Olimpiada Mexicana de Matemáticas

Veracruz

Enero de 2005

Índice general

Capítulo 1

Combinatoria

1.1. Permutaciones y Combinaciones

Definición 1. Dado $n \in \mathbb{N}$ denotaremos por $n!$ al producto de todos los números naturales menores o iguales que n; esto es,

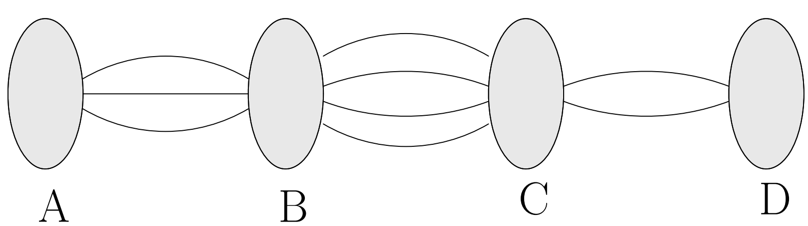
$$n! = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 3 \cdot 2 \cdot 1$$

Definición 2.

$$0! = 1$$

Principio 1. ***Fundamental de Conteo (P.F.C.)*** *Si existen m formas de que ocurra un evento A y n formas de que ocurra otro evento B distinto; el total de formas en que pueden ocurrir A y B juntos es $m \cdot n$.*

Ejemplo 1. Considere las ciudades A, B, C y D como se indica en la figura. Para ir de la ciudad A a la ciudad B existen 3 caminos, de B a C hay 4 caminos y de C a D sólamente se tienen 2 caminos. Calcule el número de rutas posibles para ir de A a D pasando por B y C y regresar sin usar sin utilizar alguno de los caminos utilizados al ir de A a D.



Solución. Por el **Principio Fundamental de conteo**, tenemos que las rutas posibles para ir de A a D son el número de caminos para ir de A a B por el número de caminos para ir de B a C por el número de caminos para ir de C a D; esto es:

$$A \longrightarrow D = 3 \cdot 4 \cdot 2 = 24$$

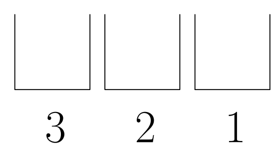
Ahora, como no podemos ocupar el mismo camino que esogimos para ir de A a D para regresar, tenemos que nos queda 1 camino para regresar de D a C, 3 caminos para regresar de C a B y 2 caminos para regresar de B a A; asi,

$$A \longleftarrow D = 2 \cdot 3 \cdot 1 = 6$$

Finalmente, usando una vez más el **Principio Fundamental de Conteo**, tenemos que las maneras en que podemos ir de A a D y regresar sin usar el mismo camino son 144 rutas.

Definición 3. Un arreglo de objetos en un **orden** determinado se llama una **permutación**.

Ejemplo 2. Si tenemos un conjunto de tres elementos $\{a, b, c\}$; determinar el número de permutaciones de esos tres elementos si no se repiten objetos.



Solución. Pensemos en el arreglo de los tres elementos en función de los lugares; es decir, cada arreglo consta de tres lugares; en el primero, podemos colocar cualquiera de los tres elementos que tenemos; en el segundo lugar sólo podemos colocar dos elementos (pues ya se ha colocado uno en el lugar anterior) y finalmente en el último lugar sólo podemos colocar un elemento; así, se tiene que, aplicando el Principio Fundamental de Conteo, la solución es 6 permutaciones.

Teorema 1. *El total de formas en que se pueden permutar n objetos tomados de n en n es*

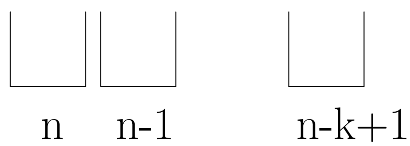
$$P_n^n = n!$$

Teorema 2. *El número de permutaciones de n objetos en k lugares está dado por*

$$P_k^n = \frac{n!}{(n-k)!}$$

para $k \leq n$.

Demostración. Volvamos a pensar en las permutaciones como acomodar n objetos en k lugares.



Es claro entonces que

$$\begin{aligned} P_k^n &= n \cdot (n-1) \cdot \ldots \cdot (n-k+1) \\ &= \frac{n \cdot (n-1) \cdot \ldots \cdot (n-k+1) \cdot (n-k) \ldots \cdot 2 \cdot 1}{(n-k)!} \\ &= \frac{n!}{(n-r)!} \end{aligned}$$

Ejemplo 3. De cuantas formas pueden sentarse 4 personas en un cuarto con nueve sillas diferentes?

Solución. Este problema lo podemos pensar de la iguiente manera: la primera persona puede elegir 9 sillas para sentarse; a la segunda persona sólo le quedan 8 sillas para escoger y así sucesivamente; de donde se ve que el resultado es

$$P_4^9 = \frac{9!}{(9-4)!} = \frac{9 \cdot 8 \cdot 7 \cdot 6 \cdot 5!}{5!} = 9 \cdot 8 \cdot 7 \cdot 6.$$

Definición 4. Una **combinación** de n objetos tomados de k en k es cualquier subconjunto de cardinalidad k de un conjunto de cardinalidad n.

Teorema 3. *El número de combinaciones de n objetos diferentes tomados de k en k, con $k \leq n$ es*

$$\binom{n}{k} = C_k^n = \frac{n!}{(n-k)! \cdot k!}$$

Teorema 4. *Para todo $n \in \mathbb{N}$, se tiene que*

$$C_0^n = 1 = C_n^n$$

Demostración.

$$C_0^n = \frac{n!}{(n-0)! \cdot 0!} = \frac{n!}{n!} = 1$$

$$C_n^n = \frac{n!}{(n-n)! \cdot n!} = \frac{n!}{0! \cdot n!} = 1$$

Teorema 5. *Para todo n y todo $k < n$, se tiene que*

$$C_k^n + C_{k+1}^n = C_{k+1}^{n+1}$$

Demostración.

$$\begin{aligned}
C_k^n + C_{k+1}^n &= \frac{n!}{(n-k)! \cdot k!} + \frac{n!}{[n-(k+1)]! \cdot (k+1)!} \\
&= \frac{n!}{(n-k)! \cdot k!} + \frac{n!}{(n-k-1)! \cdot (k+1)!} \\
&= \frac{n! \cdot (k+1) + n! \cdot (n-k)}{(n-k)! \cdot (k+1)!} \\
&= \frac{k \cdot n! + n! + n \cdot n! - k \cdot n!}{(n-k)! \cdot (k+1)!} \\
&= \frac{n! \cdot (n+1)}{(n-k+1-1)! \cdot (k+1)!} \\
&= \frac{(n+1)!}{[(n+1)-(k+1)]! \cdot (k+1)!} = C_{k+1}^{n+1}
\end{aligned}$$

Ejercicio 1.1. Pruebe que para todo n, $k \leq n$ *in* $\mathbb{N}$; se cumple que

$$\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}$$

Solución. Sea n en $\mathbb{N}$ y sea $P(k)$ la propiedad

$$\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}.$$

Es claro que $P(0)$ se cumple pues

$$\binom{n}{0} = \binom{n+0+1}{0} = \binom{n+1}{0}.$$

Supongamos que para $r \in \mathbb{N}$ es válida $P(r)$; esto es

$$\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+r}{r} = \binom{n+r+1}{r}.$$

Entonces

$$\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+r}{r} + \binom{n+r+1}{r+1} =$$
$$\binom{n+r+1}{r} + \binom{n+r+1}{r+1} = \binom{n+r+2}{r+1} = \binom{n+(r+1)+1}{r+1}.$$

Con el último teorema, podemos construir el **Triángulo de Pascal**

$$\begin{array}{ccccccccc}
 & & & & \binom{0}{0} & & & & \\
 & & & \binom{1}{0} & + & \binom{1}{1} & & & \\
 & & & & \downarrow & & & & \\
 & & \binom{2}{0} & + & \binom{2}{1} & + & \binom{2}{2} & & \\
 & & & \downarrow & & \downarrow & & & \\
 & \binom{3}{0} & & \binom{3}{1} & & \binom{3}{2} & & \binom{3}{3} & \\
\cdots & & \cdots & & \cdots & & \cdots & & \cdots
\end{array}$$

donde el renglón $n-'$ *esimo* (con $n \geq 0$) corresponde a los coeficientes del desarrollo del binomio $(x+y)^n$ como se verá a continuación.

Teorema 6. *(**Del Binomio de Newton**) Sean x y y dos números y sea n en $\mathbb{N}$. Entonces*

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^{n-i} y^i$$

Demostración. Para $n = 0$, se tiene que $(x+y)^0 = 1 = 1 \cdot 1 \cdot 1 = \binom{0}{0} x^{0-0} y^0$. Para $n = 1$,

$$(x+y)^1 = x + y = 1 \cdot x + 1 \cdot y = 1 \cdot x^1 y^0 + 1 \cdot x^0 y^1 = \binom{1}{0} x^{1-0} y^0 + \binom{1}{1} x^{1-1} y^1$$

Para $n = 2$,

$$\begin{aligned}(x+y)^2 &= x^2 + 2xy + y^2 = 1 \cdot x^2 y^0 + 2 \cdot x^1 y^1 + 1 \cdot x^0 y^2 \\ &= \binom{2}{0} x^{2-0} y^0 + \binom{2}{1} x^{2-1} y^1 + \binom{2}{2} x^{2-2} y^2.\end{aligned}$$

Supongamos entonces que para algún k en $\mathbb{N}$ se cumple que

$$(x+y)^k = \sum_{i=0}^{k} \binom{k}{i} x^{k-i} y^i$$

Entonces

$$\begin{aligned}(x+y)^{k+1} &= (x+y)^k (x+y) = \left(\sum_{i=0}^{k} \binom{k}{i} x^{k-i} y^i \right)(x+y) \\ &= \left[\binom{k}{0} x^k + \binom{k}{1} x^{k-1} y + \binom{k}{2} x^{k-2} y^2 + \cdots \right. \\ &\quad \left. + \binom{k}{k-1} x y^{k-1} + \binom{k}{k} y^k \right](x+y) \\ &= \left[\binom{k}{0} x^{k+1} + \binom{k}{1} x^k y + \binom{k}{2} x^{k-1} y^2 + \cdots \right. \\ &\quad \left. + \binom{k}{k-1} x^2 y^{k-1} + \binom{k}{k} x y^k \right] \\ &\quad + \left[\binom{k}{0} x^k y + \binom{k}{1} x^{k-1} y^2 + \binom{k}{2} x^{k-2} y^3 + \cdots \right. \\ &\quad \left. + \binom{k}{k-1} x y^k + \binom{k}{k} y^{k+1} \right] \\ &= \binom{k}{0} x^{k+1} + \left[\binom{k}{1} + \binom{k}{0} \right] x^k y + \left[\binom{k}{2} + \binom{k}{1} \right] x^{k-1} y^2 + \cdots \\ &\quad + \left[\binom{k}{k} + \binom{k}{k-1} \right] x y^k + \binom{k}{k} y^{k+1}.\end{aligned}$$

Usando los teoremas 4 y 5, podemos sustituir $\binom{k}{0}$ por $\binom{k+1}{0}$, $\binom{k}{k}$ por $\binom{k+1}{k+1}$ y cada suma $\left[\binom{k}{i} + \binom{k}{k-i}\right]$ por $\binom{k+1}{i}$ para $1 \leq i \leq k$; de tal manera que

$$\begin{aligned}(x+y)^{k+1} &= \left[\binom{k+1}{0}x^{k+1} + \binom{k+1}{1}x^k y + \cdots \right. \\ &\quad \left. + \binom{k+1}{k}xy^k + \binom{k+1}{k+1}y^{k+1}\right] \\ &= \sum_{i=0}^{k+1}\binom{k+1}{i}x^{(k+1)-i}y^i.\end{aligned}$$

Ejercicio 1.2. Considerense los 36 vértices de una cuadrícula perfecta de 6×6. Utilizando éstos como vértices de triángulos no degenerados; cuántos triángulos distintos se pueden formar?

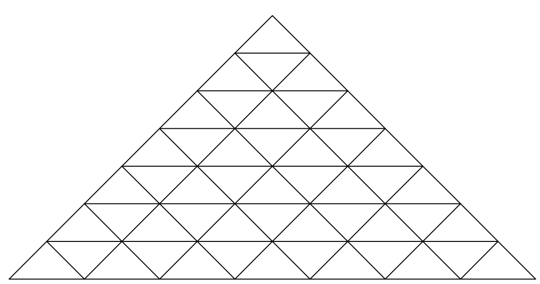
Teorema 7.

$$2^n = \sum_{i=0}^{n}\binom{n}{i}$$

Demostración.

$$2^n = (1+1)^n = \sum_{i=0}^{n}\binom{n}{i}1^{n-i}\cdot 1^i = \sum_{i=0}^{n}\binom{n}{i}.$$

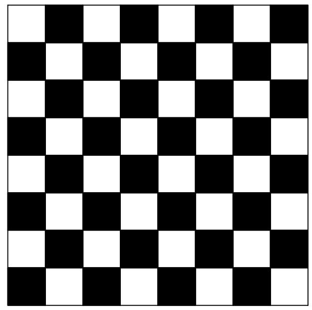
Ejercicio 1.3. Siguiendo las líneas de la figura, Cuantos caminos hay para ir del punto A al B que no pasen por el mismo vértice dos veces y que sólo avancen hacia abajo y hacia los lados pero no hacia arriba?



Ejemplo 4. De cuantas formas pueden ponerse 8 torres en un tablero de ajedrez sin que se ataquen

Solución. En la primera columna, hay 8 cuadros en los que se puede poner una torre.

$8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

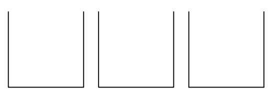


En la segunda columna, sólo quedan 7 lugares para poner una torre, debido a las condiciones del problema; si seguimos este reazonamiento, obtenemos que el número de formas es igual a $8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$.

Ejercicio 1.4. De cuantas formas podemos poner 2 torres sin que se ataquen?

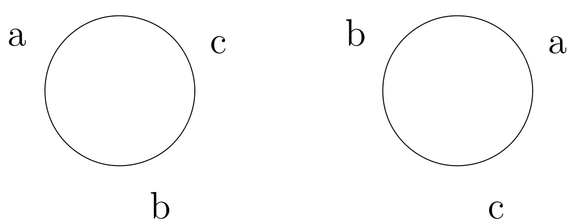
Definición 5. Llamamos **Permutaciones Cíclicas** al número de formas diferentes de acomodar n objetos en círculo y lo denotamos por PC_n.

Para observar la diferencia entre las **permutaciones** y las **permutaciones cíclicas**, observemos el ejemplo con tres objetos:



3 2 1

De donde $P_3^3 = 6$; cuando contamos de esta manera, el arreglo (a, b, c) es diferente de (c, a, b); sin embargo, cuando pensamos en los mismos objetos acomodados en círculo, es claro que son iguales



ya que la a está a la derecha de la c y la b a la derecha de la a en ambos dibujos; entonces, la manera de obtener una fórmula para PC_n es encontrar número de acomodar n objetos en n lugares (que eso es $P_n^n = n!$) y dividir entre n, ya que, dado un arreglo, este se repite n veces (por los n lugares en los que se puede acomodar el arreglo rotándolo); así, se tiene que

$$PC_n = \frac{n!}{n} = \frac{n \cdot (n-1)!}{n} = (n-1)!$$

Ejemplo 5. En un kinder se ponen a bailar a 7 niños en círculo. De cuántas formas se pueden colocar estos niños en el círculo?

Solución. Por lo anterior, el número buscado está dado por

$$PC_7 = 6! = 720$$

; esto es, hay 720 formas de acomodar a los niños.

Ejemplo 6. En la Olímpiada Veracruzana de Maemáticas de 1993 participaron 80 personas; Decuantas formas pudieron haberse repartido los premios? En ese entonces se otorgaban 6 primeros lugares, 6 segundos y 6 terceros.

Solución. Pensemos en un principio cómo pudieron repartirse los primeros lugares; como no importa si una persoana es el "primer" primer lugar o el "último" primer lugar, se puede inferir que no importa el orden en que se acomodan a las personas en los primeros lugares, así que tenemos que escoger 6 personas de 80 sin importar el orden; esto se hace de $\binom{80}{6}$ formas; ahora, como ya se acomodaron a 6 personas, para poner en los segundos lugares, nos quedan 74 personas; siguiendo el mismo razonamiento que para los primeros lugares, se tienen $\binom{74}{6}$ formas de llenar los segundos lugares y $\binom{68}{6}$ formas de llenar los terceros lugares.

1eros.	2os.	3eros.
$\binom{80}{6}$	$\binom{74}{6}$	$\binom{68}{6}$

Y finalmente, por el principio de conteo, el número de formas de repartir los premios es

$$\binom{80}{6} \cdot \binom{74}{6} \cdot \binom{68}{6} \quad .$$

Definición 6. Cuando se acomodan n objetos en k lugares con la opción de repetir los objetos, tenemos **Permutaciones con repretición**, las cuales se denotan $\bar{P}_k^n$.

Ejemplo 7. Cuantas placas de autos se pueden hacer si se usan 3 letras y 4 números? Tómese en cuenta que se tienen las letras de la A a la Z (excepto CH, LL y N) y los números del 0 al 9, pero que no existen placas con el número 0000.

Solución. Se tienen tres lugares para acomodar letras; en el primer lugar se pueden poner 26 letras; como se pueden repetir los objetos, en el segundo lugar también se pueden poner 26 letras y análogamente en el tercer lugar.

26	26	26	10	10	10	9

Con los números pasa algo parecido; en los tres primeros lugares se pueden poner 10 números en cada uno; sin embargo, en el cuarto lugar ya no se puede poner el cero (pues entonces estaríamos contando al 0000); por lo que sólo se pueden poner ahí los números del 1 al 9; por el P.F.C., al multiplicar todos estos números se obtiene el número de placas.

Ejercicio 1.5. Se tienen objetos de k tipos diferentes. Cuántas permutaciones de n elementos con $n = n_1 + n_2 + \cdots + n_k$, se pueden hacer tomando n_1 elementos del 1er. tipo, n_2 elementos del 2o. tipo, ..., n_k elementos del k-ésimo tipo?

Ejemplo 8. Encontrar todos los números de cinco cifras que además sean ascendentes.

Solución. El número más pequeño que podemos formar es 12345 y el mayor número es 56789; entonces tenemos que para todo n que cumpla las condiciones del problema, $12345 \leq n \leq 56789$. Ahora, si tomamos 5 cifras cualesquiera, se puede formar uno y sólo un número como los que queremos (por ejemplo, si elegimos 7,4,9,2,1, de todos los números que se pueden formar con estas cifras, el único que cumple las condiciones que se requieren es 12479); por lo cual el resultado es $\binom{9}{5}$.

Ejercicio 1.6. Se tiene una cuadrícula de 6×9 cuadros y se toman 25 triángulos cuyos vértices son los de la cuadrícula. Demostrar que existen al menos dos triángulos con un vértice en común.

Capítulo 2

Teoría de Números

2.1. Los enteros

$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$

- $\forall\ a \in \mathbb{Z}, a + b = b + a$;
- $\forall\ a, b, c \in \mathbb{Z}, a + (b + c) = (a + b) + c$;
- $\exists_1\ 0 \in \mathbb{Z}$ tal que $\forall\ a \in \mathbb{Z}, a + 0 = a$;
- $\forall\ a \in \mathbb{Z}, \exists_1\ -a$ tal que $a + (-a) = 0$;
- $\forall\ a, b \in \mathbb{Z}, a \cdot b = b \cdot a$;
- $\forall\ a, b, c \in \mathbb{Z}, a \cdot (b \cdot c) = (a \cdot b) \cdot c$;
- $\exists_1\ 1 \in \mathbb{Z}$ tal que $\forall\ a \in \mathbb{Z}, 1 \cdot a = a$;
- $\forall\ a, b, c \in \mathbb{Z}, a \cdot (b + c) = a \cdot b + a \cdot c$.

Teorema 8. *Para todo $a \in \mathbb{Z}, a \cdot 0 = 0$*

Demostración. Sea $a \in \mathbb{Z}$; $a \cdot 0 \in \mathbb{Z}$; pero $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ y sabemos que existe $-(a \cdot 0)$ tal que $a \cdot 0 + [-(a \cdot 0)] = a \cdot 0 + (-a \cdot 0) = 0$; así, $a \cdot 0 + (-a \cdot 0) = a \cdot 0 + a \cdot 0 + (-a \cdot 0)$; donde ya sabemos que el miembro izquierdo de la igualdad es cero y el de la derecha lo podemos desarrollar como: $a \cdot 0 + a \cdot 0 + (-a \cdot 0) = a \cdot 0 + 0$; por lo que obtenemos que $0 = a \cdot 0 + 0 = a \cdot 0$. ■

$\mathbb{N} \subset \mathbb{Z}$
$a < b$ si y solo si $\exists\ c \in \mathbb{N} - \{0\}$ tal que $a + c = b$

2.2. Propiedad de Tricotomía

Dado $a \in \mathbb{Z}$ puede suceder únicamente una de las 3 posibilidades siguientes:

- $a > 0$;
- $a = 0$;
- $a < 0$

Teorema 9. *Si $a < c$, entonces $a + b < c + b$.*

Demostración. $a < c$ si y sólo si $\exists\ d \in \mathbb{N} - \{0\}$ tal que $a + d = c$; entonces $a+d+b = c+b$, lo cual podemos ver de la siguiente manera:$(a+b)+d = c+b$ de lo cual podemos concluir que $a + b < c + d$. ■

Teorema 10. *Si $a + b < c + b$ entonces $a < c$*

Demostración. $a + b < c + b$ implica que $a + b + (-b) < c + b + (-b)$, lo cual lo podemos ver como $a < c$. ■

2.3. Divisibilidad

Definición 7. Si a y b son enteros, decimos que a **divide a** b (en símbolos, $a \mid b$) si es posible encontrar un entero x de tal manera que $ax = b$.

Propiedades

(I) Para a y b enteros, $a \,\Big|\, b$ si y sólo si $|a| \,\Big|\, |b|$.

(II) Si $a \,\Big|\, b$ y $b \neq 0$, entonces $|a| \leq |b|$.

(III) Para todo entero a se tiene que $a \,\Big|\, a$.

(IV) Si a, b y c son enteros tales que $a \,\Big|\, b$ y $b \,\Big|\, c$, entonces $a \,\Big|\, c$.

(v) Es posible que $a \mid b$ pero que $b \nmid a$.

(vi) Para a y b enteros, $a \mid b$ y $b \mid a$ si y sólo si $|a| = |b|$.

Proposición 1. *Para a, b y c enteros, $a \mid b$ y $a \mid c$ si y sólo si $a \mid rb + sc$ para cualesquiera r y s enteros.*

Demostración. $\Leftarrow \lrcorner$ Si a divide a cualquier combinación lineal de b y c entonces $a|(bx+cy)$ para cualesquiera enteros x y y.En particular $a|(b\cdot 1+c\cdot 0)$ y $a|(b \cdot 0 + c \cdot 1)$; esto es $a|b$ y $a|c$.

$\Rightarrow \lrcorner$ P.D. $a \mid b$, $a \mid c \Rightarrow a \mid (bx + cy) \forall\ x, y \in \mathbb{Z}$.

$a \mid b$ implica que $\exists\ k \in \mathbb{Z}$ tal que $ak = b$, por lo que $akx = bx$ y análogamente $\exists\ m \in \mathbb{Z}$ tal que $am = c$, por lo que $amy = cy$. De esto podemos obtener que $bx + cy = akx + amy = a(kx + my)$; por lo tanto, $a \mid (bx + cy)$. ■

Corolario 1. *Si a, b, c son enteros tales que $a \mid b$ y $a \mid c$ entonces $a \mid (b + c)$*

Demostración. Como $a \mid b$ y $a \mid c$, existen enteros x y y tales que $b = ax$ y $c = ay$. Entonces $b + c = ax + ay = a(x + y)$, es decir, $a \mid (b + c)$. ■

Definición 8. Si b y c son enteros, todo número que pueda expresarse en la forma $rb + sc$ con r y s enteros, se llama **combinación lineal** de b y c.

Ejemplo 9. Probar que ningún número impar es combinación lineal de 4 y 6.

Solución. Aplicamos la proposición 1 con $a = 2$, $b = 4$ y $c = 6$. Supongamos que un cierto número impar h es combinación lineal de 4 y 6; entonces, utilizando la proposición 1, tenemos que $2 \mid h$, lo cual es falso pues h es impar. De aquí concluimos que no es posible que h sea combinación lineal de 4 y 6. ■

Ejemplo 10. Pruébese que si $c = 30n + 6$ (n entero), entonces c no es combinación lineal de 1020 y 210.

Solución. Podemos ver que $10 \mid 1020$, que $10 \mid 210$ pero $10 \nmid 30n + 6$ y por la proposición 1, eso nos dice que c no es combinación lineal de 1020 y 210.

Corolario 2. *Si b, c y d están relacionados por la ecuación $b + c = d$, y un número a es divisor de cualesquiera dos de ellos, entonces también lo es del tercero.*

Ejercicios

Ejercicio 2.1. Aplicar la proposición 1 para probar los resultados siguientes:

(i) La suma de dos números pares es también un número par.

(ii) La suma de un número par con un número impar es impar.

(iii) el producto de un número par con cualquier otro entero es un número par.

Ejercicio 2.2. Expresar 1 como combinación lineal de 3 y 4 de tres formas distintas.

Ejercicio 2.3. Expresar -20 como combinación lineal de -7 y 4.

Ejercicio 2.4. Es posible utilizar la proposición 1 para decidir si 22 es combinación lineal de 60 y 14 ? (Si es posible, poner la combinación lineal encontrada y si no, explicar porqué no es posible.)

Ejercicio 2.5. Deducir de la proposición 1 que si $a \mid b$, entonces a divide a cualquier múltiplo de b.

2.4. Primos

Definición 9. Decimos que un entero $p \neq \pm 1$ es **primo** si sus únicos divisores son ± 1 y $\pm p$.

Un entero no cero y distinto de ± 1 es **compuesto** si no es primo. Los enteros 1 y -1 no son primos ni compuestos, se llaman **unidades** y al número 0 no se le considera dentro de ninguna de estas categorías.

Teorema 11. ***Fundamental de la Aritmética (primera parte).*** *Todo entero distinto de* 0 *y de* ± 1 *es producto de primos.*

Existe una demostración por inducción que no se desarrollará en estas notas.

Nota. Al escribir un número entero como producto de primos, se acostumbra poner primero el signo del número y después escribir sólo primos positivos en orden creciente de magnitud, agrupando los primos que son iguales en la potencia correspondiente. A esta forma la llamaremos la **descomposición canónica** del número. Por ejemplo, la descomposición canónica de -180 es $-2^2 3^2 5$.

Necesitamos saber cómo decidir si cierto número es primo o no; para esto, basta ver que si un número positivo a es producto de dos divisores positivos, entonces alguno de ellos debe ser menor o igual que $\sqrt{a}$ (pues el producto de dos números positivos mayores que $\sqrt{a}$ es mayor que a), de donde surge el siguiente lema.

Lema 1. *Sea a un número entero mayor que 1 con la propiedad de que ningún número primo menor o igual que $\sqrt{a}$ lo divide. Entonces a es primo.*

Ejemplo 11. Determinar si 1517 es un número primo o no.

Solución. Aplicando el lema, no necesitamos conocer todos los primos del 1 al 1517; bastará conocer todos los primos menores que $\sqrt{1517}$ y revisar si alguno de ellos es divisor de 1517. Como $40^2 = 1600$, basta considerar los primos menores que 40. Al hacer la división de 1517 con cada uno de éstos, vemos que 37 es el único que sí lo divide (y que $1517 = 37 \times 41$), por lo que 1517 no es primo. ■

Se enunciarán ahora algunos criterios de divisibilidad por números pequeños.

- **Criterio de divisibilidad por 2.** Un entero a es divisible por 2 si y sólo si a termina en 0, 2, 4, 6 y 8.

- **Criterio de divisibilidad por 3.** Un entero a es divisible por 3 si y sólo si la suma de las cifras de a es divisible por 3. (Por ejemplo, 474 es divisible por 3 pues $4 + 7 + 4 = 15$ y 15 es múltiplo de 3.)

- **Criterio de divisibilidad por 4.** Un entero a es divisible por 4 si y sólo si el número formado por las dos últimas cifras de a lo es. (Por ejemplo, 7923 no es divisible por 4 ya que 23 no es múltiplo de 4.)

- **Criterio de divisiblidad por 5.** Un entero a es divisible por 5 si y sólo si termina en 0 ó 5.

- **Criterio de divisibilidad por 6.** Un entero a es divisible por 6 si y sólo si a es divisible por 2 y por 3.

- **Criterio de divisibilidad por 8.** Un entero a es divisible por 8 si y sólo si el número formado por las últimas tres cifras de a lo es. (Por ejemplo, 27 256 es divisible por 8 pues 256 lo es.)

- **Criterio de divisibilidad por 9.** Un entero a es divisible por 9 si y sólo si la suma de las cifras de a es divisible por 9. (Por ejemplo, 37 6831 no es múltiplo de 9 pues $3+7+6+8+3+1=28$, que no es múltiplo de 9.)

- **Criterio de divisibilidad por 10.** Un entero a es divisible por 10 si y sólo si a termina en 0.

- **Criterio de divisibilidad por 11.** Un entero a es divisible por 11 si y sólo si la diferencia de la suma de las cifras en posición impar de a menos la suma de las cifras en posici"on par de a es divisible por 11. (Por ejemplo, 78 425 397 248 sí es divisible por 11 pues $(8+2+3+7+4)-(7+4+5+9+2+8)=24-35=-11$, que es divisible por 11.)

Existen diversos criterios de divisibilidad por 7, pero ninguno de ellos es realmente práctico como los que se mencionan arriba.

Ejercicios

Ejercicio 2.6. Encontrar la descomposición canónica de 6 916.

Ejercicio 2.7. Encotnrar la descomposición canónica de $-6\,511\,131$.

2.5. Algoritmo de la División

Teorema 12. ***Algoritmo de la División.*** *Dados dos enteros a y b con $b \neq 0$, existen enteros únicos q y r de tal forma que*

$$a = bq + r \ , \quad \textit{con} \quad 0 \leq r < |b| \ .$$

El número q en la proposición anterior es el **cociente** (de la división de a entre b) y el número r es el **residuo** (de la división de a entre b).

La prueba del **Algoritmo de la División** puede hacerse por casos, siendo ilustrativa en cuanto a la manera usual de resolver los ejmplos particulares.

Observación. Si a y b son enteros y $b \neq 0$, entonces $b \mid a$ si y sólo si el residuo r de la división de a entre b es 0.

Ahora definiremos el **máximo común divisor (mcd)**.

Definición 10. Sea $n \geq 2$ un natural. Dada una sucesión de enteros no cero $a_1, a_2, \ldots, a_n$, su **máximo común divisor**, en símbolos $mcd(a_1, a_2, \ldots, a_n)$ es el mayor de los divisores comunes a todos ellos; es decir, $d = mcd(a_1, a_2, \ldots, a_n)$ si

(I) $d \mid a_1$, $d \mid a_2$, $\ldots$, $d \mid a_n$.

(II) Para cualquier c tal que $c \mid a_1$, $c \mid a_2$, $\ldots$, $c \mid a_n$, se tiene que $c \leq d$.

Se estudiarán a continuación algunas propiedades del máximo común divisor de dos números; la genralización al caso $n > 2$ es sencilla usando la fórmula recursiva

$$mcd(a_1, a_2, \ldots, a_n) = mcd(a_1, mcd(a_2, \ldots, a_n)$$

Propiedades

Sean a y b enteros no cero. Entonces

(I) $mcd(a, b) = mcd(|a|, |b|)$;

(II) $mcd(a, b) > 0$;

(III) si $a \mid b$, entonces $mcd(a, b) = |a|$;

(IV) si $d = mcd(a, b)$, $a = da'$ y $b = db'$ (es decir, a' y b' son los respectivos cocientes de a y b entre d), entonces $mcd(a', b') = 1$.

Definición 11. Si $mcd(a, b) = 1$, decimos que a y b son **primos relativos** o **primos entre sí**.

Lema 2. *Sean a y b enteros no cero con $b \nmid a$. Si q y r son enteros tales que $a = bq + r$, entonces $mcd(a, b) = mcd(b, r)$.*

Teorema 13. ***Algoritmo de Euclides****.Sean a y b enteros no cero. Entonces $mcd(a, b)$ es combinación lineal de a y b.*

Demostración. Queremos demostrar que dados dos enteros a y b, existen enteros c y d tales que $(a, b) = ac + bd$.

Supongamos lo contrario; es decir, que para cualquier par de enteros x, y se tiene que $(a, b) \neq ax + by$; por lo cual $ax + by$En particular, $a \cdot 1 + b \cdot 0$. ■

Corolario 3. *Sean a y b dos enteros no cero y sea d su máximo común divisor. Entonces cualquier divisor común de a y de b, también lo es de d.*

Demostración. Como c divide a a y a b, también divide a cualquier combinación lineal de ellos, en particular a d. ■

El siguiente corolario nos dice qué números pueden ser combinación lineal de dos enteros a y b diferentes de cero.

Corolario 4. *Sean a y b enteros no cero y sea d su máximo común divisor. Un número c es combinación lineal de a y b si y sólo si es múltiplo de d; es decir, d es la mínima combinación lineal positiva de a y b*

Corolario 5. *Todo entero a puede expresarse como combinación lineal de* 2 *números primos p y q.*

Demostración. Siendo que el 1 es el único divisor de b y c, se tiene que $1 = px+qy$ con x y y enteros; si multiplicamos esta ecuación por a obtenemos $a = p(ax) + q(ay)$ con ax y ay enteros. ■

Ejemplo 12. Determinar si 7 y 20 son combinación lineal de 12 y 28; en caso afirmativo, escribir una combinación lineal en cada caso.

Solución. Como $mcd(12, 28) = 4$ y $4 \nmid 7$, entonces 7 no es combinación lineal de 12 y 28. Por otro lado, 20 sí es múltiplo de 4. Además, es fácil expresar 4 como combinación lineal de 12 y 28 (.ªl tanteo”): $4 = 12(-2) + 28(1)$. Multiplicando por 5 esta ecuación, obtenemos $20 = 12(-10) + 28(5)$. ■

Ejercicios

Ejercicio 2.8. Escribir el máximo común divisor de 99 y 68 como combinación lineal de estos números.

Ejercicio 2.9. Determinar si 15, -9 y 61 son combinación lineal de -24 y 93; en caso afirmativo, escribir una combinación lineal para cada caso.

Ejercicio 2.10. Determinar si 156, -12 y 60 son combinación lineal de 132 y -92; en caso afirmativo, escribir una combinación lineal para cada caso.

Corolario 6. *Sean a, b y c enteros. Si $a \mid bc$ y a y b son primos relativos, entonces $a \mid c$.*

Demostración. Sean r y s enteros tales que $ar + bs = 1$ y multipliquemos esta ecuación por c: $a(rc) + s(bc) = c$. Como $a \mid arc$ y $a \mid sbc$, entonces $a \mid c$. ■

Corolario 7. *Si p es un número primo, $b_1, b_2, \ldots, b_r$ son enteros y $p \mid b_1 b_2 \cdots b_r$, entonces p divide a alguna de las b_i.*

La prueba de este corolario puede hacerse por inducción sobre r.

Nota. el resultado anterior no es cierto si no pedimos que p sea un número primo; es decir, es posible que un número divida a un producto sin que divida a ninguno de sus factores; por ejemplo, $6 \mid 4 \times 3$.

Teorema 14. *Todo entero distinto de 0 y de ± 1 es producto de primos en forma única salvo orden y signo.*

Corolario 8. *Sean $a = \pm p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ y $b = \pm p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}$, donde $p_1 < p_2 < \cdots < p_k$ son primos positivos y los r_i y s_j son enteros no negativos. Entonces $a \mid b$ si y sólo si para toda $i = 1, \ldots, k$, se tiene que $r_i \leq s_i$*

Corolario 9. *Sean a y b como en el corolario 8 y sea $d = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}$ donde, para cada i, $t_i = min\{r_i, s_i\}$. entonces $d = mcd(a, b)$.*

Demostración. Por el corolario 8, es claro que d es diviosr común de a y b. Para ver que es el mayor, consideremos otro divisor común c. También por el corolario, $c = p_1^{u_1} p_2^{u_2} \cdots p_k^{u_k}$ con cada $u_i \leq r_i$ y $u_i \leq s_i$, pero entonces, $u_i \leq t_i$ para toda i, así que $c \mid d$; de donde $c \leq d$. ■

Nota. De la demostración anterior, podemos concluir que el máximo común divisor d de dosnúmeros no cero a y b, está caracterizado por las siguientes propiedades:

(I) $d \mid a$, $d \mid b$ y

(II) si $c \mid a$ y $c \mid b$, entonces $c \mid d$.

La segunda condición implica que el mcd de una pareja de números es único.

2.6. Sucesiones

Definición 12. La sucesión de Fibonacci (cuyos términos denotaremos por $f_1, f_2, \ldots$) se define como sigue:

$f_1 = 1,\ f_2 = 1,$

y para $n \geq 3$,

$f_n = f_{n-1} + f_{n-2}.$

Ejemplo 13. Probar que 9 divide a una infinidad de términos de la Sucesión de Fibonacci.

Solución. Llamaremos r_i al residuo de dividir f_i entre 9 con $i \in \mathbb{N} - \{0\}$; es claro que cuando 9 divida a f_i, r_i será cero.

Entonces tenemos: $r_1 = 1$,$r_2 = 1$,$r_3 = 2$,$r_4 = 3$,$r_5 = 5$,$r_6 = 8$,$r_7 = 4$,$r_8 = 3$,$r_9 = 7$,

Ejercicios

Ejercicio 2.11. Pruebe que 2 enteros cualesquiera positivos consecutivos son primos entre sí.

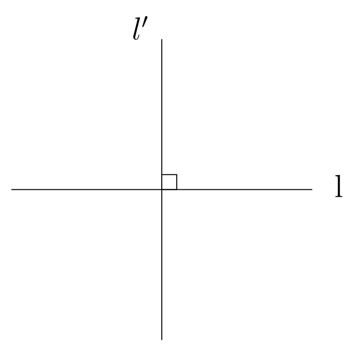
Ejercicio 2.12. Encuentre los enteros positivos n tales que $(n+1) \mid (n^2+1)$

Capítulo 3

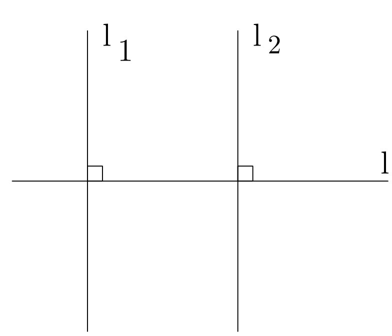
Geometría

3.1. Rectas coincidentes

Definición 13. Si dos rectas l y l' forman un ángulo de $90°$, decimos que son perpendiculares y se denota por $l \perp l'$.



Definición 14. Se dice que dos rectas l_1 y l_2 son **paralelas** si y sólo si existe una recta l tal que $l_1 \perp l$ y $l_2 \perp l$.



Axioma. *Por un punto exterior a una recta pasa una única paralela a ella.*

Teorema 15. *Sea l una recta y sea P un punto que no está en la recta l, entonces por P pasa una única perpendicular a l.*

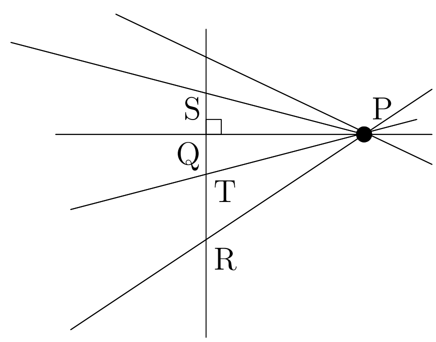
Teorema 16. *Si por un punto exterior a una recta trazamos una perpendicular y varias oblicuas; se verifica que:*

i) *El segmento de perpendicular que está comprendido entre el punto y la recta es menor que cualquier segmento de oblicua.*

ii) *Los segmentos de oblicuas cuyos pies equidistan del pie de la perpendicular son iguales.*

iii) *De dos segmentos de oblicuas cuyos pies no equidistan del pie de la perpendicular es mayor el que dista más.*

Si aplicamos el teorema anterior a la figura



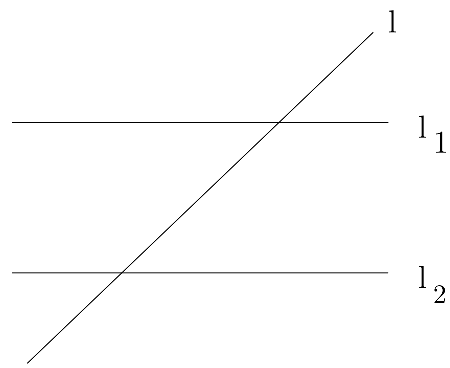
tenemos que:

i) $PQ < PR$

ii) $PS = PT$

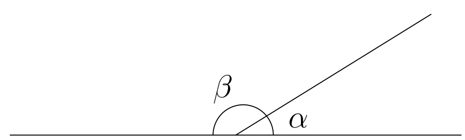
iii) $PT > PS$

Definición 15. Si una recta l corta dos líneas l_1 y l_2 se llama **secante**.

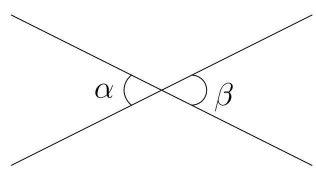


3.2. Ángulos

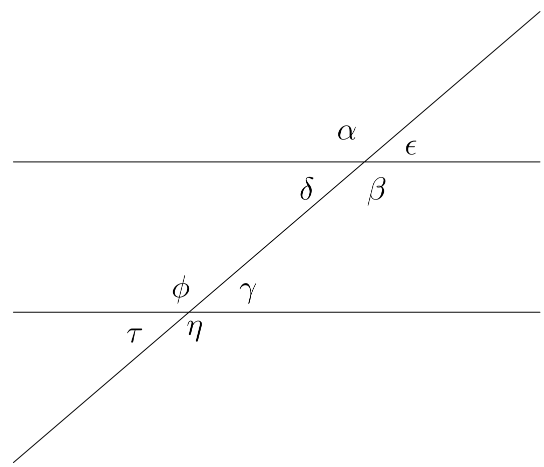
Definición 16. Dos ángulos adyacentes que tienen su lado común sobre una misma recta se llaman **suplementarios**.



Teorema 17. *Si α y β son ángulos opuestos por el vértice, entonces $\alpha = \beta$.*



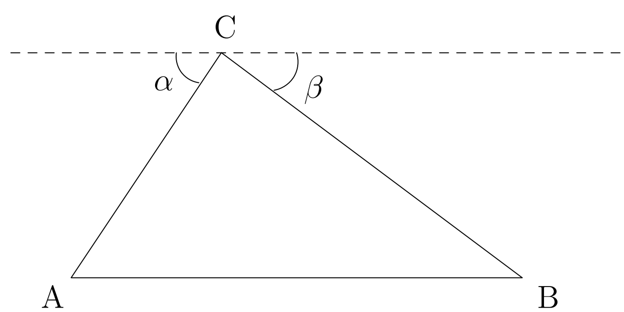
Ángulos entre paralelas cortadas por una secante:



Angulos Alternos Internos	$\angle\,\delta$, $\angle\,\gamma$	Iguales
	$\angle\,\beta$, $\angle\,\phi$	
Angulos Alternos Externos	$\angle\,\epsilon$, $\angle\,\tau$	
	$\angle\,\alpha$, $\angle\,\eta$	
Angulos Colaterales Internos	$\angle\,\delta$, $\angle\,\phi$	Suplementarios
	$\angle\,\beta$, $\angle\,\gamma$	
Angulos Colaterales Externos	$\angle\,\alpha$, $\angle\,\tau$	
	$\angle\,\epsilon$, $\angle\,\eta$	
Correspondientes	$\angle\epsilon$, $\angle\gamma$	Iguales
	$\angle\alpha$, $\angle\phi$	
	$\angle\delta$, $\angle\tau$	
	$\angle\beta$, $\angle\eta$	

3.3. Triángulos

Teorema 18. *Los ángulos interiores de un triángulos suman* $180°$



Demostración. Sea ABC un triángulo cualquiera. Tracemos una paralela a AB que pase por C. Sea α el ángulo formado por el lado AC y la paralela y sea β el ángulo formado por el lado BC y la paralela.

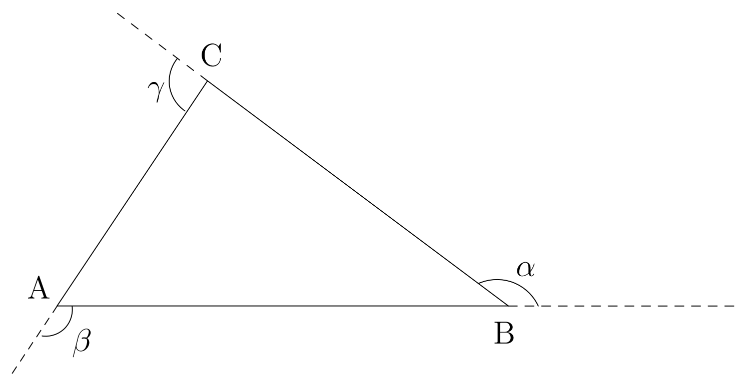
Observemos que

$$\angle\,\alpha + \angle\,BCA + \angle\,\beta + 180°$$

Además tenemos que $\angle\,\alpha = \angle\,CAB$ y $\angle\,\beta = \angle\,ABC$, por lo tanto

$$\angle\,CAB + \angle\,BCA + \angle\,ABC = 180°.$$

Corolario 10. *Los ángulos exteriores de un triángulo suman* 360°



Demostración. Sea ABC un triángulo cualquiera. Prolongamos AB y sea α el ángulo exterior en B. Es claro que $\angle\,ABC + \angle\,\alpha = 180°$. Además, por el teorema anterior tenemos que $\angle\,CAB + \angle\,BCA + \angle\,ABC = 180°$, de donde

$$\angle\,\alpha = \angle\,CAB + \angle\,BCA$$

Análogamente, si β y γ son los ángulos exteriores en A y C respectivamente, sabemos que

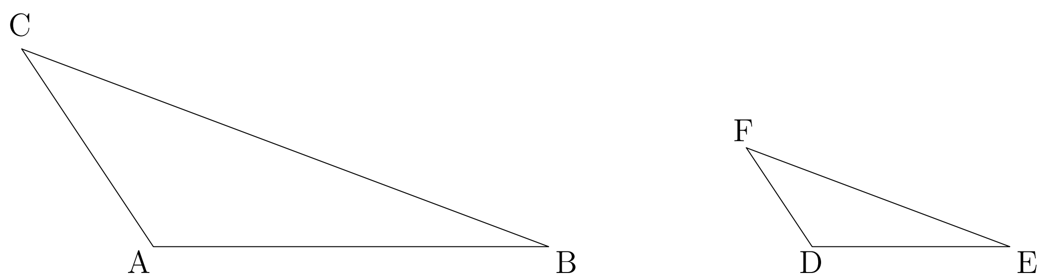
$$\begin{aligned}\angle\,\beta &= \angle\,BCA + \angle\,ABC\\ \angle\,\gamma &= \angle\,CAB + \angle\,ABC.\end{aligned}$$

Así,

$$\begin{aligned}\angle\,\alpha + \angle\,\beta + \angle\,\gamma &= \angle\,CAB + \angle\,BCA + \angle\,BCA + \angle\,ABC\\ &\quad + \angle\,CAB + \angle\,ABC\\ &= 2(\angle\,CAB + \angle\,BCA + \angle\,ABC)\\ &= 360°\end{aligned}$$

3.4. Criterios de Semejanza

Definición 17. Dos triángulos son **semejantes** si y sólo si tienen ángulos iguales y los lados correspondientes proporcionales.



Decimos que el triángulo ABC es semejante al triángulo DEF ($\triangle ABC \sim \triangle DEF$) si y sólo si se cumplen las siguientes condiciones:

i) $\angle CAB = \angle FDE$
$\angle ABC = \angle DEF$
$\angle BCA = \angle EFD$

ii) $\dfrac{CA}{FD} = \dfrac{AB}{DE} = \dfrac{BC}{EF}$

Sin embargo, no se necesita verificar que todas las condiciones se cumplen gracias al siguiente teorema:

Teorema 19. *Dos triángulos son semejantes si y sólo si*

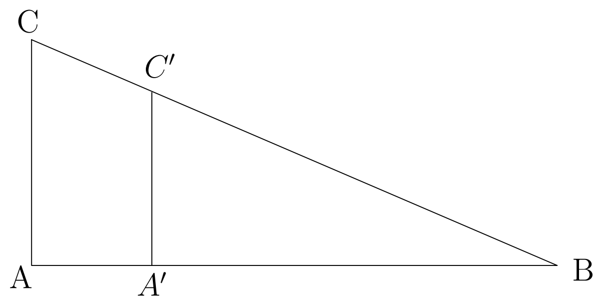
i) Tienen dos ángulos iguales

ii) Tienen sus tres lados proporcionales

iii) Tienen un ángulo igual y los lados que lo forman son proporcionales.

Las tres condiciones del teorema anterior son conocidas como los **criterios de semejanza**.

Ejercicio 3.1. Sean los triángulos ABC y $A'BC'$ tales que $AC \,||\, A'C'$ y $\angle CAB = \angle C'A'B = 90^\circ$ como se muestra en la siguiente figura

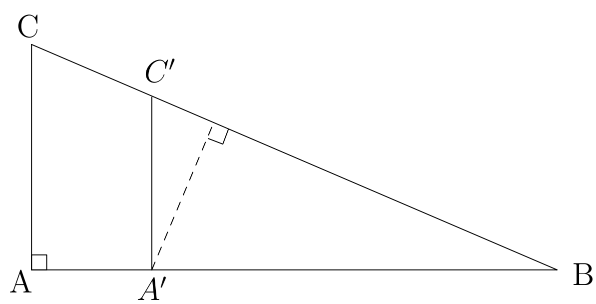


Demostrar que $\triangle ABC \sim \triangle A'BC'$.

Solución. Por hipótesis, tenemos que $\angle\, CAB = \angle\, C'A'B = 90°$ y es claro que $\angle\, ABC = \angle\, A'BC'$; entonces, aplicando el primer criterio de semejanza, obtenemos

$$\triangle ABC \sim \triangle A'BC'.$$

Ejercicio 3.2. Sea $\triangle ABC$ un triángulo rectángulo; sea A' un punto en AB; sea C' el punto sobre BC tal que $AC \,||\, A'C'$ y sea D el punto sobre BC tal que $A'D \perp BC$.



Demostrar que $AB \cdot A'B + AC \cdot A'C' = BC \cdot BC'$

Solución. Ya que $AC \,||\, A'C'$ y $\angle CAB = \angle C'A'B = \angle A'DB = \angle C'DA' = 90°$ tenemos las siguientes relaciones:

$$\triangle CAB \sim \triangle C'A'B \sim \triangle A'DB \sim \triangle C'DA'$$

de donde

$$\frac{CA}{A'D} = \frac{AB}{DB} = \frac{BC}{BA'} \qquad \frac{CA}{C'D} = \frac{AB}{DA'} = \frac{BC}{A'C'}$$