben alrededor de un círculo de manera que la suma de dos o de tres números adyacentes no sea nunca múltiplo de 3. ¿Cuántos de los cinco números son múltiplos de 3?

Problema 4.24 Halle el menor entero mayor que 1 tal que al dividirlo entre 2,3, 4, 5, 6, 7, 8 o 9 deja resto 1.

Problema 4.25 Halle el menor entero positivo tal que al dividirlo entre 2 deja resto 1, al dividirlo entre 3 deja resto 2, al dividirlo entre 4 deja resto 3, al dividirlo entre 5 deja resto 4, al dividirlo entre 6 deja resto 5, al dividirlo entre 7 deja resto 6, al dividirlo entre 8 deja resto 7 y al dividirlo entre 9 deja resto 8.

Problema 4.26 ¿Cuál es el exponente de 7 en la descomposición de 2011! en producto de factores primos?

Problema 4.27 ¿En cuántos ceros termina 2011!?

Problema 4.28 Demuestre que no existen enteros positivos x e y tales que $x^{2008} + 2008! = 21^y$.

Problema 4.29 Sean $a = \underbrace{999 \cdot 999}_{40 nueves}$ y $b = 999999999999$. Halle $mcd(a,b)$.

Problema 4.30 Juan, Mario y Pedro entrenan dando vueltas en bicicleta a una pista circular. Juan tarda 8 minutos en dar una vuelta, Mario tarda 9 minutos y Pedro tarda 12 minutos. Si los tres parten del mismo punto a las 6:00 am, ¿a qué hora volverán a encontrarse?

Problema 4.31 Pruebe que todo número natural tiene un múltiplo cuyos dígitos son solamente unos o ceros.

Problema 4.32 Pruebe que todo número natural coprimo con 10 tiene un múltiplo cuyos dígitos son todos unos.

Problema 4.33 Se tiene una hoja rectangular de papel milimetrado de 259×154 . Si se traza una diagonal, ¿cuántos cuadraditos atraviesa? Se dice que la diagonal atraviesa un cuadradito si contiene al menos un punto interior del mismo.

Problema 4.34 Ana vende galletas, que vienen en cajas pequeñas de 5 unidades y en cajas grandes de 12 unidades. Si, por ejemplo, un cliente quiere 39 galletas, Ana puede despachar el pedido exactamente con tres cajas pequeñas y dos grandes, ya que $3 \times 5 + 2 \times 12 = 39$. Pero hay pedidos que no se pueden despachar exactamente, por ejemplo, cuando un cliente quiere 7, 16 ó 23 galletas. ¿Cuál es el pedido más grande que no se puede despachar exactamente? Nota: Se supone que Ana tiene o puede pedir a la fábrica todas las galletas que le hagan falta.

Problema 4.35 Sean a y b naturales coprimos. Pruebe que cualquier natural suficientemente grande puede expresarse en la forma $sa + tb$ con s y t enteros no negativos. ¿Cuál es el mayor entero que no se puede expresar en esa forma?

Problema 4.36 Pruebe que existen infinitos números primos de la forma $4n + 3$.

Algunos problemas abiertos sobre números primos

1. Dos números primos son **gemelos** si difieren en dos unidades. Por ejemplo 3 y 5, 5 y 7, 11 y 13, 17 y 19, 101 y 103, 1997 y 1999. ¿Existen infinitos pares de primos gemelos? No se sabe.
2. **La conjetura de Goldbach**, mencionada por primera vez en una carta de Goldbach a Euler en 1742, afirma que todo número par mayor que 2 es suma de dos números primos. Por ejemplo 4 = 2+2, 6 = 3+3, 8 = 3+5, 1000 = 3+997, 10000 = 59 + 9941. Se conocen muchos resultados parciales, pero la conjetura aún no se ha probado ni refutado, aunque en los últimos años se han hecho muchos anuncios al respecto.
3. ¿Existen infinitos números primos de la forma $2^p - 1$, con p primo? (Los primos de esta forma se llaman **números primos de Mersenne**). ¿Existen infinitos números primos de la forma $2^{2^n} + 1$, con n entero no negativo)? (Los primos de esta forma se llaman **números primos de Fermat**).

4.9 curiosidades

Científico Argenetino Resuelve un problema de más de 2000 años

Ingeniero de la Universidad Nacional de Cuyo y con una riquísima experiencia en el campo de las ciencias exactas, *Horacio Retamales* logró desentrañar un enigma numérico prácticamente prehistórico. ¿Aplicación?: el mundo secreto de las "passwords". ¿De qué se trata el problema que resolvió?

-Se vincula con la Ley de Distribución de los Números Primos que ha permanecido oculta desde hace mas de 2000 años. El hallazgo consiste en explicitar los lugares que ocupan todos los primos en el conjunto de los números naturales. Ha permitido ubicar intervalos de números sin primos; es decir, lagunas, e indicar cuantos números contienen, caracterizar ubicación de primos gemelos y explicitar mecanismo de generación de primos a partir de otros menores.

Figura 4.1: HORACIO RETAMALES

4.10 Congruencias

Definición 4.10
La noción de congruencia fue introducida por Gauss (1777-1855). Se dice que dos enteros a y b son congruentes módulo m si $m|(a-b)$. En ese caso se escribe $a \equiv b(\mod m)$.

4.10.1 Propiedades

Las congruencia módulo m tiene muchas propiedades similares a las de la igualdad, entre ellas la reflexividad, la simetría y la transitividad:

1. $a \equiv a(\mod m)$,
2. $a \equiv b(\mod m) \Rightarrow b \equiv a(\mod m)$,
3. $a \equiv b(\mod m)$ y $b \equiv c(\mod m) \Rightarrow a \equiv c(\mod m)$.

También se pueden sumar, restar o multiplicar congruencias (del mismo módulo) miembro a miembro:
Si $a \equiv b(\mod m)$ y $c \equiv d(\mod m)$ entonces

$a+c \equiv b+d(\mod m)$,

$a-c \equiv b-d(\mod m)$,

$ac \equiv bd(\mod m)$.

La prueba de todas estas propiedades es inmediata. Por ejemplo la última se prueba así: como $a \equiv b(\mod m)$ y $c \equiv d(\mod m)$ se tiene, por definición, que $p|(a-b)$ y $p|(c-d)$. Pero $ac-bd = ac-ad+ad-bd = a(c-d)+(a-b)d$,

por lo tanto $p|(ac-bd)$ y $ac \equiv bd(\mod m)$.

Si $mcd(a,m) = 1$ entonces a tiene un inverso multiplicativo módulo m, es decir un número s tal que $as \equiv 1(\mod m)$. En efecto, como $sa+tm = 1$ para ciertos enteros s y t, resulta $sa = 1-tm \equiv 1(\mod m)$. Este inverso multiplicativo es único módulo m, ya que si $sa \equiv s'a \equiv 1(\mod m)$ entonces, como $mcd(a,m) = 1$, se deduce $s \equiv s'(\mod m)$. La existencia del inverso multiplicativo permite resolver ecuaciones lineales en congruencias del tipo $ax \equiv b(\mod m)$. En efecto, basta multiplicar la congruencia por s y resulta $sax \equiv sb(\mod m)$, o sea $x \equiv sb(\mod m)$.
Si $m \neq 0$ y r es el resto de la división de a entre m, entonces $a = mq+r$ y $m|(a-r)$, es decir que $a \equiv r(\mod m)$. Como $0 \leq r < m$ podemos
decir que cualquier entero es congruente módulo m con uno de los números 0,1,...,$m-1$. Si a y b dejan el mismo resto r al dividirlos entre m, entonces $a \equiv r \equiv b(\mod m)$ y
por transitividad $a \equiv b(\mod m)$. Recíprocamente, si $a \equiv b(\mod m)$ y al dividir a y b entre m se obtienen restos r y s, respectivamente,
entonces $r \equiv a \equiv b \equiv s(\mod m)$ y por transitividad resulta $r \equiv s(\mod m)$, es decir $m|(r-s)$. Pero como $0 \leq r$, $s < m$ se tiene que $0 \leq |r-s| < m$, y la única posibilidad para que m divida a $r-s$ es

$r-s=0$, es decir $r=s$. En resumen, $a \equiv b(\mod m)$ si y sólo si al dividir a y b entre m se obtienen restos iguales.

Ejemplo 4.4

Calcular el resto de la división de 2^{2011} entre 7.

Solución: Calcular 2^{2011} para después efectuar la división está claramente fuera de nuestro alcance (al menos con lápiz y papel). Pero como $2^3 = 8 \equiv 1(\mod 7)$ se tiene
$2^{2011} = 2^{3670+1} = (2^3)^{670} \cdot 2 \equiv 1^{670} \cdot 2 \equiv 2(\mod 7)$

4.11 Criterios de divisibilidad

Existen varios criterios de divisibilidad que permiten averiguar rápidamente si un número natural es divisible entre otros números naturales pequeños. Los más conocidos afirman que un número es divisible entre:

2 si y sólo si su última cifra es par.

3 si y sólo si la suma de sus cifras es divisible entre 3.

4 si y sólo si el número formado por sus dos últimas cifras es divisible entre 4.

5 si y sólo si su última cifra es 0 ó 5.

7 si y sólo si al quitarle la cifra u de las unidades y restarle 2u al número resultante, se obtiene un múltiplo de 7.

8 si y sólo si el número formado por sus 3 últimas cifras es divisible entre 8.

9 si y sólo si la suma de sus cifras es divisible entre 9.

10 si y sólo si su última cifra es 0.

11 si y sólo si la suma algebraica alternada de sus cifras es múltiplo de 11.

13 si y sólo si al quitarle la cifra u de las unidades y sumarle $4u$ al número resultante, se obtiene un múltiplo de 13.

Las pruebas son sencillas usando congruencias. Por ejemplo, como $10 \equiv 1(\mod 9)$ resulta que $10k \equiv 1(\mod 9)$ y entonces

$a_n 10^n + a_{n-1}10^{n-1} + \cdots a_1 \cdot 10 + a_0 \equiv a_n + a_{n-1} + \cdots a_1 + a_0(\mod 9)$,
de donde se deducen los criterios de divisibilidad entre 9 y 3.
como $10 \equiv -1(\mod 11)$ resulta que $10^{2k} \equiv 1(\mod 11)$ y $10^{2k+1} \equiv -1(\mod 11)$, de donde
$a_n 10^n + a_{n-1}10^{n-1} + \cdots a_1 \cdot 10 + a_0 \equiv (-1)^n a_n + \cdots + a_2 - a_1 + a_0(\mod 11)$,
de donde se deduce el criterio de divisibilidad entre 11.

Tal vez los criterios menos conocidos (y usados) sean los de divisibilidad entre 7 y 13. El criterio del 7 afirma que $n = 10a + u$ es divisible entre 7 si y sólo si $a - 2u$ lo es. Pero si $10a + u \equiv 0(\mod 7)$, multiplicando por -2
resulta $-20a - 2u \equiv 0(\mod 7)$, es decir $a - 2u \equiv 0(\mod 7)$ (pues $-20 \equiv 1(\mod 7)$), y recíprocamente si $a - 2u \equiv 0(\mod 7)$ multiplicando por 10 resulta
$10a - 20u \equiv 0(\mod 7)$, es decir $10a + u \equiv 0(\mod 7)$. Análogamente se prueba el criterio del 13.

Algunos ejemplos:

987654 es divisible entre 2 pero no entre 4.

123456 es divisible entre 3 pero no entre 9.

12345 es divisible entre 5 pero no entre 10.

123456789 es múltiplo de 9 pero no de 6. 273 es múltiplo de 7 pues $27-2\cdot 3=21$ lo es.

917652 es divisible entre 11 pues $9-1+7-6+5-2=11$ lo es. Cualquier número con una cantidad par de cifras idénticas es divisible entre 11, ya que la suma alternada de todas ellas es 0.

4.12 Función ϕ de Euler

Si n es un número natural se define $\phi(n)$ como la cantidad de números del conjunto $\{1,2,...,n\}$ que son coprimos con n. Por ejemplo $\phi(6)=2$ ya que de los números 1, 2, 3, 4, 5 y 6 solamente 1 y 5 son coprimos con 6. Si p es primo y a natural entonces entre 1 y p^a solamente los números $p,2p,3p,...,p^{a-1}p=p^a$ no son coprimos con p a , es decir que $\phi(p^a)=p^a-p^{a-1}=p^a\left(1-\frac{1}{p}\right)$.
Más en general se puede probar que si $n=p_1^{a_1}p_2^{a_2}\cdot p_k^{a_k}$

entonces

$$\phi(n)=\left(p_1^{a_1}-p_1^{a_1-1}\right)\left(p_2^{a_2}-p_2^{a_2-1}\right)\cdots\left(p_k^{a_k}-p_k^{a_k-1}\right)=$$

$$=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$$

4.13 Teorema de Euler-Fermat

Teorema 4.3

Si $mcd(a,n)=1$ entonces $a^{\phi(n)}\equiv 1(\mod n)$.

Demostración. Sean $c_1,c_2,\cdots,c_{\phi(n)}$ los elementos de $\{1,2,\cdots,n\}$ que son coprimos con n y pongamos $ac_i=q_in+r_i$, para $i=1,\cdots,\phi(n)$, con $0\leq r_i<n$.

Es claro que los restos r_i son todos diferentes, ya que $r_i=r_j\Rightarrow ac_i=ac_j(\mod n)\Rightarrow c_i=c_j(\mod n)$
(por ser a coprimo con n), absurdo. Además
$mcd(r_i,n)=mcd(ac_i-q_in,n)=mcd(ac_i,n)=1$. Se concluye que $\{c_1,c_2,\cdots,c_{\phi(n)}\}=\{r_1,r_2,\cdots,r_{\phi(n)}\}$.
Pero $r_i\equiv ac_i(\mod n)$, por lo tanto
$c_1c_2\cdots c_{\phi(n)}=r_1r_2\cdots r_{\phi(n)}\equiv a_{\phi(n)}c_1c_2\cdots c_{\phi(n)}(\mod n)$, de donde resulta a $\phi(n)\equiv 1(\mod n)$.

4.14 pequeño Teorema de Fermat

Lema 4.2 Un caso particular importante se presenta cuando n es primo. Observe que si p es primo entonces $\phi(p) = p - 1$, por lo tanto se tiene: **Teorema (pequeño) de Fermat** Si p es primo y $pno|a$, entonces

$$a^{p-1} \equiv 1(\quad \text{mód } p)$$

.

4.15 Pactico 4 (parte 2)

Problema 4.37 Un número se escribe con cien ceros, cien unos y cien doses,en algún orden. ¿Puede ser un cuadrado perfecto?

Problema 4.38 Pedro multiplicó dos enteros de dos cifras cada uno y codificó los factores y el producto con letras, usando letras iguales para dígitos iguales y letras diferentes para dígitos diferentes. Entonces le mostró al maestro su trabajo: $AB \cdot CD = EEFF$. Pero el maestro le contestó: Revisa lo que hiciste,pues cometiste un error. ¿Cómo supo eso el maestro?

Problema 4.39 Permutando las cifras del número 122333444455555666666777777 ¿podrá obtenerse un cuadrado perfecto?

Problema 4.40 Si m y n son enteros tales que m^2+n^2 es múltiplo de 3, pruebe que tanto m como n son múltiplos de 3.

Problema 4.41 Hallar el menor entero positivo x tal que $21x \equiv 2(\mod 37)$.

Problema 4.42 Pruebe el siguiente Criterio general de divisibilidad: Sea n un entero positivo coprimo con 10. Sea m un inverso multiplicativo de 10 módulo n. Entonces el entero $10a+u$ (donde $0 \leq b \leq 9$) es divisible entre n si y sólo si $a+mu$ lo es. Nota: Como casos particulares se tiene que $10a+u$ es divisible entre 13 si y sólo si $a+4u$ lo es, entre 17 si y sólo si $a-5u$ lo es, entre 19 si y sólo si $a+2u$ lo es.

Problema 4.43 Si x, y, z son enteros tales que $x^2+y^2=z^2$, pruebe que al menos uno de ellos es múltiplo de 3.

Problema 4.44 Si tres números primos mayores que 3 están en progresión aritmética, pruebe que la razón (o diferencia común) de la progresión es múltiplo de 6.

Problema 4.45 Se tienen 7 números enteros tales que la suma de 6 cualesquiera de ellos es divisible entre 5. Pruebe que los 7 números son múltiplos de 5.

Problema 4.46 Si x, y, z son enteros tales que $x^2+y^2+z^2$ es múltiplo de 4, pruebe que tanto x, y, z son los tres pares.

Problema 4.47 Pruebe que $2222^{5555}+5555^{2222}$ es divisible entre 7.

Problema 4.48 ¿Qué resto se obtiene al dividir $2^{3^{2011}}$ entre 17?

Problema 4.49 Pruebe que existe n tal que 3^n tiene al menos 2011 ceros consecutivos.

Problema 4.50 Pruebe que, dado cualquier natural N, existe n tal que2^n tiene al menos N ceros consecutivos.

5 — Ecuaciones Diofánticas

Generalidades

Estas ecuaciones reciben este nombre en honor a Diofanto , matemático que trabajó en Alejandría a mediados del siglo III a.c. Fue uno de los primeros en introducir la notación simbólica en matemáticas y escribió seis libros sobre problemas en las que consideraba la representación de números anterior como suma de cuadrados.

Definición 5.1
Se llama ecuación diofántica a cualquier ecuación algebráica con coeficientes enteros, generalmente de varias variables, planteada sobre el conjunto de los números enteros $\mathbb{Z}$ o los números Naturales $\mathbb{N}$, es decir, se trata de ecuaciones cuyas solucones son números enteros.

Ejemplos:

I. $3x+8y=5$
II. $x^2+y^2=z^2$
III. $x^4+y^4=z^4$
IV. $x^2+y^2=7z^2$
V. $x^2+1=y^2$
VI. $x^6+y^6+z^6+u^6+v^6=w^6$
VII. $x^k+y^k=n!z^k, k\geq 2, n>1$

Veremos como resolver ecuaciones diofánticas dividiendo en diferentes tipos:

5.1 Métodos elementales para resolver ecuaciones diofánticas

5.1.1 Ecuaciones Diofánticas lineales con dos incógnitas

Definición 5.2

Una ecuación diofántica es lineal con coeficientes enteros si es de la forma:

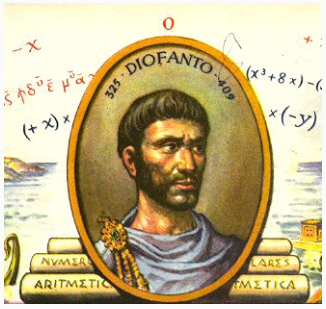
$$ax + by = c$$

donde $a, b, c \in Z$ y que exige soluciones también enteras.

Solución de una Ecuación Diofántica

Veremos un teorema que nos permite saber cuando una ecuación de este tipo tiene solución y aporta un método para calcular una solución particular de la misma.

Historia



Matemático griego de la escuela de Alejandría (a.c. 325 a.c. 410). Dejó trece libros de aritmética, de los cuales sólo los seis primeros nos han llegado, y otro sobre los Números angulares. Aunque tomó como ejemplo para sus métodos los trabajos de Hiparco, su teoría completamente nueva de ecuaciones de primer grado y la resolución que dio a las de segundo hacen de él un innovador en este campo.

Sus obras han constituido tema de meditación de sus contemporáneos griegos, y de los árabes, y, más tarde, de los geómetras del renacimiento. El mismo Viete en su obra capital, reproduce sus proposiciones, aunque sustituye los problemas abstractos por cuestiones de geometría resolubles por álgebra.

Solución Particular

Definición 5.3 Solución Particular

Sean a , b y c tres números enteros. La ecuación lineal $ax + by = c$ tiene solución entera si, y sólo si el máximo común divisor de a y b divide a c.

Demostración

Sólo sí. En efecto, supongamos que los enteros x_0 e y_0 son solución de la ecuación $ax + by = c$, es decir, $ax_0 + by_0 = c$. Pues bien, si $d = m.c.d.(a,b)$, entonces

$$d = m.c.d.(a,b) \Rightarrow d|a \qquad \text{y} \qquad d|b \Rightarrow d|ax_0 + by_0 \Rightarrow d|c$$

Si. Recíprocamente, supongamos que $d = m.c.d.(a,b)$ es divisor de c. Entonces,

$$m.c.d.(a,b) = d \Rightarrow m.c.d.\left(\frac{a}{d},\frac{b}{d}\right) = 1$$

$$\Leftrightarrow \exists p,q \in \mathbb{Z} : \frac{a}{d}p + \frac{b}{d}q = 1$$

$$a\frac{cp}{d} + b\frac{cq}{d} = c$$

siendo $\frac{c}{d}$ entero ya que, por hipótesis, d es divisor de c. Ahora bastaría tomar

$$x_0 = \frac{cp}{d} \quad \wedge \quad y_0 = \frac{cq}{d}$$

y tendríamos que

$$ax_0 + by_0 = c$$

es decir los enteros x_0 e y_0 son solución de la ecuación.
La solución encontrada se llamará solución particular del sistema.
y tendríamos que $ax_0 + by_0 = c$
es decir los enteros x_0 e y_0 son solución de la ecuación.
La solución encontrada se llamará solución particular del sistema.?
Obsérvese que este teorema además de asegurar la existencia de solución para una ecuación de este tipo, ofrece un método para calcularla. El siguiente ejemplo aclarará estas cuestiones.

Ejemplo 5.1

Encontrar una solución para la ecuación diofántica $525x + 100y = 50$

Solución:

1. Veamos si existe solución entera para la ecuación. Calculamos el máximo común divisor de 525 y 100 mediante el algoritmo de Euclides.

	5	4
525	100	**25**
25	0	

es decir, m.c.d.(525,100) = 25

y como 25 divide a 50, el teorema anterior asegura la existencia de solución entera para la ecuación.

2. Calculamos una solución para la ecuación. Siguiendo el método indicado en la demostración del teorema , hallamos los coeficientes de la com- binación lineal del máximo común divisor de 525 y 100. Bastaría seguir el algoritmo de Euclides hacia atrás.

$$25 = 1 \cdot 525 + (-5)100$$

por tanto, los coeficientes buscados son $p = 1$ y $q = -5$ y según el citado teorema una solución para la ecuación sería

$$x_0 = \frac{cp}{d} \quad \wedge \quad y_0 = \frac{cq}{d}$$

donde c es el término independiente de la ecuación y d el máximo común divisor de los coeficientes de x e y. Consecuentemente,

$$x_0 = \frac{50,1}{25} = 2 \quad \wedge \quad y_0 = \frac{50.(-1)}{25} = -10$$

5.1.2 Solución General

Solución General

Sean a , b y c tres números enteros no nulos tales que el máximo común divisor de a y b divide a c. Entonces la solución general de la ecuación $ax + by = c$ es

$$x = x_0 + k\frac{b}{d} \quad \wedge \quad y = y_0 - k\frac{a}{d}$$

donde x_0 e y_0 es una solución particular de la misma y k es cualquier número entero.

Demostración

Sea d el máximo común divisor de a y b. Por hipótesis d divide a c luego el teorema (solución particular) asegura la existencia de una solución particular $x = x_0$ e $y = y_0$ para el sistema. Entonces,

$$ax_0 + by_0 = c$$

Dividiendo ahora ambos miembros de esta ecuación por el máximo común divisor de a y b, tendremos,

$$\frac{a}{d}x_0 + \frac{b}{d}y_0 = \frac{c}{d}$$

Siendo $\frac{c}{d}$ entero y $\frac{a}{d}$, $\frac{b}{d}$ números enteros primos entre sí, luego el máximo común divisor de ambos es 1 y como 1 divide a $\frac{c}{d}$, el teorema (solución particular) asegura la existencia de una solución particular x_1 , y_1 para esta ecuación, luego

$$\frac{a}{d}x_1 + \frac{b}{d}y_1 = \frac{c}{d}$$

Pues

$$\frac{a}{d}x_0+\frac{b}{d}y_0=\frac{c}{d} \quad \textbf{(1)} \qquad \wedge \qquad \frac{a}{d}x_1+\frac{b}{d}y_1=\frac{c}{d} \quad \textbf{(2)}$$

de **(1)** y **(2)**:

$$\frac{a}{d}(x_1-x_0)+\frac{b}{d}(y_1-y_0)=0$$

$$\frac{a}{d}(x_1-x_0)=\frac{b}{d}(y_0-y_1)$$

$$\frac{b}{d}|\frac{a}{d}(x_1-x_0)$$

y al ser $\frac{b}{d}$ primo con $\frac{a}{d}$, dividirá a x_1-x_0 , luego

$\frac{b}{d}|x_1-x_0 \Leftrightarrow \exists k\in\mathbb{Z}: x_1-x_0=k\cdot\frac{b}{d} \Rightarrow x_1=x_0+k\cdot\frac{b}{d}$
Sustituimos el valor de x_1-x_0

$$\frac{a}{d}\cdot(x_1-x_0)+\frac{b}{d}\cdot(y_1-y_0)=0$$

$$\frac{a}{d}\cdot k\cdot\frac{b}{d}+\frac{b}{d}\cdot(y_1-y_0)=0 \Rightarrow \frac{a}{d}\cdot k+y_1-y_0=0$$

$$\Rightarrow y_1=y_0-k\cdot\frac{a}{d}$$

Veamos, finalmente, que x_1 e y_1 es solución de la ecuación $ax+by=c$. En efecto,

$$ax_1+by_1=a\left(x_0+k\cdot\frac{b}{d}\right)+b\left(y_0+k\cdot\frac{a}{d}\right)=$$

$$=ax_0+a\cdot k\cdot\frac{b}{d}+by_0-b\cdot k\cdot\frac{a}{d}=ax_0+by_0=c$$

luego,

$$x=x_0+k\cdot\frac{b}{d}$$
$$y=y_0-k\cdot\frac{a}{d}$$

es solución de la ecuación $ax+by=c$ cualquiera que sea $k\in Z$. La llamaremos solución general de dicha ecuación.

En el ejemplo anterior, teníamos que $x_0=2$ e $y_0=-10$
era una solución particular para la ecuación $525x+100y=50$
luego una solución general de la misma, será:

$$x = 2 + k \cdot \frac{100}{25} = 2 + 4k$$

$$y = -10 - k \cdot \frac{525}{25} = -10 - 21k$$

siendo k cualquier número entero. ?

Ejemplo 5.2

Calcular las soluciones enteras de la ecuación diofántica $66x + 550y = 88$

Solución:

$$66x + 550y = 88$$

1. Veamos si la ecuación admite solución entera. Calculamos el máximo común divisor de 66 y 550 por el algoritmo de Euclides.

$$\begin{array}{lll} 550 & = 66 \cdot 8 & + 22 \\ \hline 66 & = \boxed{\mathbf{22}} \cdot 3 & \mathbf{0} \end{array}$$

   Luego, $m.c.d.(66, 550) = 22$
   y como 22 divide a 88, término independiente de la ecuación, por el teorema se sigue que la ecuación propuesta admite una solución particular $x = x_0$, $y = y_0$.
2. Calculamos esta solución particular.

   Volviendo hacia atrás en el algoritmo de Euclides, tendremos

$$22 = (-8) \cdot 66 + 1 \cdot 550$$

   luego,

$$x_0 = \frac{88 \cdot (-8)}{22} = -32$$

$$y_0 = \frac{88 \cdot 1}{22} = 4$$

   es una solución particular de la ecuación.

3. Calculemos ahora la solución general.

   Según lo visto en el teorema si una solución particular de la misma es $x_0 = -32$ e $y_0 = 4$, entonces la solución general es:

$$x = -32 + k \cdot \frac{550}{22} = -32 + 25 \cdot k$$

$$y = 4 - k \cdot \frac{66}{22} = 4 - 3k$$

   siendo k cualquier número entero.

Ejemplo 5.3

Se queremos cambiar $40 en monedas de 25 centavos y 10 centavos. ¿De cuántas maneras posibles se puede efectuar el cambio?

Solución:

planteamos la ecuación

$$40 = 0,25 \cdot x + 0,10 \cdot y$$

multiplicamos por 100 para dejar la ecuación con coeficientes enteros.

$$25 \cdot x + 10 \cdot y = 4000$$

Calculamos el máximo común divisor de 25 y 10 por el algoritmo de Euclides.

$$\begin{array}{llll} 25 & = 10 \cdot 2 & +5 \\ \hline 10 & = \boxed{\mathbf{5}} \cdot 2 & +\mathbf{0} \end{array}$$

5|4000 entonces tiene solución

podemos simplificar la ecuación:

$$5 \cdot x + 2 \cdot y = 800$$

Volviendo hacia atrás el algoritmo de Euclides.

$$5 \cdot 1 + 2 \cdot (-2) = 1$$

multiplicamos por 800.

$$5 \cdot 800 + 2 \cdot (-1600) = 800$$

$$x_0 = 800 + 2k$$

$$y_0 = -1600 - 5k$$

Luego tenemos que

$$x_0 = 800 + 2k \geq 0$$

$$y_0 = -1600 - 5k \geq 0$$

resolviendo las inecuaciones

$$-400 \leq k \leq -320$$

En este caso tendremos **81** posibilidades.

Ejemplo 5.4

Hallar las soluciones enteras para la ecuación

$$\sqrt{(x+y)(x-y)+(2x+2y-3)y-2(x-7)} = x+y+3$$

Solución:

$$x^2-y^2+2xy+2y^2-3y-2x+14 = x^2+y^2+2xy+6x+6y+9$$

y simplificando, resulta

$$8x+9y = 5$$

ahora resovemos la ecuación difantica, y tiene solución ya que $(8:9)|5$.
9 = 8 · 1 + 1
8 = 1 · 8 + 0

Comenzamos a despejar

$1 = 9-8\cdot$ **1**

$1 = 8\cdot$ **(-1)** $+9\cdot$ **1**
multiplicamos por 5 Y nos queda

$5 = 8\cdot$ **(-5)** $+9\cdot$**(5)**

Solución particular: $\boxed{x_0 = -5}$ y $\boxed{y_0 = 5}$
Solución general:

$$\begin{cases} x &= -5+9k \\ y &= 5-8k \end{cases}$$

Ejemplo: si $k = 1$

$$\begin{cases} x &= -5+9\cdot 1 = \mathbf{4} \\ y &= 5-8\cdot 1 = \mathbf{-3} \end{cases}$$

Verificamos:

$$\sqrt{(4-3)(4+3)+(2\cdot 4+2\cdot(-3)-3)\cdot(-3)-2(4-7)} = 4-3+3$$

$$\sqrt{7+(-1)\cdot(-3)-2(-3)}=4$$

$$\sqrt{16}=4$$

Si verifica. Entonces cualquier par $(-5+9k;5-8k)$ siendo $k\in\mathbb{Z}$ satisface la ecuación.

5.1.3 Método de factorización

El método de factorización consiste en expresar una de las partes como un producto y teniendo en cuenta el otro lado *analizando* los casos posibles.

Ejemplo 5.5

Halle todos los números naturales n y los números primos p que sean soluciones de la siguiente ecuación.

$$n^3+7n^2+14n+8=6p$$

Solución:

Fractorizando el primer miembro

$$n^3+7n^2+14n+8=n^3+6n^2+n^2+6n+8n+8=6p$$

$$=n^3(n+1)+6n(n+1)+8(n+1)$$

$$=(n+1)(n^2+6n+8)$$

$$=(n+1)(n+2)(n+4)$$

Además $6p=1\cdot2\cdot3\cdot p$ y $n+4>n+2>n+1>1$, donde $n+1=2, n+2=3, n+4=p$; por lo cual $n=1$ y $p=5$; es decir la solución es $(1,5)$.

5.1.4 Método de paridad

Tablas de paridad

Par: P impar: I

+	P	I
P	P	I
I	I	P

Cuadro 5.1: Tabla de paridad en la suma

·	P	I
P	P	P
I	P	I

Cuadro 5.2: Tabla de paridad en la multiplicación

Ejemplo 5.6

¿ Existen números enteros n y m que satisfacen la siguiente igualdad?

$$n^4 + 16m = 7993$$

Solución:

Si el número n fuese par entonces la ecuación no tiene solución pues 7993 es impar. Por lo tanto, si existe una solución, necesariamente $n = 2k+1$ para un entero k. Entonces reeplazando en la ecuación se tiene

$$(2k+1)^2 + 16m = 7993$$

$$(4k^2+4k+1)^2 + 16m = 7993$$

$$16k^4 + 16k^2 + 1 + 32k^3 + 8k^2 + 8k + 16m = 7993$$

$$8(2k^4 + 2k^2 + 4k^3 + k^2 + k) + 16m = 7992$$

$$2(k^4 + k^2 + 2k^3 + m) + k(k+1) = 999$$

Debido a que $k(k+1)$ es el producto de dos números consecutivos, siempre es divisible por 2 y por lo tanto el número del lado izquierdo es par, mientras que 999 es impar. Esto significa que la ecuacón no tiene solución.

5.1.5 Método de los restos

Ejemplo 5.7

Pruebe que la ecuación $x^2+y^2=2006$ no tiene solución en los enteros.

Solución:

En primer lugar si los números son pares , entonces la suma de los cuadrados siempre es divisible por $4(4|4k^2=(2k)^2)$; y si uno de ellos es impar, entonces la suma de cuadrados deja resto 1 al ser dividido por $4(2k+1)^2=4(k^2+k)+1\equiv 1(\mod 4)$. La ecuación no tendrá solución pues 2006 deja resto 2 al ser dividido por 4. Falta comprobar cuando x e y son impares. Sea $x=2m+1$, $y=2n+1(m,n\in z)$, reemplazando en la ecuación.

$$(2m+1)^2+(2n+1)^2=2006$$

$$4(m^2+m+n^2+n)=2004$$

$$\underbrace{m(m+1)+n(n+1)}_{par}=501$$

Vemos que el lado izquierdo y el derecho son de diferente paridad, de donde se deduce que la ecuación no tiene solución.

5.1.6 El Método de la desigualdad

Este método se utiliza con fracuencia para reducir el conjunto de posibles soluciones, y luego analizar los posibles casos al conjunto reducido. El método de desigualdad se utiliza a menudo en combinación con otros métodos para resolver ecuaciones diofánticas no lineales.

Ejemplo 5.8

Hallar todas la soluciones naturales de la ecuación: $a!+b!=c!$

Solución:

Es evidente que $a<c$ y $b<c$. Sin pérdida de generalidad, podemos suponer que $a\leq b$. De la ecuación $a!+b!-c!=0$

$$a!\left(1+\frac{b!}{a!}-\frac{c!}{a!}\right)=0$$

como $a!>0$, entonces

$$1+\frac{b!}{a!}-\frac{c!}{a!}=0$$

de donde

$$1 = \frac{c!}{a!} - \frac{b!}{a!} = \underbrace{\frac{b!}{a!}}_{\in\mathbb{Z}} \underbrace{\left(\frac{c!}{b!} - 1\right)}_{\in\mathbb{Z}}$$

para $a < b$, se tendrá $\frac{b!}{a!} > 1$ con lo cual, la desigualdad no se verifica, y por lo tanto, es necesario que $a = b$, de donde

$$\frac{c!}{b!} = 2$$

como $c > b \geq 1$ no tendría ninguna solución para $c > 2$ y la única solución es $c = 2$, $b = 1$.

Entonces $a = 1$, y por lo tanto tenemos una única solución que es la terna ordenada $(1\ ;\ 1\ ;\ 2)$.

5.1.7 Ecuaciones diofánticas Exponenciales

Aunque no existe un único método para resolver esto tipos de ecuaciones, veremos a través de diferentes ejemplos como se describen los diferentes enfoques para resolver una ecuación diofántica exponencial.

Ejemplo 5.9 **Método de los factores**

Hallar todos números naturales x (si existen) que sean soluciones de la siguiente ecuación.

$$4^x + 3 \cdot 2^x = 88$$

Solución:

La ecuación es equivalente a

$$2^x(2^x + 3) = 2^3 \cdot 11$$

Como $2^x + 3$ es impar y 2^x es una potencia de 2, entonces se debe tener $2^x = 2^3$ y $2^x + 3 = 11$.

El único número natural que verifica estas dos ecaciones a la vez es $x = 3$. Por lo tanto, la única solución es 3.

Ejemplo 5.10

¿Existen números naturales x e y que sean soluciones de la siguiente ecuación?

$$3^x - 2^y = 1$$

Solución:

Analicemos dos casos: cuando x es un número impar y cuando x es par.

I) Sea x un número impar, $x = 2m+1$, $m \in N_0$. Entonces

$$3^x = 3^{2m+1} = (3^2)^m \cdot 3 = 9^m \cdot 3$$

Como $9 \equiv 1(\mod 4)$, entonces $9^m \cdot 3 \equiv 3(\mod 4)$, de donde

$2^y = 3^x - 1 \equiv 2(\mod 4)$

que solo es posible para $x = y = 1$

II) Sea x un número par, $x = 2m, m \in N$. Entonces

$2^y = 3^m - 1 = (3^m - 1)(3^m + 1)$

De donde los factores $3^m - 1$ y $3^m + 1$ deben ser potencias de 2. Esto es posible solo cuando $3^m - 1 = 2$ y $3^m + 1 = 4$, es decir, cuando $m = 1$, de lel cual $x = 2$ e $y = 3$. Es decir, la única solución de la ecuación diofántica es $(2;3)$.

5.1.8 Ecuaciones con dos incógnita del tipo $x^2 - y^2 = a$

Dada la ecuación $x^2 - y^2 = a$ con $a \in Z$, se puede escribir como $(x+y)(x-y) = a$; si hacemos $m = x+y$ y $n = x-y$ se tendrá $m \cdot n = a$; donde m y n deben ser ambos pares o ambos impares, pues la suma de dos números y su diferencia son ambas pares o ambos impares. Entonces al resolver el sistema.

$$\begin{cases} x+y &= m \\ x-y &= n \end{cases} \quad \text{se obtiene} \quad \begin{cases} x &= \dfrac{m+n}{2} \\ y &= \dfrac{m-n}{2} \end{cases}$$

Ejemplo 5.11

Resuelva la ecuación $x^2 - y^2 = 98$

Solución:

tenemos que $n.m = 98 = 2 \cdot 7^2$

$n = 2$ y $m = 49$, no habría solución.

$n = 7$ y $m = 14$, no habría solución.

Esto implica que si $a \in Z$ tiene un factor 2 con multiplicidad 1, no puede haber una descomposición como se requiere para la ecuación. Por lo tanto, la ecuación no tiene solución.

5.1.9 Método general para resolver ecuaciones Diofánticas Homogéneas de segundo grado

Se descomponen en cruz en dos coeficientes de funciones lineales, igualados a $\frac{m}{n}$ irreducible y que da lugar, con dos fracciones, a dos ecuaciones entre las que se eliminan m y n.

Ejemplo 5.12

Resolver la ecuación Pitagórica

$$x^2+y^2=z^2$$

solución:

$$x^2+y^2=z^2 \longleftrightarrow x^2=z^2-y^2$$

$$\longleftrightarrow x^2=(z+y)(z-y)$$

Acomodando se obtiene

$$\frac{x}{z-y}=\frac{z+y}{x}=\frac{m}{n}$$

$$\begin{cases} nx &= mz-my \\ mx &= nz+ny \end{cases}$$

$\rightarrow m^2z-m^2y=n^2z+n^2y$

$\rightarrow (m^2-n^2)z=(m^2+n^2)y$

De donde $z=m^2+n^2$, $y=m^2-n^2$, $x=2mn$

Hay infinitas soluciones con la libre elección de m y n. Además $(x;y)$ intercambian sus valores.

Curiosidades

La ecuación de Fermat $x^n + y^n = z^n$

El Enunciado del último Teorema de Fermat (1601 - 1665) quedó anotado en el margen de su ejemplar de la Aritmética de Diofánto de Alejandría (150a.n.e) traducida al Latín por Clade Gasper Bachet (1581 - 1638) publicado en 1621. Este libro, con las numerosas notas marginales de Fermat, fué publicado en 1670 por su hijo Clemente Samuel. La ecuación $x^n + y^n = z^n$ no tiene solución entera no trivial (es decir distinta de $x = y = z = 0$) cuando $n \geq 3$

El enunciado del teorema dice lo siguiente:
para $n = 2$, las soluciones son ternas Pitágoricas.
Fermat enunció su conjetura en 1637, escribiendo en el margen de su ejemplar de Aritmética de Diofánto de Alejandría lo siguiente(en Latín):

Es imposible dividir un cubo en suma de otros dos o un bicuadrado en otros dos bicuadrados, en general una potencia superior en dos potencias del mismo grado, he descubierto una demostración maravillosa pero en este margen es demaciado estrecho para contenerla.

Un Matemático aficionado *Andrew Beals* empresario y poseedor de un banco en Texas ofrece 100 000 Dólares USA al que encuentre una demostración para su conjetura, que sea aceptada en el mundo académico o para aquel que encuentre un contraejemplo que demestre su falsedad.

5.2 Práctico 5

Ejercicio 5.1 Calcular todas las soluciones enteras de la ecuaciones en el caso que sea posible.

1. $10x+13y=2$
2. $10x-3y=15$
3. $3x-12y=4$
4. $125x-30y=20$
5. $14x-12y=2$
6. $1,2x+0,5=0,15$
7. $40x-30y=9$

■

Problema 5.1 Queremos echar 21 litros de gasóleo a un depósito usando bidones de 2 y 5 litros. Responder a las siguientes cuestiones:

a) ¿Es posible? ¿Por qué?

b) En caso afirmativo, dar todas las combinaciones posibles.

Problema 5.2 Hallar el menor número de cuatro cifras que dividido por 4, 7 y 11 da resto 3, y que dividido por 13 da resto 1.

Problema 5.3 Los enteros positivos x, y, z cumplen $x+2y=z$, $x^2-4y^2z^2=310$.
Halla todos los posibles valores del producto xyz.

Problema 5.4 Una mujer tiene un cesto de manzanas. Haciendo grupos de 3 sobran 2 y haciendo grupos de 4 sobran 3. Hallar el número de manzanas que contiene el cesto sabiendo que están entre 100 y 110.

Problema 5.5 Hallar todas las soluciones enteras de la ecuación $3xy+2y=7$

Problema 5.6 Resolver la ecuación diofántica $(x-y)^3\cdot(y-z)^3\cdot(z-x)^3=17$.

Problema 5.7 Hallar los x e y tal que $x^2+y^2=2\cdot(x+y)$.

Problema 5.8 Hallar todas las soluciones enteras de la ecuación diofántica

$$3xy+y=7$$

Problema 5.9 Hallar todas las soluciones enteras de la ecuación diofántica

$$2x^2+xy-3y^2=17$$

Problema 5.10 Hallar todas las soluciones enteras de la ecuación diofántica

$$(x-y)^3+(y-z)^3+(z-x)^3=35$$

Problema 5.11 Determine los valores enteros positivos de n para que en número $n^2-4n+16$ sea el cuadrado de un número natural.

Problema 5.12 Hallar todos los números x e y tales que $x^2+10y=1234567$

Problema 5.13 ¿Existen números enteros m y n que satisface la siguiente igualdad ?

$$n^4+16m=7993$$

Problema 5.14 Hallar todos los números naturales que satisfacen la ecuación $a+b+c=abc$

Problema 5.15 ¿Existen números naturales x e y que sean soluciones de la siguiente ecuación?

$$3^{x^2+y-1}-3^{x^2+1}=1944$$

Problema 5.16 ¿Existen números naturales x e y que sean soluciones de la siguiente ecuación?

$$5^x+2^{x+1}\cdot 3^x=3^{2x}+2^{2x}$$

Problema 5.17 ¿Existen números naturales x e y que sean soluciones de la siguiente ecuación?

$$x^2=3^y+7$$

Problema 5.18 Resolver la ecuación

$$x^2-xy+y^2=z^2$$

Problema 5.19 Resolver la ecuación

$$x^2+xy+y^2$$

Problema 5.20 Resolver la ecuación

$$x^2-xy=y^2$$

Problema 5.21 Resolver la ecuación

$$x^2+y^2=5z^2$$

Problema 5.22 ¿Existen números enteros x e y de modo que el resto que se obtiene al dividir x^4+y^4 por 25 es 3?

Problema 5.23 Hallar los valores de x (si existen) que satisfacen la siguiente ecuación.

$$4^x+3\cdot 2^x=88$$

Bibliografía

[1] Filosofía - 1ro Bachillerato - Salustiano Fernández Viejo

[2] Filosofía y Ciudadanía - Lógica proposicional

[3] INDUCCIÓN MATEMÁTICA- EDUARDO SÁEZ , IVÁN SZÁNTÓ - DEPARTAMENTO DE MATEMÁTICA UNIVERSIDAD TECNICA FEDERICO SANTA MARIA.

[4] Teoría de Números para Olímpiadas Matemáticas - José Heber Nieto Said - Departamento de Matemática Facultad de Ciencias - Universidad del Zulia Maracaibo, Venezuela.

[5] Introducción a la Teoría de Números - Walter Mora F.

[6] Preparación Olimpiadas Matemáticas Ecuaciones Diofánticas- David Crespo Casteleiro.

[7] NOCIONES BÁSICAS DE TEORÍA DE CONJUNTOS - UNIVERSIDAD DE SANTIAGO DE CHILE, FACULTAD DE CIENCIA.

6 — Respuestas

6.1 Capítulo 1

Soluciones del Capítulo 1

1.1 $\sim p \wedge q$

1.2 $\sim p \wedge \sim q$

1.3 $\sim (p \wedge q)$

1.4 $p \wedge \sim q$

1.5 $\sim p \wedge \sim q$

1.6 $p \vee q$

1.7 $\sim p \rightarrow \sim q$

1.8 $p \wedge (q \vee r)$

1.9 $(p \wedge q) \vee r$

1.10 $p \rightarrow (\sim q \wedge \sim r)$

1.11 $p \leftrightarrow q$

1.12 $p \rightarrow q$, $r \rightarrow q$, entonces $(p \vee r) \rightarrow q$

1.13 $[(p \rightarrow q) \wedge (p \wedge r) \wedge (s \rightarrow \sim q)] \rightarrow \sim s$

1.14 $\{[\sim (p \wedge q) \rightarrow (r \wedge \sim s)] \wedge (q \rightarrow \sim p)\} \rightarrow r$

1.15 $\{(\sim p \vee q) \wedge [q \rightarrow (r \wedge s)] \wedge \sim (r \wedge s)\} \rightarrow \sim p$

6.2 Capítulo 2

Soluciones del Capítulo 2

a) $(A \cup B^c) \cap (C - A)^c = \{7; d; 1; h; f\}$

b) $(A \cap C) \cup (B - A^c)^c = \{d; 7; 6; a; g; f; h; 1; e; 4; 2; b\}$

c) i) $B \cap C \cup Sub_C\{6\}$

c) ii)$A \cap C$

c) iii) $A \cup B - C$

2.53 a) 8, b) 15, c) 7.

2.55 a) 20, b) 8, c) 33.

2.56 a) 11, b) 12, c) 8, d) 8.

2.57 a) 15 b) 50 c) 40

2.58 20

6.3 Capítulo 3

Soluciones del Capítulo 3

3.1 Demostración: Sea $p(n) : n+(n+1)+(n+2) = 6q$, $q \in N$. Entonces $p(1) : 1+2+3 = 6$ es verdadera $(q = 1.)$ **Hipótesis inductiva :** $p(k) = k+(k+1)+(k+2) = 6q_1$,$q_1 \in N$ es verdadera

Por demostrar $p(k+1) : (k+1)+(k+2)+(k+3) = q_2$, $q_2 \in N$ es verdadera.

Como $(k+1)+(k+2)+(k+3) = k+(k+1)+(k+2)+3 = 6q_1+3 = 6(q_1+\frac{1}{2}) \notin N$. Luego $p(k)$ verdadero no implica $p(k+1)$ verdadero. Por lo tanto, $p(n) : n+(n+1)+(n+2) = 6q$, $q \in N$, es falso. La suma de 3 enteros consecutivos no es necesariamente divisible por 6. Observación: Es facil ver que$n+(n+1)+(n+2) = 3(n+1)$, de donde para que sea divisible por 6, necesariamente el factor $(n+1)$ debe ser un número impar para cualquier n natural, lo que es falso.

3.2 La fórmula no es válida para $n = 1,2,3$ Para $n = 4$, se tiene que $24 = 1 \cdot 2 \cdot 3 \cdot 4 > 2^4 = 16$ es verdadera.
Supongamos que la desigualdad es válida para $k \in N$, con $k \geq 4$; esto es $1 \cdot 2 \cdot 3 \cdot 4 \cdots k > 2^k$, $k \geq 4$.
Por demostrar que la desigualdad es válida para $k+1$, es decir que $1 \cdot 2 \cdot 3 \cdot 4 \cdots k \cdot (k+1) > 2^{k+1}$, $k \geq 4$.
En efecto: $1 \cdot 2 \cdot 3 \cdot 4 \cdots k \cdot (k+1) = (1 \cdot 2 \cdot 3 \cdot 4 \cdots k) \cdot (k+1) > 2^k(k+1) > 2^k \cdot 2 = 2^{k+1}$. Luego $1 \cdot 2 \cdot 3 \cdot 4 \cdots n > 2^n$, y por lo tanto $\forall n \in N$, $n \geq 41 \cdot 2 \cdot 3 \cdot 4 \cdots n > 2^n$

3.3 Demostrar por inducción, que si n es un número impar, $7^n + 1$ es divisible por 8. Antes de aplicar inducción conviene hacer un cambio de índices. Sea $n = 2^i - 1$. Entonces si $i = 1,2,3,...$ se tiene que $n = 1,3,5,...$ y nuestro enunciado se transforma en: 7^{2i-1} es divisible por 8, $i \in N$. Para $i = 1, 7^1 + 1 = 8$ es divisible por 8, lo que es una proposición verdadera. Hipótesis inductiva: $7^{2i-1} + 1$ es divisible por 8. Tesis: 7^{2i+1} es divisible por 8. Dado que nuestra única información es la hipótesis, debemos hacer que la expresión $7^{2i-1} + 1$ aparezca en el desarrollo $7^{2i+1} + 1 = 7^2(7^{2i-1}) + 1 =$

$= 7^2(7^{2i-1} + 1) - 7^2 + 1 = 7^2(7^{2i-1} + 1) - 48$

y aquí ambos sumandos son divisibles por 8, luego 8 divide a $7^{2i+1} + 1$. Luego resulta que $7^n + 1$ es divisible por 8 para todo n impar.

6.4 Capítulo 4

Soluciones del Capítulo 4

4.1 si es escribimos los números :

$$1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,26,27,28,...,,2007,2008,2009$$

y borramos primero los números impares son de la forma $2k+1$,y nos queda:

$$2,4,6,8,10,12,14,16,18,20,22,24,26,28,...,,2008$$

Luego si borramos los números alternados empezando por 2, son de las forma $2\cdot(2k+1)$, y nos queda:

$$4,8,12,16,20,24,28,\cdots$$

Luego si borramos los números alternados empezando por 4, son de la forma $2\cdot(4k+2)$, y nos queda:

$$8,16,24,\cdots$$

Luego los números que borraremos en las proximas series serán de la forma:
4ta ——->$2\cdot(8k+4)$
5ta ——->$2\cdot(16k+8)$
6ta ——->$2\cdot(32k+16)$
7ta ——->$2\cdot(64k+32)$
ect....
Luego verificando el número 1728 corresponde con la forma $2\cdot(64k+32)$ ya que :

$$2\cdot(64k+32)=1728$$

para $k=13$

Por lo tanto, el número 1728 se borra en la 7ma vez y en la posición 13 de la serie.

4.8 Como entre dos números consecutivos uno de ellos siempre es par, entonces $n(n+1)$ es *par* ,y entre tres números consecutivos uno es múltiplo de 3. Entonces $n(n+1)(n+2)$ es múltiplo de 6, por ser múltiplo de 2 y 3 simultanemente.

4.3 Debemos probar que $n(n+1)(n+2)(n+3)$ es múltiplo de 6 y 4 simultaneamente, y como ya vimos en el problema anterior (4.2) el producto de tres números consecutivos siempre es múltiplo de 6, ahora deberíamos probar que también es múltiplo de 4.

si $n=2k$ (par) resulta:

$$n(n+1)(n+2)(n+3)=2k(2k+1)(2k+2)(2k+3)$$

desarrollando y simplificando $\cdots 16k^4+48k^3+24k^2+12k = 4\cdot(4k^4+12k^3+6k^2+3k) = 4q$ luego si n es par es múltiplo de 4 y 6 por lo tanto es múltiplo de 24.

Si $n = 2k+1$ (impar) resulta:

$$n(n+1)(n+2)(n+3) = (2k+1)(2k+1+1)(2k+1+2)(2k+1+3) =$$

$$= (2k+1)(2k+2)(2k+3)(2k+4) = 4\cdot(4k^4+12k^3+6k^2+3k)(2k+4) = 4t$$

luego si n es impar es múltiplo de 4 y 6 por lo tanto para cualquier n es múltiplo de 24.

4.8 Para resolver este problema debemos probar que $1+k^2+k^4$ se puede descomponer en factores.

$$1+k^2+k^4 = 1+k^2+k^4+k^2-k^2 =$$

$$= (1+2k^2+k^4)-k^2 = (1+k^2)^2-k^2 = (1+k^2-k)\cdot(1+k^2+k)$$

listo $1+k^2+k^4$ puede expresarse como producto de factores entonces no es primo y por lo tanto es *compuesto*.

4.5 Si n es múltiplo de 3 entonces $n^3+2n = n(n^2+2)$ también lo es. De lo contrario n debe ser de la forma $3k+1$ o $3k-1$. Pero entonces $n^2+2 = 9k^2 \pm 6k+3 = 3(3k^2 \pm 2k+1)$ es múltiplo de 3.

4.6 Observe que $9m+5n+4(2m+3n) = 17(m+n)$.

4.7 El número de divisores del número $n = {p_1}^{a_1}\cdot {p_2}^{a_2}\cdot\cdots\cdot {p_k}^{a_k}$ es $(a_1+1)(a_2+1)\cdot(a_k+1)$, que es impar si y sólo si todos los a_i son pares, lo cual ocurre si y sólo si n es un cuadrado perfecto. Por Ejemplo: 324 tiene una cantidad de divisores impares ya que $324 = 2^2\cdot 3^4$ y el número de divisores es (2+1)·(4+1) = 15.

Luego $2^2\cdot 3^4 = 2^1\cdot 2^1\cdot 3^2\cdot 3^2 = (2\cdot 3^2)(2\cdot 3^2) = 18^2$ que es cuadrado perfecto.

4.8 Ninguna operación puede incrementar el exponente de 5 sin hacer lo mismo con el de 3. Eso descarta (b) y (e). A (d) sólo se puede llegar multiplicando por 2 y elevando luego al cubo, o elevando al cubo primero y luego multiplicando por 2 tres veces, es decir en 2 o 4 operaciones, y nunca en 5. Para obtener (c) habría que elevar una única vez al cuadrado (por el 5^2), lo cual obliga a realizar al menos cinco operaciones para obtener 2^8 , y al menos otra para obtener 3^4 . Finalmente (a) se obtiene multiplicando dos veces por 2, multiplicando luego por 3, elevando al cubo y multiplicando por 5.

4.9 Para que $10A$ sea un cuadrado perfecto los factores primos 2 y 5 deben aparecer en la descomposición de A con exponente impar. Para que $6A$ sea un cubo perfecto los exponentes de los factores primos 2 y 3 en la descomposición de A deben ser de la forma $3k+2$. Además debe aparecer 5 con exponente múltiplo de 3. Como el menor entero impar de la forma $3k+2$ es cinco, A debe ser divisible entre $2^5\cdot 3^2\cdot 5^3 = 36000$, y éste es el menor A posible. Es fácil ver que los valores de A que cumplen la condición son todos los de la forma $36000n^6$, para n natural.

4.10 Hay 9 primos extraños, a saber 2, 3, 5, 7, 23, 37, 53, 73 y 373.

4.13 El 19. En realidad ningún primo p puede aparecer, pues si aparece los dos números no adyacentes serían múltiplos de p, pero como son adyacentes entre sí se llega a una contradicción. Puede probarse que cualquier número compuesto puede aparecer, pues si $p \neq$ q son dos factores primos de n y r, s y t son primos que no dividen a n, la disposición pr, st, n, rt, qs cumple la condición del problema.

4.14 Si d es el menor divisor de N mayor que 1, entonces el mayor divisor de N menor que N es $45d$ y $d \cdot (45d) = 45d^2 = N$. Es claro que d debe ser primo y que sus únicos valores posibles son 2 y 3. Luego, sólo hay dos números N posibles: $180 = 45 \cdot 2^2$ y $405 = 45 \cdot 3^2$.

4.15 Descomponiendo cada miembro de la igualdad $56a = 65b$ en producto de factores primos, se ve que $a = 65A$ y $b = 56B$ para ciertos naturales A y B, y sustituyendo en la igualdad queda $56 \cdot 65A = 65 \cdot 56B$, de donde $A = B$. Por lo tanto $a + b = 65A + 56A = 11^2 A$ es compuesto.

4.16 Si $n = 1$ se toma cualquier compuesto, si $n > 1$ entonces por ejemplo $(n+1)! + 2, (n+1)! + 3, ..., (n+1)! + n$. Ejemplo: si $n = 4$ los números compuestos serán

$$(4+1)! + 2, (4+1)! + 3, ..., (4+1)! + 4$$

$$5! + 2, 4! + 3, 3! + 4$$

$$122, 123, 124$$

4.17 Como $15n = 5(3n)$ es multiplo de 5, debe terminar en 5 ó en 0. En este caso debe terminar en 0. Como $15n = 3(5n)$ es multiplo de 3, la suma de sus dígitos debe ser múltiplo de 3 y, por tanto, la menor cantidad de doses necesarios para obtener un múltiplo de 3 son tres. Ceros, no hace falta más que el último dígito. Luego, el valor más pequeño para $15n$ es $2220 = 15 \cdot 148$ y el menor n posible es 148.

4.18

$$x \cdot (y-3) - 2y = 15$$

sumando 6 ambos miembros nos queda:

$$x \cdot (y-3) - 2y + 6 = 15 + 6$$

$$x \cdot (y-3) - 2 \cdot (y-3) = 21$$

$$(x-2) \cdot (y-3) = 21$$

Luego como $21 = 3 \cdot 7$ tenemos 4 posibilidades:

$x-2$	$y-3$	x	y
3	7	5	10
7	3	9	6
21	1	23	4
1	21	3	24

4.19 Si n^2 es un cubo perfecto, entonces también n es un cubo perfecto. Los cubos perfectos menores que 1000 son 1, 8, 27, 64, 125, 216, 343, 512 y 729, de los cuales sólo cumplen la condición 1 y 27.

4.20 Si no fuera así, los únicos factores primos de B serían 3 y 7. Pero esto contradice el hecho de que todos los números de la forma $3^n \cdot 7^m$ tienen la cifra de las decenas par. En efecto, esto es cierto para 3 y 7, y si un número tiene la cifra de las decenas par y termina en 1, 3, 7 ó 9, al multiplicartlo por 3 o por 7 seguirá teniendo la misma característica, ya que el acarreo desde la columna de la derecha será siempre par (0, 2, 4 ó 6).

4.21 Sea $n = 5k+3$ y pongamos $k = 4q+r$, con $0 \leq r < 4$. Entonces $n = 5(4q+r)+3 = 20q+5r+3$ deja el mismo resto que $5r+3$ al dividirlo entre 4, y para que ese resto sea 1 debe ser $r = 2$. Por lo tanto la respuesta es $5 \cdot 2 + 3 = 13$.

4.22 Observemos que $n > 2$ y que se puede escribir $336 = qn+2$. Como $336 \cdot 6 = 2016$ se tiene $2007 = 336 \cdot 6 - 9 = 6(qn+2) - 9 = 6qn+3$. Ahora bien, n no puede ser 3 (pues 336 entre 3 deja resto 0 y no 2), es decir que $n > 3$ y la igualdad $2007 = 6qn+3$ muestra que el resto buscado es 3.

4.23 Fijándonos en los restos al dividir los números entre 3 (que pueden ser 0, 1 ó 2) observamos que no puede haber dos ceros contiguos, ni un 1 y un 2 contiguos, ni tres restos iguales consecutivos, ni restos 0, 1 y 2 (en algún orden) consecutivos. De esto se deduce que debe haber algún 0 (de lo contrario habría un 1 y un 2 contiguos, o serían todos unos o todos ceros). Los vecinos de ese 0 deben ser ambos 1 o ambos 2. En el primer caso, los dos restantes deben ser 1 y 0. En el segundo caso, los dos restantes deben ser 2 y 0. Es decir que la configuración cíclica de restos debe ser (1,1,0,1,0) o (2,2,0,2,0) y dos de los cinco números deben ser múltiplos de 3.

4.24 $n-1$ debe ser múltiplo de 2, 3, 4, 5, 6, 7, 8 y 9, por lo tanto el menor posible cumple $n-1 = mcm(2,3,4,5,6,7,8,9) = 2^3 \cdot 3^2 \cdot 5^7 = 2520$, y la respuesta es $n = 2521$.

4.25 Análogamente $n+1 = mcm(2,3,4,5,6,7,8,9) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$, por lo tanto $n = 2519$.

4.26 Desde 1 hasta 2011 hay $\left\lfloor \frac{2011}{7} \right\rfloor = 287$ múltiplos de 7, por lo tanto el exponente buscado es al menos 287. Pero los múltiplos de $7^2 = 49$ contribuyen al menos con dos sietes, por lo tanto se debe sumar $\left\lfloor \frac{2011}{49} \right\rfloor = 41$. Del mismo modo hay que sumar un siete por cada múltiplo de $7^3 = 343$, es decir $\left\lfloor \frac{2011}{343} \right\rfloor = 5$. La respuesta es entonces $287+41+5 = 333$. En general, el exponente de un primo p en $n!$ es

$$\left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \left\lfloor \frac{n}{p^4} \right\rfloor + \cdots$$

4.27 el exponente de 5 en 2011! es

$$\left\lfloor \frac{2011}{5^2} \right\rfloor + \left\lfloor \frac{2011}{5^3} \right\rfloor + \left\lfloor \frac{2011}{5^4} \right\rfloor = 402+80+16+3 = 501$$

y el exponente de 2 es obviamente mayor que el de 5, por lo tanto 2011! termina en 501 ceros.

4.28 Observe que $21 = 3 \cdot 7$.La cantidad de factores primos 3 en 2008! es

$$n = \left\lfloor \frac{2008}{3} \right\rfloor + \left\lfloor \frac{2008}{9} \right\rfloor + \cdots < 2008$$

. Como $3|21$ y $3|2008!$ resulta que $3|x$ y la cantidad de factores primos 3 en x^{2008} es por lo menos 2008. Por lo tanto la mayor potencia de 3 que divide al miembro izquierdo es 3^n , de donde $y = n$. Razonando de manera similar con el 7, y debería ser igual a la cantidad de factores 7 en 2008!. Pero eso es imposible, pues ese número es claramente menor que n.

4.29 Si se divide a entre b el cociente es 10000000000010000000000010000 y el resto 9999. Como obviamente 999999999999 es divisible entre 9999, $mcd(a,b) = 9999$.

4.30 Se volverán a encontrar a los $mcm(8,9,12) = 72$ minutos, o sea , a las 7:12 am.

4.31 Dado n considere los n+1 números 1, 11, 111,..., $\underbrace{11..,11}$n +1*unos*

n+1 unos . Por el Principio de las casillas debe haber dos de ellos, digamos 11...11 | z h unos y 11...11 | z k unos , con i ? h <k ? n+1, que dejan el mismo resto al dividirlos entre n. Por lo tanto su diferencia, es decir 11...11 | z k?h unos 00...00 | z h ceros , es múltiplo de n.

4.15 Como la suma de sus cifras es 300, el número es divisible entre 3 pero no entre 9 y por lo tanto no puede ser un cuadrado perfecto.

4.38 Suponiendo que los números hayan sido correctamente codificados, el resultado $EEFF$ es múltiplo de 11 (pues $E-E+F-F=0$). Entonces al menos uno de los factores es múltiplo de 11. Pero los múltiplos de 11 de dos dígitos tienen ambas cifras iguales, mientras que los que escribió Pedro las tienen diferentes.

4.39 No. Cualquier número que se obtenga es congruente módulo 3 con la suma de los dígitos, que es $1+2\cdot 2+3\cdot 3+4\cdot 4+5\cdot 5+6\cdot 6+7\cdot 7=1+4+9+16+25+36+7^2=140\equiv 2 \pmod 3$, pero los cuadrados sólo pueden ser congruentes con 0 ó 1 módulo 3.

4.40 Como los cuadrados sólo pueden ser congruentes con 0 ó 1 módulo 3, m^2+n^2 será congruente con 0 módulo 3 sólo cuando lo sean m y n.

4.41 Con el algoritmo de Euclides se halla que $1=mcd(37,21)=4\cdot 37-7\cdot 21$, por lo tanto -7 es inverso multiplicativo de 21 (mod 37), de donde $x\equiv -7\cdot 21 x\equiv -7\cdot 2\equiv 23 \pmod{37}$ y la solución es $x=23$.

4.15 Un cuadrado no puede ser congruente con 2 módulo 3, ya que si $3|x$ entonces $x^2\equiv 0$ (mód 3) y si 3 no div a x entonces $x^2\equiv 1$ (mód 3). Entonces si ni x ni y fuesen múltiplos de 3 se tendría $z^2=x^2+y^2\equiv 2$ (mód 3), absurdo.

4.47 Como $2222=317\cdot 7+3$, $5555=793\cdot 7+4$ y $2222^6\equiv 5555^6\equiv 1 \pmod 7$,se tiene

$$2222^{5555}+5555^{2222}\equiv 3^{925\cdot 6+5}+4^{370\cdot 6+2}\equiv 3^5+4^2\equiv 259\equiv 0(mod 7)$$

4.48 Como $2^{16}\equiv 1 \pmod{17}$, busquemos el resto de dividir 3^{2011} entre 16.Como $\phi(16)=2^4-2^3=8$ se tiene $3^{2011}=3^{251\cdot 3+3}\equiv 3^3=27\equiv 11 \pmod{16}$, por lo tanto $2^{3^{2011}}\equiv 2^{11}=2^4\cdot 2^4\cdot 2^3\equiv (-1)(-1)8=8 \pmod{17}$.

4.49 Por el Teorema de Euler se tiene que $3^{\phi(10^{2012})}\equiv 1 \pmod{10^{2012}}$, por lo tanto la cifra de las unidades de $3^{\phi(10^{2012})}$ es un 1 y está precedida de al menos 2011 ceros. La misma prueba se aplica a cualquier primo p distinto de 2 y 5.

4.50 Por el Teorema de Euler $2^{\phi(5^j)}\equiv 1 \pmod{5^j}$, es decir que $2^{\phi(5^j)}$=A$\cdot 5^j+1$ para cierto natural A. Multiplicando por 2^j resulta $2^{\phi(5^j)}+j=A\cdot 10^j+2^j$, y basta escoger j suficientemente grande para que j supere en N al número de cifras de 2^j . Esto siempre es posible pues 2^j tiene $\left\lfloor log 10^{2^j}\right\rfloor+1\leq 1+j\cdot 10^2$ y $j-1-j\cdot log 10^2=-1+j\cdot log 10^5$ se puede hacer tan grande como queramos. Con el j adecuado, se toma la potencia de 2 de exponente $\phi(5^j)+j=4^j+j$. Una demostración similar se puede aplicar al caso $p=5$.

6.5 Capítulo 5

Soluciones del Capítulo 5

5.1 1) $x_0=8$; $y_0=-6$; $x=8+13k$; $y=-6-10k$
2) $x_0=15$; $y_0=45$; $x=15+3k$; $y=45+10k$

3) no tiene solución ya que (3:12) no div a 4.
4) $x_0 = 4$; $y_0 = -16$; $x = 4 + 6k$; $y = -16 - 25k$
5) $x_0 = 1$; $y_0 = -1$; $x = 1 + 6k$; $y = -1 - 7k$
6) $x_0 = -24$; $y_0 = 60$; $x = -24 + 5k$; $y = 60 - 12k$
7) no tiene solución ya que (40:-30) no div a 9.

5.1 a) Es posible ya que $(2:5)|21$.
b) Resolvemos la ecuación $2x + 5y = 21$
$x_0 = 42$; $y_0 = 21$; $x = -42 + 5k$; $y = 21 - 2k$
luego $x = -42 + 5k > 0$ y $y = 21 - 2k > 0$.

Resolviendo nos queda: $k = \{9, 10\}$, luego: las posibles soluciones son : $(x, y) = \{(3,3); (8,1)\}$
Entonces, 3 bidones de $2l$ y $5l$.
y 8 bidones de $2l$ y 1 bidón de $5l$.

5.2 $x \equiv 3$ (mód 4)
$x \equiv 3$ (mód 7)
$x \equiv 3$ (mód 11)
$x \equiv 1$ (mód 13)

$x \equiv 3$ (mód 4) $\Rightarrow$ $\quad x = 4t_1 + 3$
$x = 4t_1 + 3 \equiv 3$ (mód 7)
$4t_1 \equiv 0$ (mód 7)
$t_1 \equiv 0$ (mód 7)

$\boxed{t_1 = 7t_2}$

Volviendo $x = 4t_1 + 3 = 4 \cdot 7t_2 + 3 = 28t_2 + 3$

$28t_2 + 3 \equiv 3$ (mód 11)
$28t_2 \equiv 0$ (mód 11)
$t_2 \equiv 0$ (mód 11)

$\boxed{t_2 = 11t_3}$

Volviendo $x = 28 \cdot 11t_3 + 3 = 308t_3 + 3$

$x = 308t_3 + 3$

$308t_3 + 3 \equiv 1$ (mód 13)
$308t_3 \equiv -2$ (mód 13)
$308t_3 + 13 \equiv -2 + 13$ (mód 13)
$308t_3 \equiv 11$ (mód 13)
$9t_3 \equiv 11$ ya que $9 \cdot 7 \equiv 11$ (mód 13)

$t_3 \equiv 7$ (mód 13)

$\boxed{t_3 = 13t_4 + 7}$

Volviendo $x = 308 \cdot (13t_4 + 7) + 3 = 4004t_4 + 2159$

Por lo tando el menor número es el 2159 cuando $t_4 = 0$.

5.3

$$(x - 2yz)(x + 2yz) = 310 = 1 \cdot 2 \cdot \cdot 5 \cdot 31$$

luego los posibles valores de $x - 2yz$ y $x + 2yz$

$x - 2yz$	$x + 2yz$
± 1	± 310
± 2	± 155
± 5	± 62
± 10	± 31

Luego observamos que $(x - 2yz) \cdot (x + 2yz)$ es impar por regla de la paridad. Por lo tanto, No tiene Solución entera.

5.4

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 4 \\ x \equiv x_0 \pmod{12} \end{cases} \tag{6.1}$$

Aplicamos el terema Chino del resto: $x \equiv x_0$ (mod 12) ya que (3:4)=1
Resolviendo $x = 2 \cdot 4 \cdot 1 + 3 \cdot 3 \cdot 3 = 35$

$x \equiv 35$ (mod 12) $\Rightarrow$x $\equiv 11$ (mod 12)
Luego, $x = 12k + 11$ y buscamos k tal que

$$100 < 12k + 11 < 110$$

$$7,41 < k < 8,25$$

$\boxed{\text{k = 8}}$

Luego $x = 12{,}8 + 11 = 107$
La canasta tenía 107 manzanas.

5.5 $y.(3x + 2) = 7 \quad \Rightarrow \quad$ y = ± 1 y $3x + 2 = \pm 7$.
La única solución es $(x, y) = (-3, -1)$.

5.7

$$x^2 = 2 \cdot (x + y) - y^2$$

$$x \cdot x = (\sqrt{2 \cdot (x + y)} - y) \cdot (\sqrt{2 \cdot (x + y)} + y)$$

igualando factores $x=\sqrt{2\cdot(x+y)}-y$**(a)** $\quad x=\sqrt{2\cdot(x+y)}+y$**(b)**

(a)

$$x+y=\sqrt{2\cdot(x+y)}$$

llamamos $u=x+y$ y nos queda:

$$u=\sqrt{2\cdot u}$$

elevamos al cuadrado ambos miembros

$$u^2=2\cdot u$$

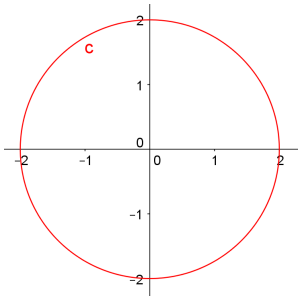
$$u^2-2\cdot u=0$$

resolviendo $u=0$ y $u=2$. Entonces tenemos la solución trivial $x+y=0$, o sea, $x=-y$

Reemplazo en la ecuación original $(-y)^2+y^2=2\cdot 0 \quad \Rightarrow \quad$ (x,y)=(0,0)

Para $u=2$

$x^2+y^2=4$ La solución son los puntos enteros de la circunferencia centrada en el origen de radio 2.



los únicos posibles valores son: $(x,y)=\{(2,0);(0,2);(-2,0);(0,-2)\}$

(b)

$$x-y=\sqrt{2\cdot(x+y)}$$

llamamos $u=x+y$ y $v=x-y$ nos queda:

$$v=\sqrt{2\cdot u}$$

elevamos al cuadrado ambos miembros

$$v^2=2\cdot u$$

$$v^2-2\cdot u=0$$

resolviendo $u=0$ y $u=v=2$. Que son la mismas soluciones ateriores.

5.9

$$x\cdot(2x+y)-3y^2=17$$

factorizando

$$\left[\sqrt{x(2x+y)}-\sqrt{3}y\right]\cdot\left[\sqrt{x(2x+y)}+\sqrt{3}y\right]=17$$

como $\left[\sqrt{x(2x+y)}-\sqrt{3}y\right] < \left[\sqrt{x(2x+y)}+\sqrt{3}y\right]$, la única posibilidad es que

$\left[\sqrt{x(2x+y)}-\sqrt{3}y\right] = 1$ (a) y $\left[\sqrt{x(2x+y)}+\sqrt{3}y\right] = 17$ (b)

sumando (a) y (b) resulta:

$$2\cdot\sqrt{x(2x+y)} = 18$$

Simplificando
$x(2x+y) = 81$ y como $81 = 3^4$ la pasibilidades son: $(x,y) = \{(1,81);(3,27)\}$.

5.10 Como 17 no tiene otra factorización posible que $17 = \pm 17\cdot\pm 1\cdot\pm 1$ y 17 no es cubo perfecto, la ecuación no tiene solución.

5.11

$$n^2-4n+16 = x^2$$

$$n^2-4n+4+12 = x^2$$

$$(n-2)^2+12 = x^2$$

$$(n-2)^2 = x^2-12$$

Despejando n

$$n = \sqrt{x^2-12}+2$$

llamamos $u^2 = x^2-12$ ya que el radicando debe ser cuadrado perfecto.
luego resulta que

$$x^2-u^2 = 12$$

$$(x-u)\cdot(x+u) = 1\cdot 2\cdot 2\cdot 3$$

$x-u$	$x+y$
1	12
2	6
3	4

Luego la única solución encontrada es $x = 4$ que verifica.

$$4^2-4\cdot 4+16 = 16 = 4^2$$

5.12

$$10y = 1234567-x^2$$

para que y sea entero el número de la derecha debe ser múltiplo de 10, o sea, $1234567-x^2 \equiv 0$ (mod 10).

$$7-x^2 \equiv 0(mod 10)$$

resolvienndo la ecuación de cogruencia de orden 2. se llega a la conclusión que no tiene solución.

Por lo tanto la ecuación no tiene solución entera.

5.13 No tiene solución entera y podemos justificarla de esta manera:

$$n^4 + 16m + 64m^2 - 64m^2 = 7993$$

$$(n^2)^2 + 2 \cdot 8 + (8m)^2 - 64m^2 = 7993$$

$$(n^2 + 8m)^2 - 64m^2 = 7993$$

$$(n^2 + 8m - 8m) \cdot (n^2 + 8m + 8m) = 7993$$

$$n^2 \cdot (n^2 + 16m) = 7993$$

Luego como 7993 es primo. $7993 = 1 \cdot 7993$ y como n $^2 < n^2 + 16m$.

Resulta:

$n^2 = 1$ y $n^2 + 16m = 7993$ y se demuestra que no tiene solución entera.

5.14

5.15

$$3^{x^2+y-1} - 3^{x^2+1} = 2^3 \cdot 3^5$$

$$3^{x^2+1} \cdot (3^{y-2} - 1) = 2^3 \cdot 3^5$$

y igualando factores $3^5 = 3^{x^2+1} \Rightarrow x^2 + 1 = 5$
$2^3 = 3^{y-2} - 1 \Rightarrow 3^2 = 3^{y-2}$
La solución es $(x, y) = (2, 4)$
Verificamos

$$3^{2^2+4-1} - 3^{2^2+1} = 1944$$

$$3^7 - 3^5 = 1944$$

5.16

$$5^x + 2 \cdot 2^x \cdot 3^x = 3^{2x} + 2^{2x}$$

$$5^x = (3^x)^2 + (2^x)^2 - 2 \cdot 2^x \cdot 3^x$$

$$5^x = (3^x - 2^x)^2$$

$$5^{x/2} = 3^x - 2^x$$

Luego por el momento x debe ser necesariamente par $(x = 2k)$

Entonces $5^k = 3^{2k} - 2^{2k}$ y para probar que: $5^k \equiv 3^{2k} - 2^{2k}$ (mód 3)

La única posibilidad que esta ecuación tenga solución es que k sea par
y $5^k \equiv 3^{2k} + 2^{2k} \equiv 2$ (mód 3).

5.17

$$x^2 - 3^y = 7$$

factorizando

$$(x - 3^{\frac{1}{2}y})(x + 3^{\frac{1}{2}y}) = 7$$

$$(x - 3^{\frac{1}{2}y})(x + 3^{\frac{1}{2}y}) = 1 \cdot 7 = 7$$

$$\begin{cases} (x - 3^{\frac{1}{2}y}) & = 1 \quad \textbf{(1)} \\ (x + 3^{\frac{1}{2}y}) & = 7 \quad \textbf{(2)} \end{cases} \tag{6.2}$$

sumando **(1)** y **(2)**.

$$2x = 8$$

$$\boxed{\text{x=4}}$$

luego

$$4 + 3^{\frac{1}{2}y} = 7$$

$$\boxed{\text{y=2}}$$

La única solución posible es $(x, y) = (4, 2)$.

5.23