Matemáticas para las Olimpiadas

Helga Fetter Nathansky Berta Gamboa de Buen
Fausto Ongay Larios

Contenido

[1]Notas de Berta Gamboa de Buen
[2]Notas de Helga Fetter Nathansky
[3]Notas de Fausto Ongay Larios

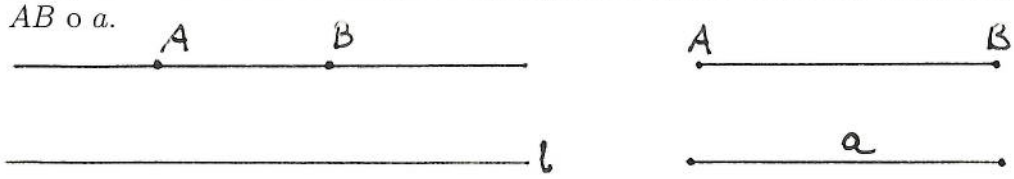
Capítulo 1

Geometría[1]

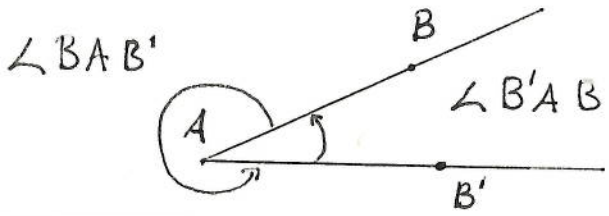
1.1 Notación

La notación que usaremos en estas notas será la siguiente.

Por dos puntos A, B pasa una línea recta; AB denotará indistintamente la recta que pasa por A y B o el segmento de recta comprendido entre A y B, quedando claro en el contexto. También denotaremos a las rectas y los segmentos por letras minúsculas como l, l' y a, b, c, respectivamente. Los segmentos no son dirigidos así que son el mismo el AB y el BA y para no complicar la notación la longitud del segmento estará denotada también por AB o a.



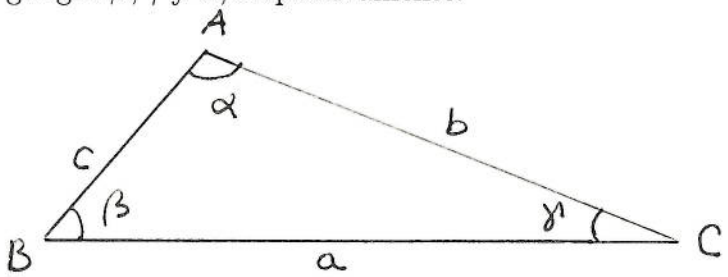
Un ángulo está determinado por dos segmentos de recta que tienen un extremo común y en este caso sí importa el orden pues dos segmentos nos determinan dos ángulos que suman 360^0.



[1]Notas de Berta Gamboa de Buen

Así por $\prec BAB'$ denotaremos al ángulo entre los segmentos de recta AB y AB' y por $\prec B'AB$ denotaremos al ángulo entre los segmentos de recta AB' y AB. Notemos que los ángulos están dirigidos en el sentido de las manecillas del reloj. Los ángulos también los denotaremos por letras griegas minúsculas.

Tres puntos A, B y C determinan tres segmentos de recta AB, BC y CA y tres ángulos $\prec ABC, \prec BCA$ y $\prec CAB$, es decir los tres puntos determinan un triángulo que llamaremos triángulo ABC. Los puntos A, B y C son los vértices del triángulo y denotaremos los lados AB, BC y CA por las letras minúsculas c, a y b respectivamente y los ángulos $\prec ABC, \prec BCA$ y $\prec CAB$ por las letras griegas β, γ y α, respectivamente.



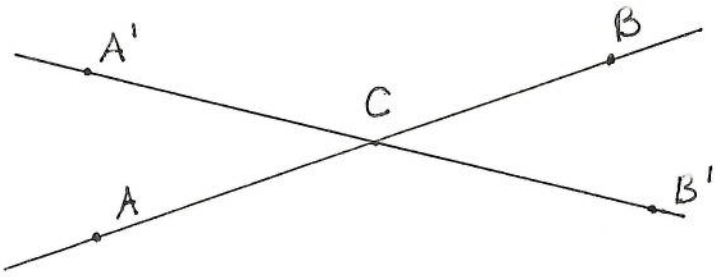
Las alturas de un triángulo son los segmentos de recta que van de los vértices al lado opuesto y son perpendiculares éste. El área de un triángulo es la mitad del producto de un lado por la altura sobre dicho lado.

1.2 Rectas y Angulos

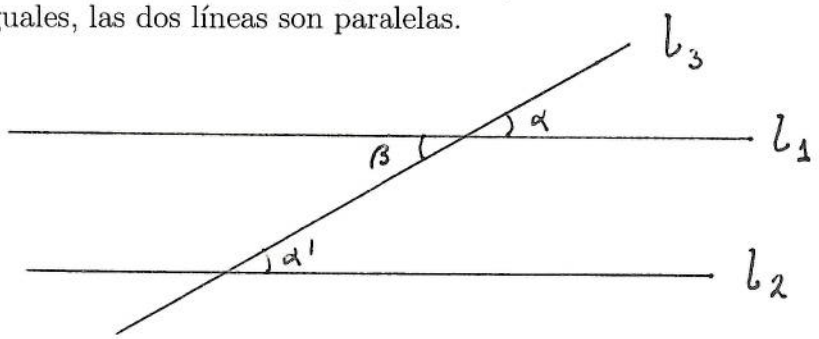
Dos rectas que nunca se cortan son paralelas, es decir dos rectas paralelas están separadas una distancia constante.

Recordemos las siguientes propiedades elementales sobre rectas y ángulos.

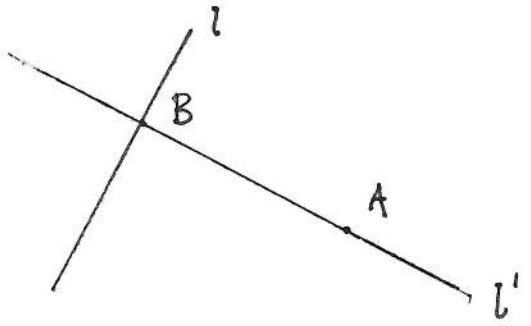
P1 Si dos rectas AB y $A'B'$ se cortan en un punto C entonces los ángulos $\prec A'CA$ y $\prec B'CB$ son iguales y los ángulos $\prec ACB'$ y $\prec BCA'$ también son iguales (son ángulos opuestos por el vértice) y tanto los ángulos $\prec A'CA$ y $\prec BCA'$, como los $\prec BCA'$ y $\prec B'CB$ son suplementarios, es decir suman 180^0.



P2 Si l_1 y l_2 son dos rectas paralelas y l_3 es una línea transversal, los ángulos correspondientes α y α' son iguales, también son iguales los ángulos alternantes β y α'. Recíprocamente si una transversal corta dos líneas de tal manera que los ángulos correspondientes o los alternantes son iguales, las dos líneas son paralelas.



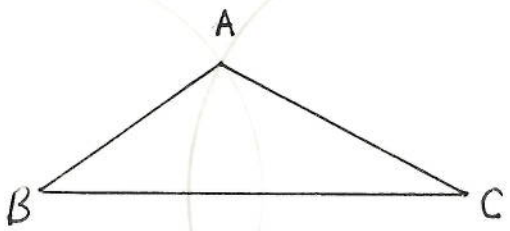
P3 Para encontrar la distancia de un punto A a una recta l tracemos la perpendicular l' a l que pasa por A y sea B la intersección de l y l'. La distancia de A a l es la longitud del segmento AB.



1.3 Triángulos

Hemos dicho que tres segmentos nos determinan un triángulo, veamos como lo podemos construir.

Construcción de un triángulo dado sus tres lados. Si a, b y c son los tres lados de un triángulo, para construirlo tomamos el segmento a y denotamos sus extremos por B y C. Con centro en B y radio c trazamos un círculo y con centro en C y radio b trazamos otro círculo. Si A es uno de los puntos de intersección de los dos círculos trazados, entonces ABC es el triángulo deseado.



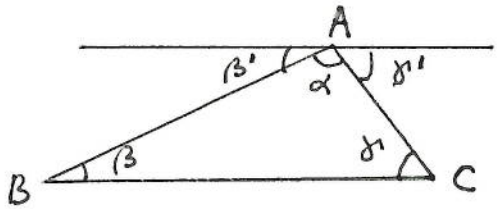
Si los círculos son tangentes se trata de un triángulo degenerado en una línea pues el punto de tangencia está sobre el segmento que une sus centros, a saber sobre a. Si los círculos no se intersectan entonces no se puede construir un triángulo que tenga esos lados.

Hemos obtenido entonces la siguiente proposición.

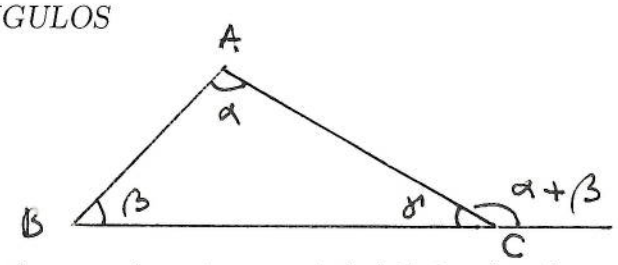
Proposición 1.1 *En un triángulo la suma de las longitudes de dos de sus lados es mayor que la longitud del lado restante.*

Proposición 1.2 *La suma de los ángulos interiores en un triángulo cualquiera es igual a* 180^0.

Demostración: Sea el triángulo ABC. Por A trazamos la paralela a BC, entonces los ángulos β y β' son iguales y los ángulos γ y γ' son iguales por ser ángulos alternos y claramente $\beta' + \alpha + \gamma' = 180^0$.



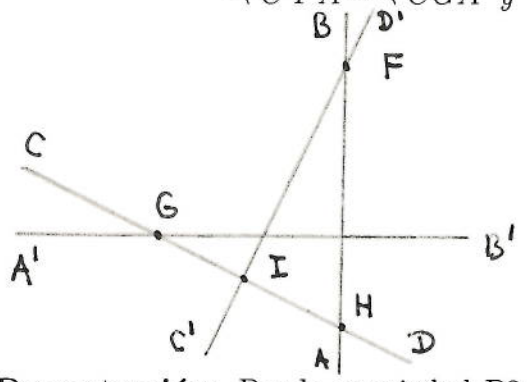
Corolario 1.3 *Un ángulo exterior de un triángulo es igual a la suma de los dos ángulos interiores opuestos.*

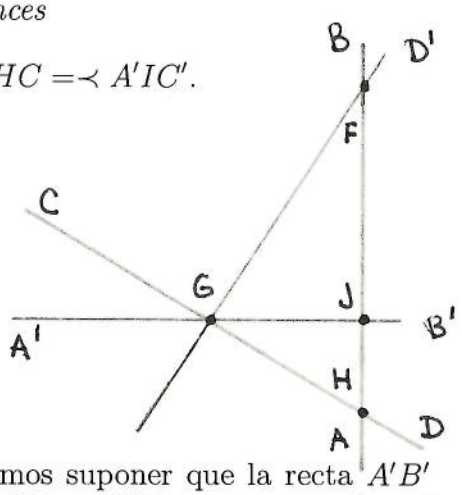


Podemos ahora probar otra propiedad de los ángulos entre ciertas rectas.

Proposición 1.4 *Sean AB y $A'B'$ dos rectas perpendiculares entre sí y CD y $C'D'$ otro par de rectas perpendiculares entre sí. Si F, G, H e I son los puntos de intersección de las rectas AB con $C'D'$, $A'B'$ con CD, AB con CD y $A'B'$ con $C'D'$ respectivamente, entonces*

$$\prec C'FA = \prec CGA' \text{ y } \prec AHC = \prec A'IC'.$$





Demostración: Por la propiedad P2 podemos suponer que la recta $A'B'$ pasa el punto de intersección de las rectas CD y $C'D'$ y entonces G e I coinciden con ese punto. Como las rectas CD y $C'D'$ son perpendiculares entre sí, de

$$\prec CGA' + \prec D'GC + \prec AGF = 180^0$$

obtenemos que

$$\prec CGA' = 90^0 - \prec AGD'. \tag{1.1}$$

Por otra parte si J es la intersección de las rectas AB y $A'B'$, del triángulo FGJ

$$\prec C'FA + \prec FJA' + \prec AGF = 180^0$$

y usando que las rectas CD y $C'D'$ son perpendiculares entre sí deducimos

$$\prec C'FA = 90^0 - \prec AGF. \tag{1.2}$$

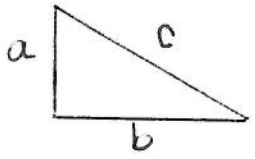
La primera igualdad que queremos probar es consecuencia de (1.1) y (1.2) y la otra se prueba de manera análoga.

Recordemos que un triángulo es equilátero si sus tres lados son iguales, isósceles si dos de sus lados son iguales y rectángulo si uno de sus ángulos es recto, es decir de 90^0. En un triángulo rectángulo, los lados adyacentes al ángulo recto se llaman catetos y el lado opuesto hipotenusa.

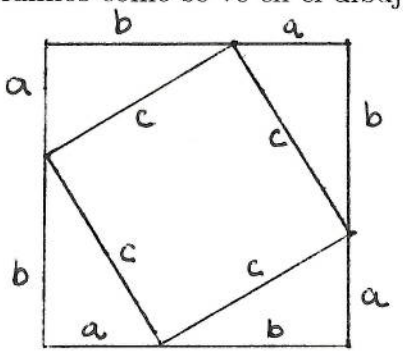
Uno de los teoremas más conocidos e importantes sobre triángulos es

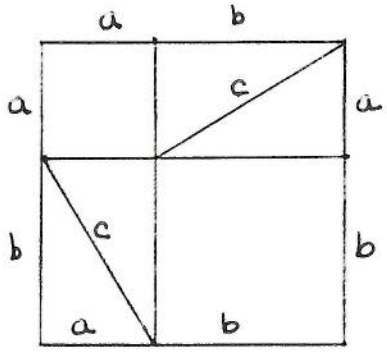
Teorema 1.5 (de Pitágoras) *En un triángulo rectángulo el cuadrado de la hipotenusa es igual a la suma de los cuadrados de los catetos.*

Demostración: Sea ABC un triángulo rectángulo con hipotenusa c y catetos a y b. Tenemos que probar que $c^2 = a^2 + b^2$.



Como el cuadrado de un segmento representa el área del cuadrado de lado el segmento, debemos probar que el área del cuadrado de lado c es igual a la suma de las áreas de los cuadrados de lados a y b. Para ello denotemos por $\mathcal{A}$,$\mathcal{B}$ y $\mathcal{C}$ las áreas de los cuadrados de lado a, b y c respectivamente y por $\mathcal{T}$ el área del triángulo ABC y construimos dos cuadrados de lado $a + b$ y los dividimos como se ve en el dibujo





Según el dibujo de la derecha el área del cuadrado de lado $a+b$ es igual a $4\mathcal{T} + \mathcal{C}$ y según el dibujo de la izquierda es igual a $4\mathcal{T} + \mathcal{A} + \mathcal{B}$. Por lo tanto $\mathcal{A} + \mathcal{B} = \mathcal{C}$ y esto prueba el teorema.

El recíproco del teorema de Pitágoras es cierto.

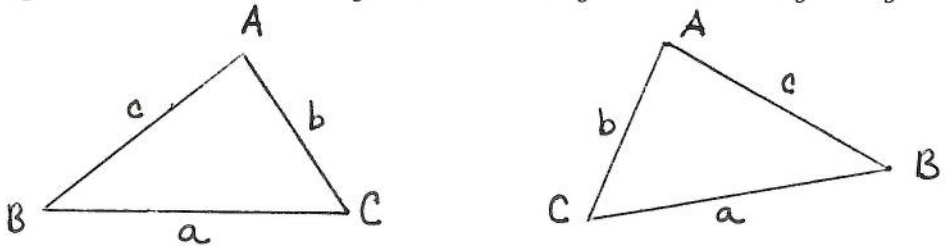
Proposición 1.6 *Si en un triángulo con lados a, b, c se tiene que $a^2+b^2 = c^2$, entonces el triángulo es rectángulo.*

Demostración: Construimos un triángulo rectángulo con catetos a y b y con hipotenusa c'. Entonces por el teorema de Pitágoras $(c')^2 = a^2 + b^2 = c^2$ y por lo tanto los dos triángulos son iguales, según la proposición siguiente.

Dos triángulos son iguales o congruentes si podemos superponer uno sobre el otro, es decir si se puede establecer una correspondencia entre sus vértices de tal forma que sus lados correspondientes y sus ángulos correspondientes son iguales.

Para ver que dos triángulos son iguales no necesitamos comprobar la igualdad de los tres lados y los tres ángulos.

Proposición 1.7 *Dos triángulos con lados iguales son triángulos iguales.*



Demostración: Sean a, b, c y a', b' y c' los lados de los dos triángulos con $a = a'$, $b = b'$ y $c = c'$ y A, B, C y A', B', C' los vértices. Trasladamos el triángulo primo de tal manera que a' quede sobre a, como $b = b'$, entonces A' está en el círculo con centro en $C = C'$ y radio b y como $c = c'$, A' está en el círculo con centro en $B = B'$ y radio c y entonces $A = A'$.

Existen otros criterios para la igualdad de triángulos, pero los obtendremos en la siguiente sección como consecuencia de los criterios para que dos triángulos sean semejantes.

Cuando hacemos planos de una casa o ciudad, queremos un dibujo que conserve la "forma" y las "proporciones" de la casa o la ciudad respectivamente, pero que sea de otro tamaño, es decir el plano es "semejante" a la casa o la ciudad .

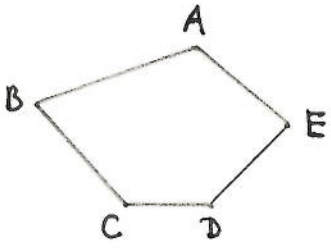
Diremos que dos polígonos son semejantes si tienen la misma "forma" y "proporciones", formalmente:

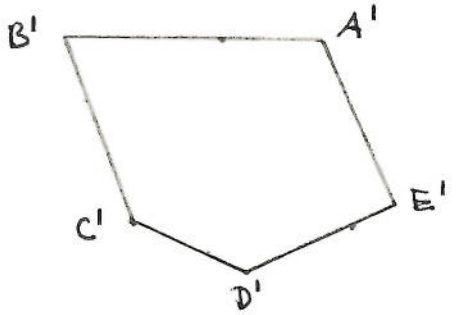
Dos polígonos con el mismo número de lados son semejantes si hay una correspondencia entre sus vértices tal que los lados correspondientes son proporcionales y los ángulos correspondientes son iguales.

Es decir, el polígono $ABCDE$ con lados a, b, c, d y e es semejante al polígono $A'B'C'D'E'$ con lados a', b', c', d' y e' si sus ángulos correspondientes son iguales y

$$\frac{a}{a'} = \frac{b}{b'} = \frac{c}{c'} = \frac{d}{d'} = \frac{e}{e'} = k$$

para alguna constante k.





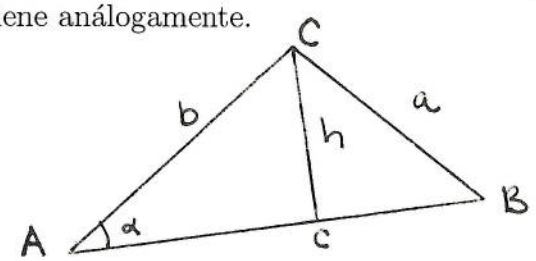
Observemos que dos polígonos son iguales si son semejantes con $k = 1$.

Para ver algunos criterios para la semejanza de triángulos necesitamos recordar las leyes de los senos y de los cosenos.

Proposición 1.8 (Ley de los senos) *Sea ABC un triángulo con lados a, b, c y ángulos opuestos α, β y γ respectivamente. Entonces*

$$\frac{a}{sen\alpha} = \frac{b}{sen\beta} = \frac{c}{sen\gamma}.$$

Demostración: Si D es el pie de la altura h sobre el lado c, entonces los triángulos ADC y BDC son rectángulos y tenemos que $sen\alpha = \frac{h}{b}$ y $sen\beta = \frac{h}{a}$, despejando $\frac{1}{h}$ e igualando obtenemos que $\frac{a}{sen\alpha} = \frac{b}{sen\beta}$. La otra igualdad se obtiene análogamente.

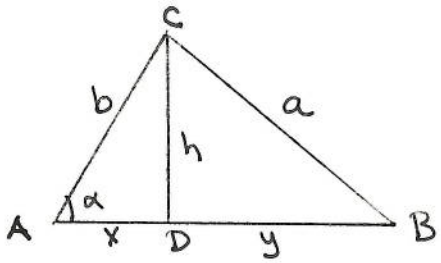


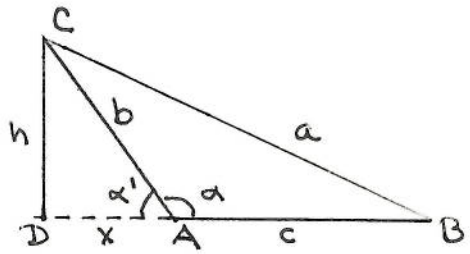
Proposición 1.9 (Ley de los cosenos) *Sea ABC un triángulo con lados a, b, c y ángulos opuestos α, β y γ respectivamente. Entonces*

$$a^2 = b^2 + c^2 - 2bc\cos\alpha.$$

Demostración: Si $\alpha \leq 90^0$, D es el pie de la altura h sobre el lado c, $x = AD$ y $y = DB$, como los triángulos ADC y BDC son rectángulos, entonces $x = b\cos\alpha$, $h = bsen\alpha$ y por el teorema de Pitágoras

$$\begin{aligned} a^2 &= h^2 + y^2 = h^2 + (c-x)^2 = h^2 + c^2 - 2cx + x^2 = \\ &= b^2 sen^2\alpha + c^2 - 2cb\cos\alpha + b^2\cos^2\alpha = b^2 + c^2 - 2bc\cos\alpha. \end{aligned}$$





Si $\alpha > 90^0$, D es el pie de la altura h sobre el lado c, $x = AD$ y $\alpha' = 180^0 - \alpha$, entonces $x = b\cos\alpha'$, $h = bsen\alpha'$ y como $\cos\alpha = -\cos\alpha'$, usando nuevamente el teorema de Pitágoras

$$\begin{aligned} a^2 &= h^2 + (c+x)^2 = h^2 + c^2 + 2cx + x^2 = \\ &= b^2 sen^2\alpha' + c^2 + 2cb\cos\alpha' + b^2\cos^2\alpha' = \\ &= b^2 + c^2 + 2bc\cos\alpha' = b^2 + c^2 - 2bc\cos\alpha. \end{aligned}$$

Proposición 1.10 *Dos triángulos son semejantes si dos de sus ángulos correspondientes son iguales.*

Veremos dos demostraciones de este resultado, la primera usando trigonometría (ley de los senos).

Demostración: Sean ABC y $A'B'C'$ dos triángulos tales que $\alpha = \alpha'$ y $\beta = \beta'$. Como la suma de los ángulos internos de un triángulo es de 180^0 tenemos que también $\gamma = \gamma'$.

La ley de los senos aplicada a los dos triángulos nos da

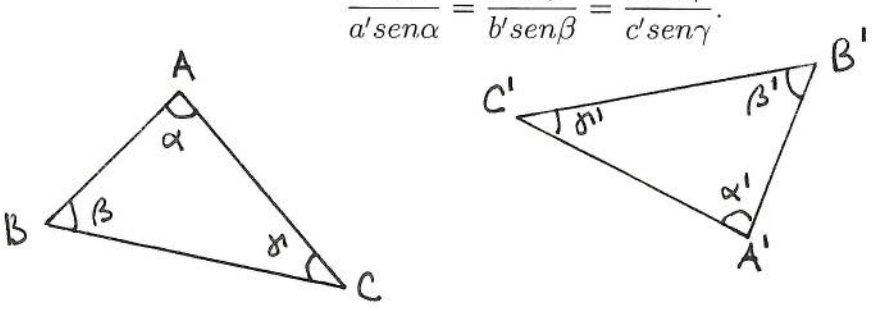
$$\frac{a}{sen\alpha} = \frac{b}{sen\beta} = \frac{c}{sen\gamma}$$

y

$$\frac{a'}{sen\alpha'} = \frac{b'}{sen\beta'} = \frac{c'}{sen\gamma'}$$

y dividiendo la primera serie de igualdades sobre la segunda obtenemos

$$\frac{asen\alpha'}{a'sen\alpha} = \frac{bsen\beta'}{b'sen\beta} = \frac{csen\gamma'}{c'sen\gamma}.$$



Como por hipótesis $\frac{sen\alpha'}{sen\alpha} = \frac{sen\beta'}{sen\beta} = \frac{sen\gamma'}{sen\gamma} = 1$, tenemos que

$$\frac{a}{a'} = \frac{b}{b'} = \frac{c}{c'}$$

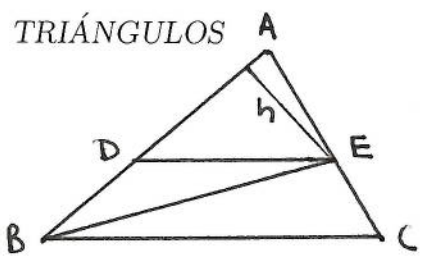
igual a alguna constante, que es lo que queríamos probar.

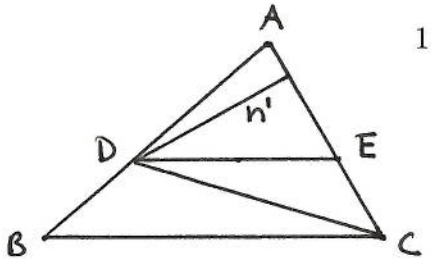
La segunda demostración usa el hecho de que el área de un triángulo es el producto de la base por la altura sobre dos y requiere del siguiente lema. Denotaremos por $\mathcal{A}_{ABC}$ el área del triángulo ABC.

Lema 1.11 *Sean ABC un triángulo y D y E puntos en los segmentos AB y AC respectivamente, de manera que las líneas que pasan por BC y DE sean paralelas. Entonces $\frac{DB}{AD} = \frac{EC}{AE}$. Recíprocamente si D y E son puntos en los lados AB y AC de un triángulo ABC tales que $\frac{DB}{AD} = \frac{EC}{AE}$, entonces las líneas BC y DE son paralelas.*

Demostración: Sean ABC un triángulo y D y E puntos cualesquiera en los segmentos AB y AC respectivamente. Como los triángulos ADE y DEB tienen la misma altura h desde E, entonces

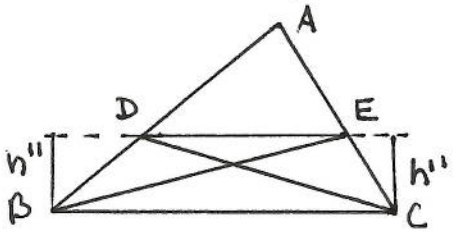
$$\frac{\mathcal{A}_{DEB}}{\mathcal{A}_{ADE}} = \frac{DB\frac{h}{2}}{AD\frac{h}{2}} = \frac{DB}{AD}. \tag{1.3}$$





Como los triángulos ADE y DEC tienen la misma altura h' desde D, entonces

$$\frac{\mathcal{A}_{DEC}}{\mathcal{A}_{ADE}} = \frac{EC\frac{h'}{2}}{AE\frac{h'}{2}} = \frac{EC}{AE}. \tag{1.4}$$



Supongamos ahora que las líneas que pasan por BC y DE son paralelas. Entonces los triángulos DEC y DEB tienen a DE como base común y la misma altura h'' sobre B y C respectivamente y entonces

$$\mathcal{A}_{DEC} = \mathcal{A}_{DEB}. \tag{1.5}$$

Finalmente de (0.3), (0.4) y (0.5), obtenemos

$$\frac{DB}{AD} = \frac{\mathcal{A}_{DEB}}{\mathcal{A}_{ADE}} = \frac{\mathcal{A}_{DEC}}{\mathcal{A}_{ADE}} = \frac{EC}{AC}.$$

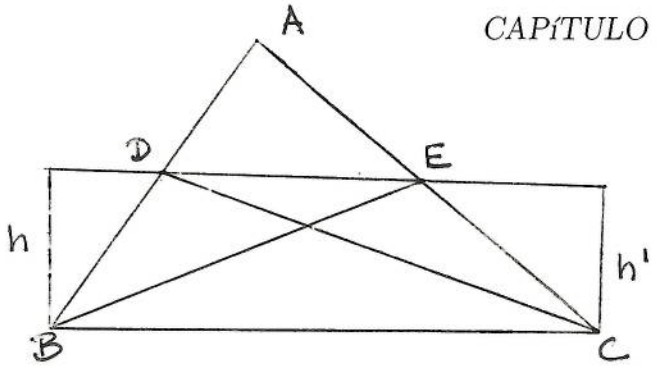
Supongamos ahora que los puntos D y E satisfacen $\frac{DB}{AD} = \frac{EC}{AE}$. De (1.3) y (0.4) obtenemos entonces que $\frac{\mathcal{A}_{DEB}}{\mathcal{A}_{ADE}} = \frac{\mathcal{A}_{DEC}}{\mathcal{A}_{ADE}}$, es decir

$$\mathcal{A}_{DEB} = \mathcal{A}_{DEC}$$

Si h es la altura del triángulo DEB y h' es la altura del triángulo DEC, entonces

$$\frac{ED \cdot h}{2} = \mathcal{A}_{DEB} = \mathcal{A}_{DEC} = \frac{ED \cdot h'}{2},$$

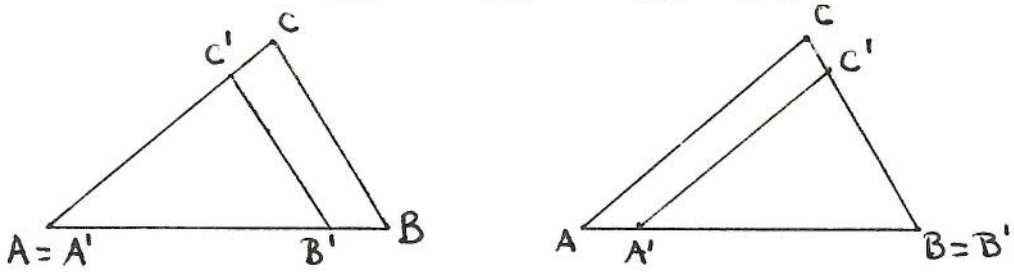
de donde $h = h'$ y las líneas ED y BC son paralelas.



Ahora sí podemos dar la otra demostración de la proposición 1.10.

Demostración: Sean ABC y $A'B'C'$ dos triángulos con dos ángulos correspondientes iguales. Por lo tanto tienen los tres ángulos correspondientes iguales y si encimamos A y A' y ponemos a B' sobre la línea AB, entonces C' quedará sobre la línea AC y las líneas BC y $B'C'$ serán paralelas. Por el lema anterior obtenemos entonces que $\dfrac{AB'}{B'B} = \dfrac{AC'}{C'C}$, de donde

$$\begin{aligned}\frac{AB}{A'B'} &= \frac{AB}{AB'} = \frac{AB' + B'B}{AB'} = 1 + \frac{B'B}{AB'} = \\ &= 1 + \frac{C'C}{AC'} = \frac{AC' + C'C}{AC'} = \frac{AC}{AC'} = \frac{AC}{A'C'}.\end{aligned}$$



Si ahora encimamos los vértices B y B' obtenemos análogamente que

$$\frac{BC}{B'C'} = \frac{BA}{B'A'}.$$

Esto termina la prueba de la proposición.

Corolario 1.12 *Si dos triángulos tienen dos ángulos y un lado respectivos iguales, entonces son congruentes.*

Demostración: Sean a y a' los lados iguales, entonces en la proposición anterior se obtiene $\dfrac{a}{a'} = 1$.

Proposición 1.13 *Dos triángulos son semejantes si sus lados correspondientes son proporcionales.*

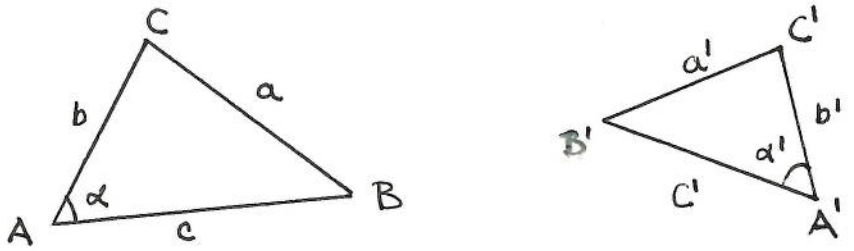
Demostración: Sean ABC y $A'B'C'$ tales que $\frac{a}{a'} = \frac{b}{b'} = \frac{c}{c'} = k$.

De la ley de los cosenos aplicada a cada triángulo obtenemos

$$\begin{aligned} a^2 &= b^2 + c^2 - 2bc\cos\alpha \\ \text{y } (a')^2 &= (b')^2 + (c')^2 - 2b'c'\cos\alpha' \end{aligned}$$

de donde

$$\begin{aligned} \cos\alpha &= \frac{b^2 + c^2 - a^2}{2bc} \\ &\text{y} \\ \cos\alpha' &= \frac{(b')^2 + (c')^2 - (a')^2}{2b'c'}. \end{aligned}$$



Dividiendo las igualdades anteriores y usando que $\frac{u}{v} = \frac{x}{y}$ implica que $\frac{u+x}{v+y} = \frac{u}{v} = \frac{u-x}{v-y}$ y que $\frac{u^2}{v^2} = \frac{x^2}{y^2}$,

$$\frac{\cos\alpha}{\cos\alpha'} = \frac{b^2 + c^2 - a^2}{(b')^2 + (c')^2 - (a')^2}\frac{b'c'}{bc} = k^2\frac{1}{k^2} = 1.$$

Como ambos ángulos son menores que 180^0, $\alpha = \alpha'$. Análogamente se prueba que $\beta = \beta'$ y que $\gamma = \gamma'$.

Como corolario se obtiene el resultado que ya vimos que dos triángulos con lados iguales son iguales.

Proposición 1.14 *Dos triángulos son semejantes si dos de sus lados correspondientes son proporcionales y los ángulos entre esos dos lados son iguales.*

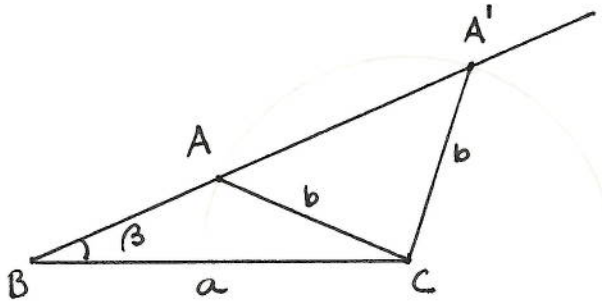
Demostración: Sean ABC y $A'B'C'$ dos triángulos tales que $\frac{b}{b'} = \frac{c}{c'} = k$ y $\alpha = \alpha'$. Como en la segunda demostración de la proposición 1.10 encimamos los triángulos de manera que $A = A'$ y que B' y C' estén respectivamente en las líneas AB y AC. Esto se puede porque $\alpha = \alpha'$. Es fácil ver que la condición $\frac{b}{b'} = \frac{c}{c'}$ implica que $\frac{AB'}{B'B} = \frac{AC'}{C'C}$ y entonces por el lema 1.11 las rectas BC y $B'C'$ son paralelas, es decir $\beta = \beta'$ y $\gamma = \gamma'$, que es lo que queríamos probar.

Corolario 1.15 *Si dos triángulos tienen dos lados correspondientes iguales y los ángulos entre ellos son iguales, entonces son congruentes.*

Por lo anterior se le ocurre a uno que la siguiente afirmación también debe de ser cierta:

Si dos triángulos tienen iguales dos lados y el ángulo adyacente a uno de los lados, entonces son iguales.

Construyamos un triángulo dados dos lados y el ángulo adyacente a uno sólo de ellos. Sean a y b los lados y β el ángulo adyacente al lado a, pero no al lado b. Si B y C son los extremos de a, trazamos la recta l que pasa por B y forma un ángulo β con a y el círculo $\mathcal{C}$ con centro en C y radio b.



La recta l puede intersectar al círculo $\mathcal{C}$ en dos puntos A y A', en un sólo punto T o no intersectarla. En el primer caso obtenemos dos triángulos,

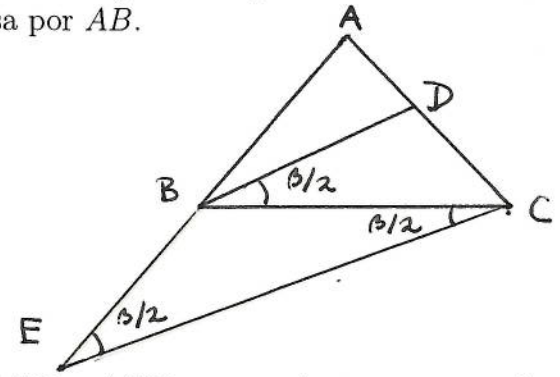
a saber ABC y $A'BC$ que claramente no son iguales. En el segundo caso obtenemos un único triángulo TBC y en el tercer caso no se puede construir ningún triángulo con esas propiedades.

Como podemos encontrar lados a y b y ángulos β de manera que l intersecte a $\mathcal{C}$ en dos puntos, hemos probado que la afirmación en cuestión es falsa.

Finalizaremos esta sección con un resultado que se prueba usando algunos de los criterios para la semejanza de triángulos vistos.

Teorema 1.16 *Un ángulo bisector en un triángulo divide el lado opuesto en dos segmentos que tienen la misma razón que los otros dos lados.*

Demostración: Si ABC es un triángulo, tracemos la línea que bisecta al ángulo β y sea D la intersección de dicha línea con el lado AC. Por C trazamos una paralela a BD y sea E el punto de intersección de dicha paralela con la línea que pasa por AB.



Los triángulos ABD y AEC son semejantes pues sus ángulos correspondientes son iguales; entonces $\dfrac{AB}{AD} = \dfrac{AE}{AC} = \dfrac{AB + BE}{AD + DC}$ de donde

$$\frac{AB}{AD} = \frac{AB + BE - AB}{AD + DC - AD} = \frac{BE}{DC}. \tag{1.6}$$

Por otra parte

$$\prec DBC = \prec BCE = \frac{\beta}{2}$$

y como

$$\prec ABD = \prec AEC = \prec DBC = \frac{\beta}{2}$$

resulta que el triángulo BCE es isósceles y que $BC = BE$. Sustituyendo en (1.6) obtenemos $\frac{AB}{AD} = \frac{BC}{DC}$, es decir

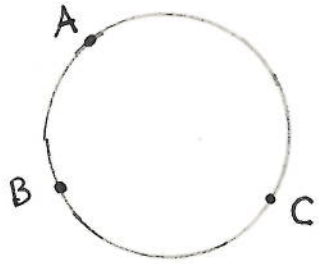
$$\frac{AB}{BC} = \frac{AD}{DC}.$$

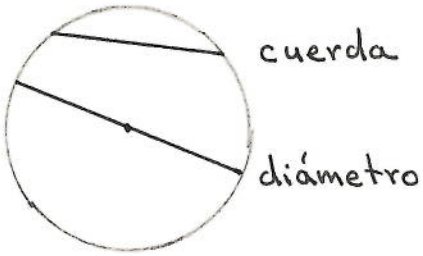
Esto termina la prueba.

1.4 Círculos

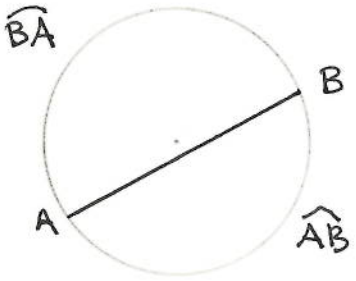
Tres puntos no colineales definen un círculo, el círculo circunscrito al triángulo que tiene como vértices dichos puntos.

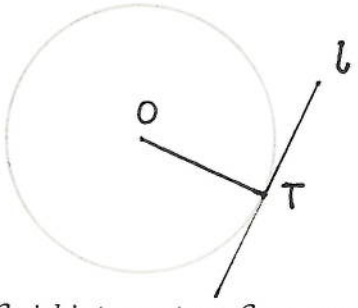
Una cuerda es un segmento de recta cuyos extremos están sobre el círculo. Un diámetro es una cuerda que pasa por el centro del círculo.





Si $\mathcal{C}$ es un círculo con centro en O y A y B son dos puntos en $\mathcal{C}$, estos puntos nos determinan la cuerda AB y dos arcos en el círculo $\mathcal{C}$, que denotaremos por $\widehat{AB}$ y $\widehat{BA}$.

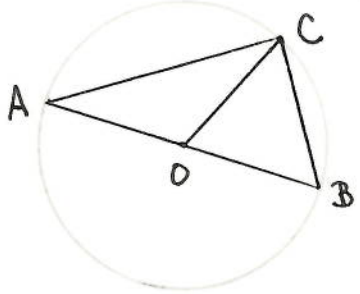




Una recta l es tangente a un círculo $\mathcal{C}$ si l intersecta a $\mathcal{C}$ en uno y sólo un punto. Si l es tangente en T al círculo $\mathcal{C}$ con centro en O, entonces OT es perpendicular a l.

Supongamos que queremos construir un triángulo rectángulo dada su hipotenusa, este problema se puede resolver fácilmente si conocemos cierto resultado sobre el ángulo entre dos cuerdas que se intersectan sobre el círculo.

Sean AB un segmento de recta, $\mathcal{C}$ el círculo con diámetro AB, O el centro del círculo y C cualquier punto en $\mathcal{C}$.



Entonces los triángulos CAO y COB son isósceles y por lo tanto tenemos las siguientes igualdades $\prec OCB = \prec CBO$ y $\prec ACO = \prec CAO$. Por otra parte como ACB es un triángulo la suma de sus ángulos internos es de 180^0, es decir

$$\prec OAC + \prec ACO + \prec OCB + \prec CBO = 180^0$$

de donde

$$2 \prec ACO + 2 \prec OCB = 180^0$$

y por lo tanto

$$\prec ACB = \prec ACO + \prec OCB = 90^0.$$

Hemos probado que para cualquier punto C sobre el círculo $\mathcal{C}$ el triángulo ABC es rectángulo. Notemos que esto significa que la hipotenusa de un triángulo no es suficiente para determinarlo.

Lo que acabamos de ver es un caso particular de la siguiente situación: Supongamos que AB es cualquier cuerda fija de un círculo $\mathcal{C}$ y C es cualquier punto sobre $\mathcal{C}$, veremos que el ángulo $\prec ACB$ no depende de C siempre que C este sobre el círculo $\mathcal{C}$ y del mismo lado de la cuerda AB, es decir que esté en el mismo arco de los dos determinados por AB. Para ello sea O el centro de $\mathcal{C}$, supongamos que C está en el arco $\widehat{BA}$ y tracemos los triángulos OAC, OAB y OBC. Como todos ellos son triángulos isósceles, $\prec OAC = \prec ACO = \alpha$, $\prec OCB = \prec CBO = \beta$ y $\prec OBA = \prec BAO = \gamma$. Entonces

$$2\alpha + 2\beta + 2\gamma = 180^0$$

pues es la suma de los ángulos internos del triángulo ABC, por lo tanto

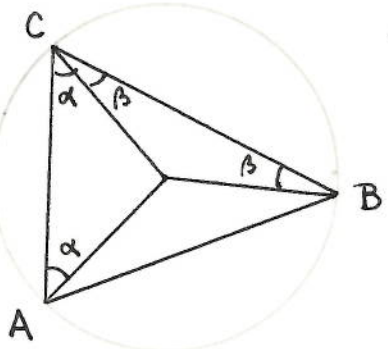
$$2 \prec ACB + 2\gamma = 2(\alpha + \beta) + 2\gamma = 180^0. \tag{1.7}$$

Por otra parte si nos fijamos en el triángulo OAB obtenemos que

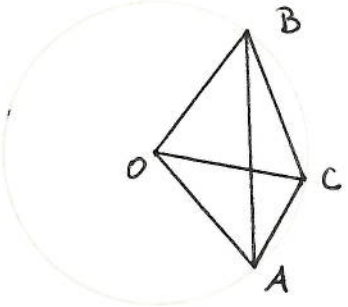
$$\prec AOB + 2\gamma = 180^0. \tag{1.8}$$

Finalmente, de (1.9) y (1.10) obtenemos que

$$\prec AOB = 2 \prec ACB.$$



Si ahora C está en el arco $\widehat{AB}$ igual que en el otro caso, trazamos los triángulos OAC, OAB y OBC y como todos ellos son triángulos isósceles, $\prec OAC = \prec ACO = \alpha$, $\prec OCB = \prec CBO = \beta$ y $\prec OBA = \prec BAO = \gamma$.



Entonces

$$(\alpha - \gamma) + (\beta - \gamma) + (\alpha + \beta) = 2(\alpha + \beta - \gamma) = 180^0$$

pues es la suma de los ángulos internos del triángulo ABC, por lo tanto

$$2 \prec ACB - 2\gamma = 2(\alpha + \beta) - 2\gamma = 180^0. \tag{1.9}$$

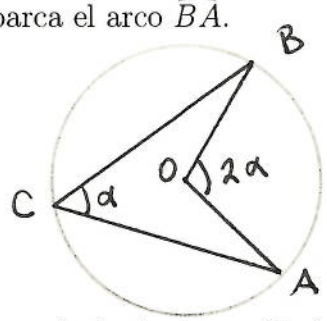
Por otra parte si nos fijamos en el triángulo OAB obtenemos que

$$\prec AOB + 2\gamma = 180^0 \tag{1.10}$$

y de ahí, como $\prec BOA = 360^0 - \prec AOB$, usando (1.9), obtenemos que

$$\prec BOA = 360^0 - 180^0 + 2\gamma = 2 \prec ACB.$$

El ángulo $\prec AOB$ es el ángulo central que abarca el arco $\widehat{AB}$ y $\prec BOA$ es el ángulo central que abarca el arco $\widehat{BA}$.

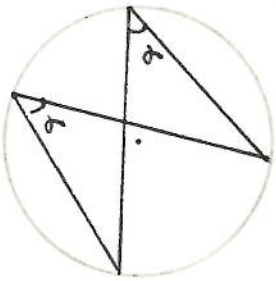


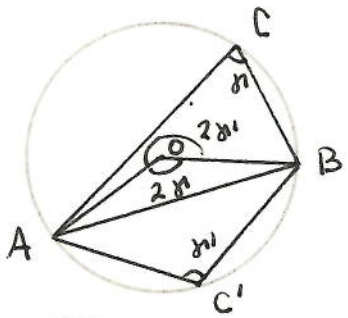
Hemos probado entonces el siguiente resultado conocido como teorema del ángulo central.

Teorema 1.17 (del ángulo central) *Sean $\mathcal{C}$ una círculo con centro O, AB una cuerda en $\mathcal{C}$ y C un punto en el arco $\widehat{BA}$. Entonces el ángulo central que abarca el arco $\widehat{AB}$ es el doble del ángulo ACB.*

El siguiente corolario es de gran utilidad.

Corolario 1.18 *Si dos ángulos inscritos en una circunferencia abarcan el mismo arco, entonces son iguales.*





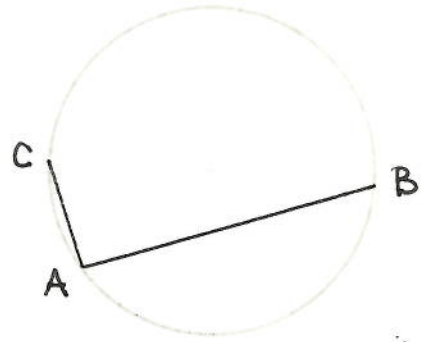
Observemos ahora que si C está en el arco $\widehat{BA}$ y C' está en el arco $\widehat{AB}$, como

$$2 \prec ACB + 2 \prec BC'A = \prec AOB + \prec BOA = 360^0,$$

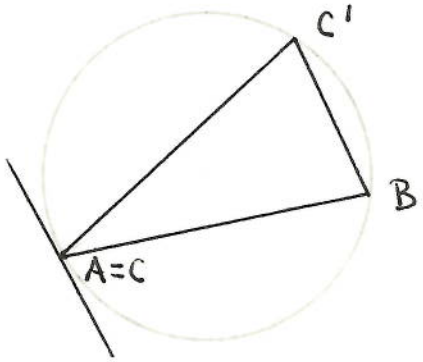
tenemos que

$$\prec ACB + \prec BC'A = 180^0.$$

Cuando el punto C en el teorema del ángulo central se aproxima a uno de los extremos de la cuerda AB, digamos a A, entonces la cuerda AC se aproxima a una tangente al círculo $\mathcal{C}$.

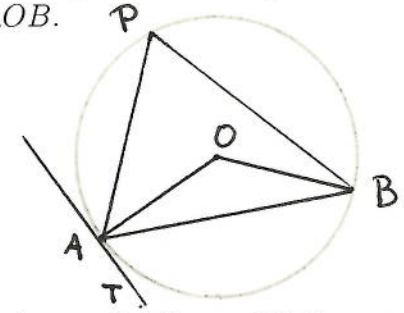


Si $A = C$, tenemos



Teorema 1.19 (de la tangente) *El ángulo entre la tangente a un círculo y una cuerda que pase por el punto de tangencia es igual al ángulo subtendido desde cualquier punto de la circunferencia hacia la cuerda en el lado opuesto de la cuerda.*

Demostración: Sean AB una cuerda en el círculo $\mathcal{C}$, AT la tangente a $\mathcal{C}$ que pasa por A, O el centro de $\mathcal{C}$ y P cualquier punto en $\mathcal{C}$ distinto de A y B y en el lado opuesto de la cuerda con respecto a la tangente. Por el teorema del ángulo central, $2 \prec APB = \prec AOB$.



Como el triángulo AOB es isósceles, $\prec BAO = \prec OBA$ y entonces

$$2 \prec APB + 2 \prec BAO = \prec AOB + 2 \prec OAB = 180^0.$$

De donde

$$\prec APB + \prec BAO = 90^0. \tag{1.11}$$

Por otra parte como el ángulo $\prec OAT$ es recto, tenemos que

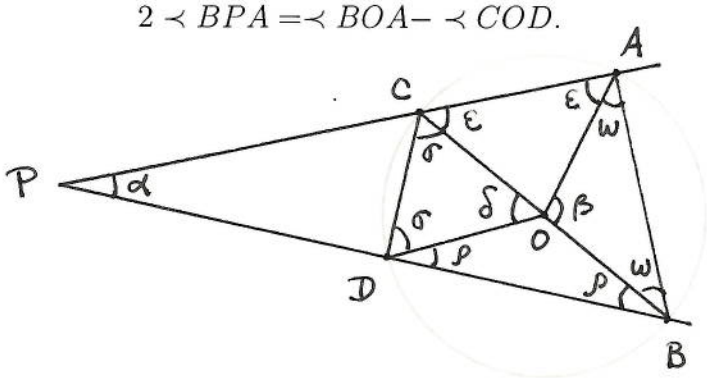
$$\prec BAT = 90^0 - \prec BAO. \tag{1.12}$$

De (1.11) y (1.12) obtenemos el resultado deseado.

Cuando el punto está fuera o dentro del círculo el teorema del ángulo central se generaliza en las dos siguientes proposiciones.

Proposición 1.20 *Sean $\mathcal{C}$ un círculo con centro en O y P un punto fuera de $\mathcal{C}$. Si las cuerdas AC y BD se intersectan en P, entonces*

$$2 \prec BPA = \prec BOA - \prec COD.$$



Demostración: Si denotamos los ángulos como en la figura, obtenemos las siguientes relaciones. Sumando los ángulos internos del triángulo PAB

$$\alpha + \varepsilon + 2\omega + \rho = 180^0,$$

de donde

$$2\alpha = 360^0 - 2\varepsilon - 4\omega - 2\rho. \tag{1.13}$$

De los triángulos COD y AOB

$$\delta = 180^0 - 2\sigma \tag{1.14}$$

y

$$\beta = 180^0 - 2\omega. \tag{1.15}$$

Como los ángulos internos de un cuadrilátero suman 360^0

$$2\varepsilon + 2\omega + 2\rho + 2\sigma = 360^0. \tag{1.16}$$

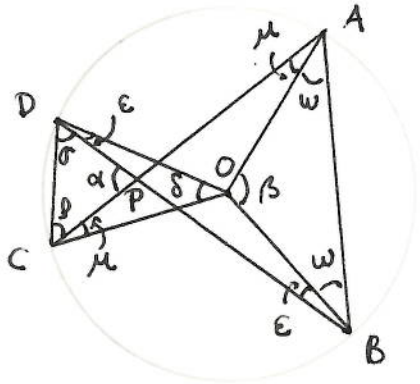
Sumando (1.13) y (1.15) y sustituyendo (1.16) y (1.15)

$$\begin{aligned} 2\alpha + \delta &= 540^0 - 2\varepsilon - 2\omega - 2\rho - 2\sigma - 2\omega = \\ &= 540^0 - 360^0 - 2\omega = 180^0 - 2\omega = \\ &= \beta. \end{aligned}$$

De donde se obtiene directamente el resultado deseado.

Proposición 1.21 *Sean C un círculo con centro en O y P un punto dentro de C. Si las cuerdas AC y BD se intersectan en P, entonces*

$$2 \prec BPA = \prec BOA + \prec DOC.$$



Demostración: Notando que varios de los triángulos que aparecen en la figura son isósceles, denotamos los ángulos como en la figura. Como el triángulo OCD es isósceles

$$\sigma + \varepsilon = \rho + \mu = \vartheta. \tag{1.17}$$

Sumando los ángulos internos del triángulo APB

$$\alpha + \varepsilon + 2\omega + \mu = 180^0,$$

de donde

$$2\alpha = 360^0 - 2\varepsilon - 4\omega - 2\mu. \tag{1.18}$$

Por otra parte, sumando los ángulos internos del triángulo DPC

$$\alpha + \sigma + \rho = 180^0$$

y usando (1.17)

$$\alpha = 180^0 - 2\vartheta + \varepsilon + \mu.$$

Despejando $\varepsilon + \mu$ y sustituyéndolo en (1.18),

$$2\alpha = 360^0 - 4\omega - 2\alpha - 4\vartheta + 360^0.$$

De ahí

$$4\alpha = 720^0 - 4\omega - 4\vartheta,$$

y como de los triángulos OAB y ODC se tiene que $\beta + 2\omega = 180^0$ y $\delta + 2\vartheta$, deducimos

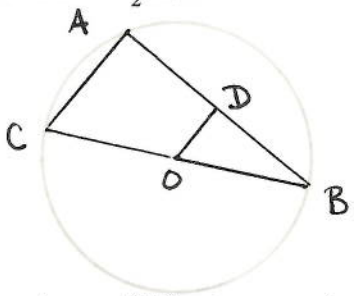
$$2\alpha = 360^0 - 2\omega - 2\vartheta = \beta + \delta.$$

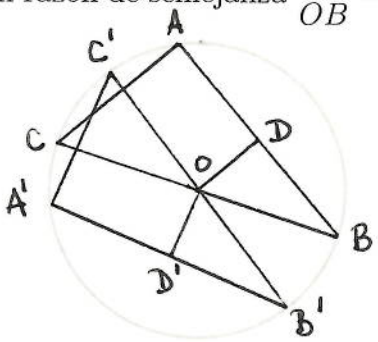
Esto prueba el resultado deseado.

Veremos ahora un par de resultados sobre cuerdas.

Proposición 1.22 *Cuerdas iguales en un círculo equidistan del centro.*

Demostración: Sea AB una cuerda en el círculo $\mathcal{C}$ y sean C el otro extremo del diámetro que pasa por B y O el centro del círculo. Sea D la intersección de la paralela a AC que pasa por O con la cuerda AB. Como el ángulo $\prec CAB$ abarca un diámetro es recto y entonces los triángulos ABC y DBO son triángulos rectángulos semejantes con razón de semejanza $\dfrac{CB}{OB} = \dfrac{1}{2}$. Por lo tanto $OD = \frac{1}{2}AC$.





Sea ahora $A'B'$ otra cuerda en $\mathcal{C}$ tal que $AB = A'B$; construimos C' y D' como antes. Entonces los triángulos rectángulos ABC y $A'B'C'$ son semejantes con $BC = B'C'$ (ambos son diámetros) y entonces

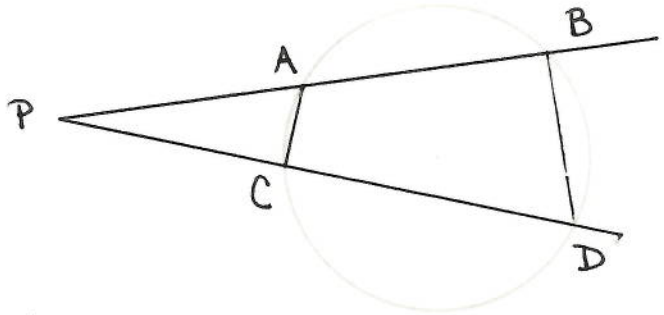
$$OD = \frac{1}{2}AC = \frac{1}{2}A'C' = OD'.$$

Esto prueba que las cuerdas equidistan del centro pues OD y OD' son las distancias de O a la cuerdas AB y $A'B'$ respectivamente.

Proposición 1.23 *Si AB y CD son dos cuerdas en el círculo $\mathcal{C}$ y P es el punto de intersección de las cuerdas, entonces $PA \cdot PB = PC \cdot PD$.*

Demostración: Los triángulos APC y DPB son semejantes ya que tienen un ángulo en común y el ángulo $\prec DCA$ es suplementario tanto al ángulo

$\prec ACP$, por estar en una línea, como al $\prec PBD$, pues ambos subtienden la misma cuerda AD pero de lados opuestos.

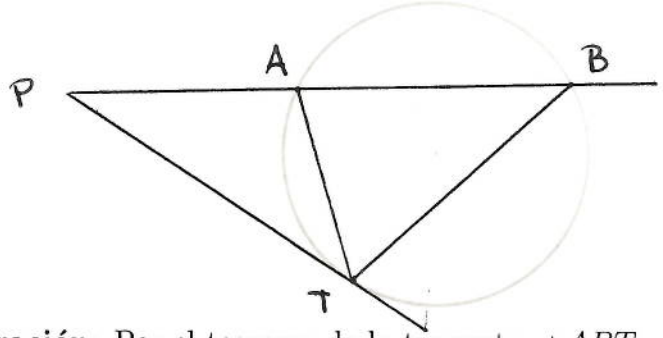


Por lo tanto

$$\frac{PA}{PC} = \frac{PD}{PB}.$$

El caso límite de la proposición anterior dice así:

Proposición 1.24 *Si AB es una cuerda en el círculo $\mathcal{C}$ y PT es una tangente a $\mathcal{C}$ con P en la línea AB, entonces $PT^2 = PA \cdot PB$.*



Demostración: Por el teorema de la tangente $\prec ABT = \prec ATP$, entonces los triángulos PTA y PBT son semejante y de ahí

$$\frac{PT}{PA} = \frac{PB}{PT}.$$

Corolario 1.25 *Si desde un punto P fuera de un círculo $\mathcal{C}$ se trazan las tangentes a $\mathcal{C}$ con puntos de tangencia T y T', entonces $PT = PT'$.*

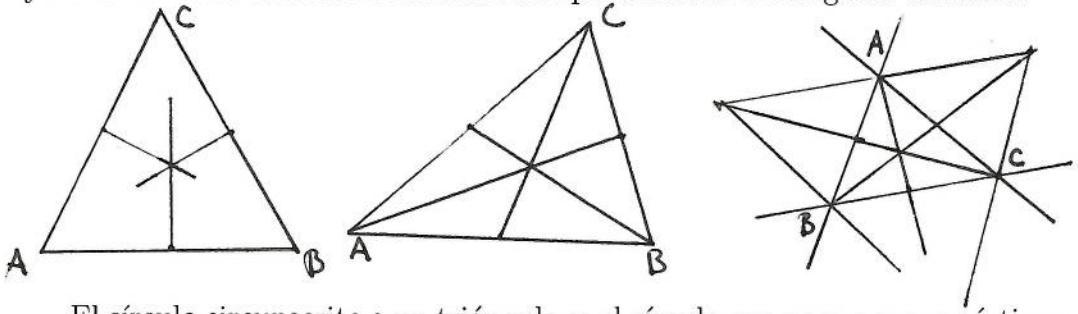
1.5 Círculos y triángulos

Dado un triángulo podemos construir varios círculos asociados. Estudiaremos algunas de las propiedades de los triángulos relacionadas con dichos círculos. Para ello debemos recordar algunas definiciones:

Las mediatrices de un triángulo son las rectas perpendiculares a sus lados y que pasan por los puntos medios de ellos.

Las medianas son las rectas que pasan por un vértice y el punto medio del lado opuesto. El punto de intersección de las medianas es llamado punto mediano.

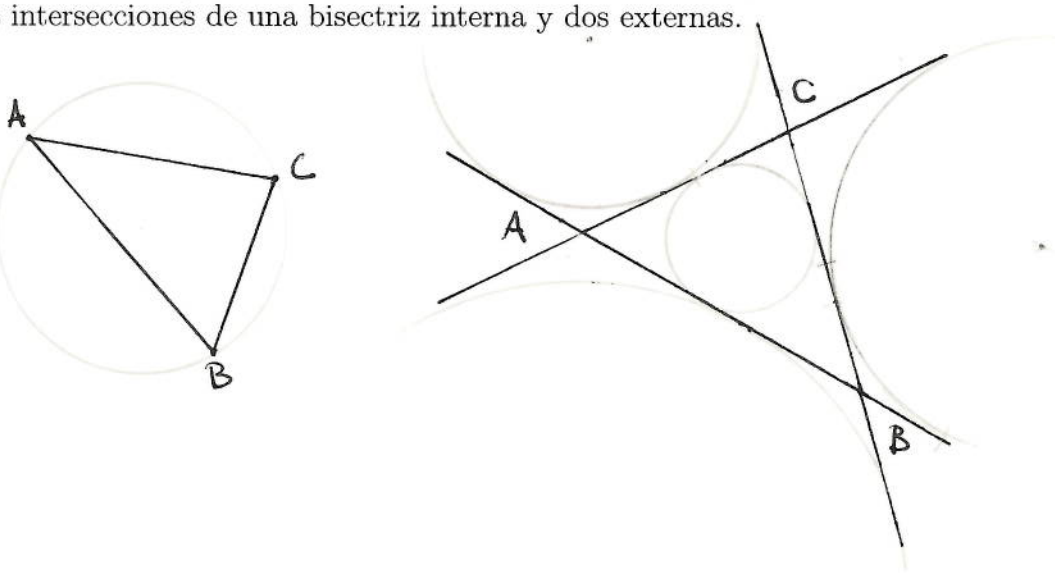
Las bisectrices internas son las rectas que bisectan los ángulos del triángulo y las bisectrices externas son las rectas que bisectan los ángulos externos.



El círculo circunscrito a un triángulo es el círculo que pasa por sus vértices y su centro es la intersección de las mediatrices del triángulo.

El círculo inscrito a un triángulo es el círculo que es tangente a los tres lados del triángulo. El centro del círculo inscrito es el punto de intersección de las bisectrices de los ángulos interiores del triángulo.

Los círculos excritos a un triángulo son los que son tangentes a las tres líneas que contienen los lados del triángulo, de manera que el punto de tangencia con una de las líneas está sobre un lado y los otros dos puntos están sobre las prolongaciones de los lados. Los centros de los círculos excritos son las intersecciones de una bisectriz interna y dos externas.



Proposición 1.26 *Sea ABC un triángulo con lados a, b, c y ángulos α, β, γ, C el círculo circunscrito y r el radio del círculo. Entonces*

$$2r = \frac{a}{sen\alpha} = \frac{b}{sen\beta} = \frac{c}{sen\gamma}.$$

Demostración: Por el teorema del ángulo central $2\alpha = \prec BOC$. Sea D el pie de la altura sobre BC del triángulo OBC; como el triángulo OBC es isósceles $CD = DB$ y

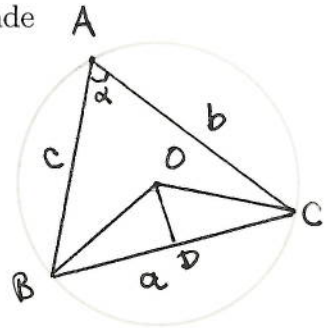
$$\prec BOD = \prec DOC = \frac{1}{2} \prec BOC = \alpha.$$

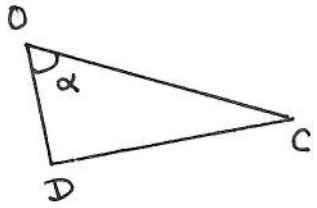
Por lo tanto del triángulo rectángulo ODC obtenemos

$$sen\alpha = sen \prec DOC = \frac{CD}{OC} = \frac{a}{2r},$$

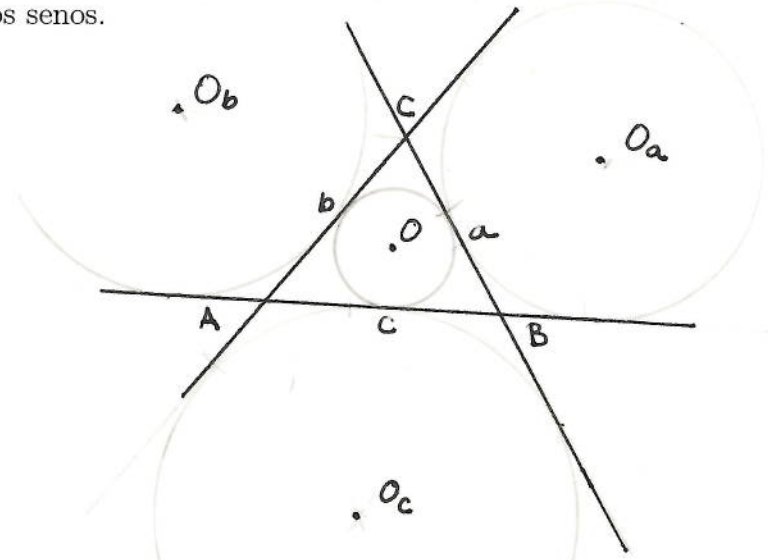
de donde

$$2r = \frac{a}{sen\alpha}.$$





El resto de las igualdades se pueden probar análogamente o usando la ley de los senos.



Si ABC es un triángulo con lados a, b, c, denotaremos a sus 3 círculos excritos por $\mathcal{C}_a$, $\mathcal{C}_b$ y $\mathcal{C}_c$ y a sus radios por r_a, r_b y r_c si es tangente en un punto sobre el lado a, b y c, respectivamente.

Teorema 1.27 *Si r es el radio del círculo inscrito a un triángulo con lados a, b, c y semiperímetro s y r_a, r_b y r_c son los radios de los círculos excritos a los lados a, b y c respectivamente, entonces*

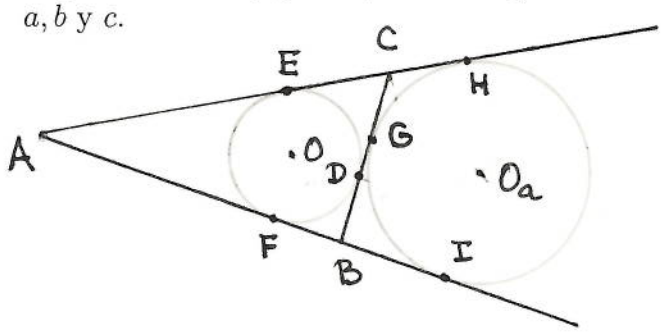
$$r = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}},$$

$$r_a = \sqrt{\frac{s(s-b)(s-c)}{s-a}},$$

$$r_b = \sqrt{\frac{(s-a)s(s-c)}{s-b}} \quad y$$

$$r_c = \sqrt{\frac{(s-a)(s-b)s}{s-c}}.$$

Demostración: Sean ABC un triángulo con lados $a.b.c$ y semiperímetro s, $\mathcal{C}$ su círculo inscrito, r el radio y O el centro de $\mathcal{C}$. Sea $\mathcal{C}_a$ el círculo excrito al lado a, r_a su radio y O_a su centro. Recordemos que $s = \frac{a+b+c}{2}$ y denotemos por D, E y F los puntos de tangencia de $\mathcal{C}$ con los lados a, b y c respectivamente y por G, H e I los puntos de tangencia de $\mathcal{C}_a$ con los lados a, b y c.



Del corolario 1.25, deducimos las siguientes igualdades

$$AF = AE,\ BF = BD \text{ y } CD = CE \tag{1.19}$$

y entonces el perímetro del triángulo ABC es $2AF + 2BD + 2CE$, de donde

$$s = AF + BD + CE. \tag{1.20}$$

Además tenemos

$$a = BD + CD,\ b = CE + AE \text{ y } c = AF + BF \tag{1.21}$$

y

$$\begin{aligned} s - a &= \frac{a+b+c}{2} - a = \frac{-a+b+c}{2}, \\ s - b &= \frac{a-b+c}{2} \quad \text{y} \\ s - c &= \frac{a+b-c}{2}. \end{aligned} \tag{1.22}$$

Sustituyendo (1.21) en (1.22) y usando (1.19)

$$\begin{aligned} s - a &= \frac{-BD - CD + CE + AE + AF + BF}{2} = AF \\ s - b &= \frac{BD + CD - CE - AE + AF + BF}{2} = BD \\ s - c &= \frac{BD + CD + CE + AE - AF - BF}{2} = CE. \end{aligned} \tag{1.23}$$

Para el círculo $\mathcal{C}_a$ usando el corolario 1.25 se obtienen las relaciones

$$AI = AH,\ BI = BG \text{ y } CG = CH$$

y entonces

$$\begin{aligned} 2s &= AB + BG + CG + AC = \\ &= AI - BI + BG + CG + AH - CH = 2AI, \end{aligned}$$

de donde

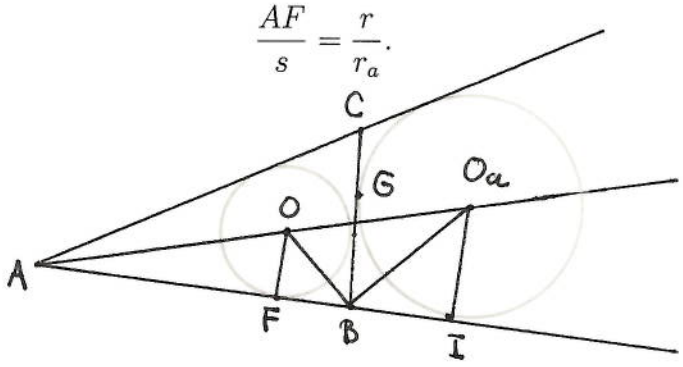
$$s = AI. \tag{1.24}$$

Por lo tanto, usando (1.23)

$$BI = s - c = CE. \tag{1.25}$$

Por otra parte, como los triángulos AOF y AO_aI son semejantes pues tienen en común un el ángulo $\prec OAF$ y los ángulos $\prec OAF$ y $\prec O_aAI$ son rectos, $\dfrac{AF}{AI} = \dfrac{OF}{O_aI}$. Usando (1.24)

$$\frac{AF}{s} = \frac{r}{r_a}. \tag{1.26}$$



También tenemos que los triángulos rectángulos OFB y BIO_a son semejantes ya que BO y BO_a son las bisectrices interna y externa de $\prec ABC$, por lo tanto $\prec OBO_a = 90^0$ y entonces $\prec OBF = \prec BO_aI$. Por ende $\dfrac{BI}{OF} = \dfrac{OaI}{BF}$ y usando (1.25) y $BD = BF$,

$$\frac{CE}{r} = \frac{r_a}{BD},$$

es decir

$$CE \cdot BD = r \cdot r_a. \tag{1.27}$$

Finalmente, multiplicando (1.26) y (1.27) y usando (1.23)

$$\frac{(s-a)(s-b)(s-c)}{s} = \frac{AF \cdot BD \cdot CE}{s} = r^2,$$

de donde

$$r = \sqrt{\frac{(s-a)(s-b)(s-c)}{s}}.$$

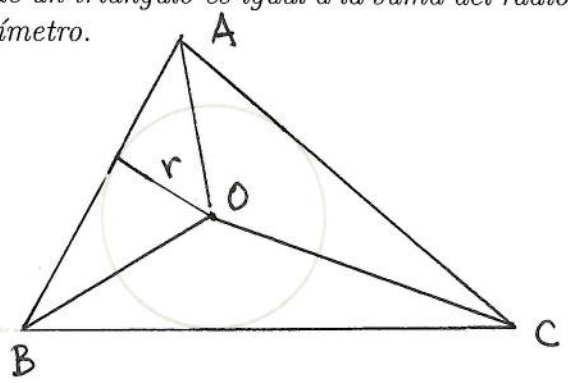
Por otra parte, despejando r_a en (1.27)

$$r_a = \frac{BD \cdot CE}{r} = \frac{(s-b)(s-c)}{\sqrt{\frac{(s-a)(s-b)(s-c)}{s}}} =$$

$$= \sqrt{\frac{s(s-b)^2(s-c)^2}{(s-a)(s-b)(s-c)}} = \sqrt{\frac{s(s-b)(s-c)}{s-a}}.$$

Las otras igualdades se prueban análogamente.

Lema 1.28 *El área de un triángulo es igual a la suma del radio de su círculo inscrito y su semiperímetro.*



Demostración: Sean ABC un triángulo, $\mathcal{C}$ su círculo inscrito, r el radio y O el centro de $\mathcal{C}$ y s el semiperímetro del triángulo ABC. Si denotamos por $\mathcal{A}_{EDF}$ el área del triángulo EDF, entonces

$$\mathcal{A}_{ABC} = \mathcal{A}_{AOB} + \mathcal{A}_{BOC} + \mathcal{A}_{COA}.$$

Como la altura del triángulo AOB es el radio r del círculo $\mathcal{C}$, tenemos que $\mathcal{A}_{AOB} = \dfrac{AB \cdot r}{2}$. Análogamente $\mathcal{A}_{BOC} = \dfrac{BC \cdot r}{2}$ y $\mathcal{A}_{COA} = \dfrac{CA \cdot r}{2}$ y entonces

$$\begin{aligned} \mathcal{A}_{ABC} &= \frac{AB \cdot r}{2} + \frac{BC \cdot r}{2} + \frac{CA \cdot r}{2} = \\ &= \frac{AB + BC + CA}{2} r = sr. \end{aligned}$$

Teorema 1.29 (Fórmula de Herón) *El área de un triángulo ABC con lados a, b, c y semiperímetro s es*

$$\mathcal{A}_{ABC} = \sqrt{s\,(s-a)\,(s-b)\,(s-c)}.$$

Demostración: Sea r el radio del círculo inscrito. Como por el teorema 1.27

$$r = \sqrt{\frac{(s-a)\,(s-b)\,(s-c)}{s}}$$

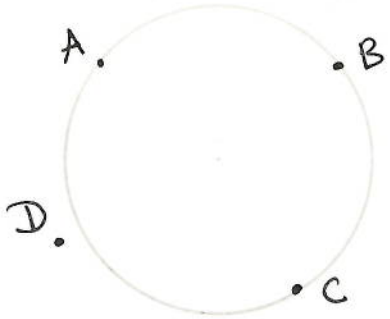
del lema anterior obtenemos

$$\mathcal{A}_{ABC} = s\sqrt{\frac{(s-a)\,(s-b)\,(s-c)}{s}} = \sqrt{s\,(s-a)\,(s-b)\,(s-c)}.$$

1.6 Cuadriláteros cíclicos

Un polígono es cíclico si todos sus vértices están en un círculo.

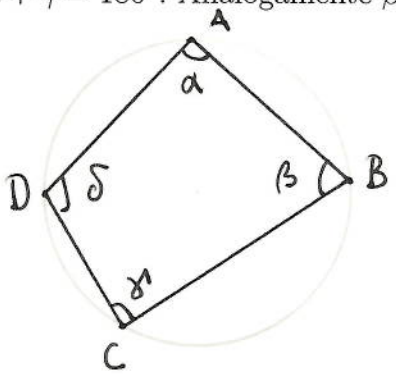
Hemos visto que cualquier triángulo es cíclico, pero no todo cuadrilátero lo es. Para verlo basta tomar tres puntos A, B y C en un círculo $\mathcal{C}$ y otro D fuera de $\mathcal{C}$, pues si existiera otro círculo $\mathcal{C}'$ que contuviera a los cuatro puntos dados, debería ser $\mathcal{C}$ pues los tres puntos A, B y C determinan un único círculo.

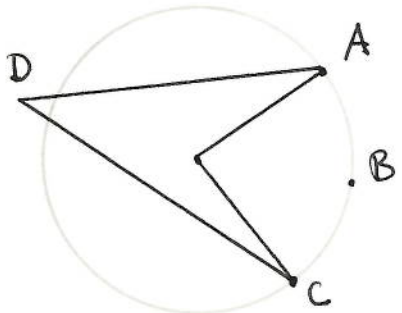


En esta sección daremos condiciones necesarias y suficientes para que un cuadrilátero sea cíclico y veremos algunas de sus propiedades.

Proposition 1 *Un cuadrilátero convexo es cíclico si y sólo si la suma de cada par de ángulos opuestos es igual a* 180^0.

Demostración: Sea $ABCD$ un cuadrilátero con ángulos α, β, γ y δ. Si es cíclico entonces los ángulos α y γ subtienden la cuerda BD pero de lados opuestos y por la observación que sigue del teorema del ángulo central $\alpha + \gamma = 180^0$. Análogamente $\beta + \delta = 180^0$.





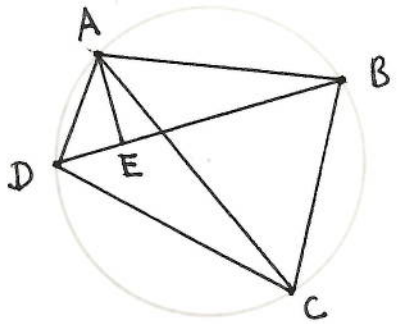
Supongamos ahora que $\alpha + \gamma = 180^0$ y $\beta + \delta = 180^0$ y sean $\mathcal{C}$ el círculo que pasa por A, B y C y O su centro. Si D no perteneciera a $\mathcal{C}$, entonces, usando las proposiciones 1.20 y 1.21, $2\delta \neq \prec COA$ y como $2\beta = \prec AOC$

tendríamos que $2\delta + 2\beta \neq 360^0$ lo que contradice que $\beta + \delta = 180^0$. Por lo tanto D también está en $\mathcal{C}$ y el cuadrilátero es cíclico.

Ptolomeo (150 DC) probó el siguiente teorema sobre los cuadriláteros cíclicos.

Teorema 1.30 (de Ptolomeo) *El producto de las diagonales de un cuadrilátero cíclico es igual a la suma de los productos de los lados opuestos.*

Demostración: Sean $ABCD$ un cuadrilátero cíclico y $\mathcal{C}$ el círculo que lo contiene. Sea E sobre la diagonal BD de manera que $\prec DAE = \prec CAB$.



Los triángulos DAE y CAB son semejantes pues $\prec EDA = \prec BCA$ ya que ambos ángulos subtienden el arco $\widehat{BA}$. Por lo tanto $\dfrac{AD}{ED} = \dfrac{AC}{BC}$, es decir

$$AD \cdot BC = ED \cdot AC. \tag{1.28}$$

Por otra parte los triángulos ADC y AEB son semejantes pues

$$\prec DAC = \prec DAE + \prec EAC = \prec EAB$$

y

$$\prec ABE = \prec ABD = \prec ACD$$

ya que subtienden el arco $\widehat{AD}$. Por lo tanto $\dfrac{AB}{BE} = \dfrac{AC}{CD}$, de donde

$$AB \cdot CD = BE \cdot AC. \tag{1.29}$$

Sumando (1.28) y (1.29) obtenemos

$$\begin{aligned} AD \cdot BC + AB \cdot CD &= ED \cdot AC + BE \cdot AC = \\ &= (ED + BE)\, AC = BD \cdot AC \end{aligned}$$

que es lo que deseábamos probar.

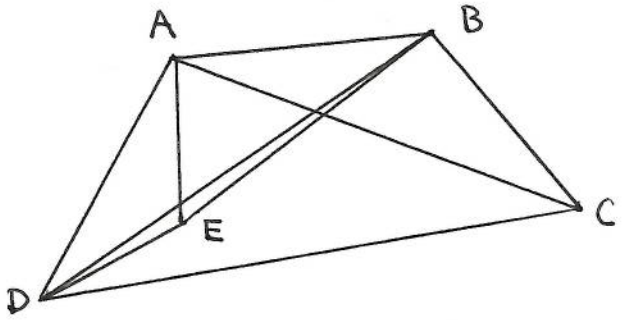
El inverso del teorema de Ptolomeo también es cierto.

Teorema 1.31 *Todo cuadrilátero tal que el producto de las diagonales es igual a la suma de los productos de los lados opuestos es cíclico.*

Demostración: Dado el cuadrilátero $ABCD$ tal que

$$BD \cdot AC = AD \cdot BC + AB \cdot CD \tag{1.30}$$

sea E tal que los triángulos AED y ABC sean semejantes.



Entonces

$$\frac{AD}{AC} = \frac{AE}{AB} = \frac{DE}{BC} \tag{1.31}$$

y

$$\prec DAE = \prec CAB,$$

de donde

$$\frac{AD}{AE} = \frac{AC}{AB}$$

y

$$\prec DAC = \prec DAE + \prec EAC = \prec EAB$$

y entonces por la proposición 1.14 los triángulos AEB y ADC son semejantes. Obtenemos así que

$$\frac{AB}{BE} = \frac{AC}{CD} \tag{1.32}$$

y como en la prueba del teorema de Ptolomeo de (1.31) y (1.32) deducimos que

$$AD \cdot BC + AB \cdot CD = (DE + EB)\, AC,$$

que junto con la igualdad (1.30) nos da

$$DE + EB = BD,$$

lo que significa que E es colineal con B y D y por lo tanto

$$\prec ADB = \prec ACB$$

y D está en círculo generado por A, B y C.

Proposición 1.32 *Si $ABCD$ es un cuadrilátero cíclico con lados $a = AB$, $b = BC, c = CD$ y $d = DA$ y E es la intersección de las diagonales AC y BD entonces*

$$abDE = cdBE.$$

Demostración: Los triángulos ADE y BCE son semejantes porque $\prec EDA = \prec BCE$, ya que ambos subtienden el arco $\widehat{BA}$, y, al ser opuestos por el vértice, $\prec ADE = \prec CEB$. Por lo tanto

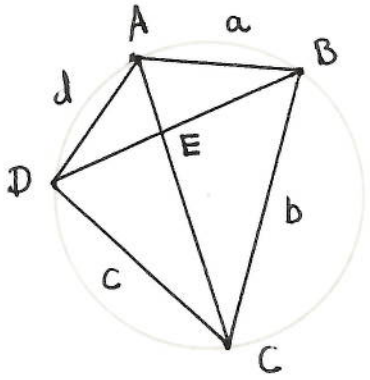
$$\frac{CE}{DE} = \frac{b}{d}. \tag{1.33}$$

Por otra parte se prueba de manera análoga que los triángulos DCE y ABE son también semejantes, de donde

$$\frac{CE}{BE} = \frac{c}{a}. \tag{1.34}$$

Despejando CE en las ecuaciones (1.33) y (1.34) e igualándolas obtenemos $\frac{bDE}{d} = \frac{cBE}{a}$, es decir

$$abDE = cdBE.$$



Proposición 1.33 *Si $ABCD$ es un cuadrilátero cíclico con lados $a = AB$, $b = BC, c = CD$ y $d = DA$ entonces*

$$\frac{AC}{BD} = \frac{ad + bc}{ab + cd}.$$

Demostración: Si E es la intersección de las diagonales AC y BD, por la proposición 1.32 tenemos

$$abDE = cdBE. \tag{1.35}$$

De manera análoga se prueba también

$$bcAE = adCE. \tag{1.36}$$

Si le sumamos $cdDE$ a los dos lados de la igualdad (1.35) obtenemos

$$(ab + cd)\, DE = cd\,(DE + BE) = cdBD$$

y si le sumamos $bcCE$ a los dos lados de la igualdad (1.36),

$$bcAC = bc\,(AE + CE) = (ad + bc)\, CE.$$

Haciendo el cociente de las dos últimas igualdades,

$$\frac{bcAC}{cdBD} = \frac{(ad + bc)\, CE}{(ab + cd)\, DE}$$

y como $\dfrac{CE}{DE} = \dfrac{b}{d}$ por la semejanza de los triángulos ADE y BCE (ver (1.33)), tenemos el resultado deseado.

1.7 Ejercicios

1. El segmento entre los puntos medios de dos lados de un triángulo mide la mitad de la longitud del tercer lado y es paralelo a ese lado.

2. Pruebe el la proposición 1.13 usando el lema 1.11.

3. Pruebe la proposición 1.14 usando la ley de los cosenos.

4. Pruebe que dos triángulos rectángulos que tienen la hipotenusa y un cateto iguales son congruentes.

5. Pruebe que si ABC es un triángulo isósceles con lados iguales AB y AC y D es el pie de la altura sobre BC, entonces $BD = DC$ y $\prec BAD = \prec DAC$.

6. Pruebe que las alturas correspondientes de dos triángulos semejantes tienen la misma razón que los lados correspondientes

7. Para ver que dos triángulos isósceles son semejantes basta comprobar la igualdad de uno de sus ángulos. ¿Cuál y porqué?

8. Para ver que dos triángulos rectángulos son semejantes basta comprobar la igualdad de uno de sus ángulos. ¿Cuál y porqué?

9. Pruebe que la altura sobre la hipotenusa de un triángulo rectángulo divide el triángulo en dos triángulos semejantes entre sí.

10. Pruebe que si unimos los puntos medios de los lados de un triángulo obtendremos un triángulo semejante al triángulo dado. ¿Cuál es la razón de semejanza?

11. Pruebe que el punto mediano del triángulo es el punto de trisección de cada mediana.

12. Enuncie y pruebe el recíproco de la proposición 1.22.

13. Pruebe el corolario 1.25.

14. Verifique numéricamente el teorema de Ptolomeo para cada uno de los siguientes cuadriláteros inscritos en un círculo de radio uno.

    a) Un cuadrado

    b) Un trapecio isósceles uno de cuyos lados es un diámetro y sus otros tres lados son iguales.

    c) Un rectángulo cuyas dimensiones están en la relación 2:1.

15. Demuestre que el teorema de Ptolomeo aplicado a un rectángulo da el teorema de Pitágoras.

16. Sean AB el diámetro de un círculo con centro en O y C un punto en el círculo tal que $\prec BOC = 60^0$. Si el diámetro del círculo mide 5 unidades, ¿cuánto mide la cuerda AC?

17. Sean $\mathcal{C}_1$ y $\mathcal{C}_2$ dos círculos de radios 10 y 17 unidades respectivamente. Si los círculos se intersectan de tal manera que la cuerda común tiene una longitud de 16 unidades, ¿cuál es la distancia entre los centros de los círculos?

18. Los lados de un triángulo ABC están en razón $2 : 3 : 4$. Si AC es el lado más corto, D es el punto en AC tal que BD es la recta que bisecta el ángulo en B y la longitud de AC es 10, ¿cuál es la longitud de los segmentos AD y DC?

19. Sea $ABCD$ un rectángulo de lados 5 y 3 y E y F los puntos que dividen la diagonal AC en tres partes iguales. Encuentre el área del triángulo BEF.

20. En un triángulo ABC las medianas AM y CN sobre los lados BC y AB, respectivamente, se intersectan en el punto O. Si P es el punto medio del lado AC y MP intersecta a CN en el punto Q, encuentre el área del triángulo ABC en términos del área del triángulo OMQ.

21. Sea ABC un triángulo equilátero de lado s. Se inscribe un círculo en el triángulo y un cuadrado en el círculo. Encuentre el área del cuadrado.

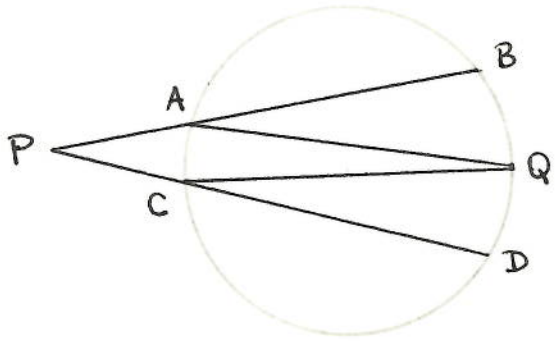
22. Sea ABC el triángulo circunscrito a un círculo de radio r. Si el perímetro del triángulo ABC es p y el área es k, encuentre $\frac{p}{k}$ en términos de r.

23. Sean $\mathcal{C}$ un círculo, AB un diámetro de $\mathcal{C}$ y AD y BC tangentes a $\mathcal{C}$ que se intersecten en un punto de $\mathcal{C}$. Si $AD = a$ y $BC = b$ con $a \neq b$, encuentre AB.

24. Un triángulo equilátero y un hexágono regular tienen el mismo perímetro. Encuentre el área del hexágono si el área del triángulo es a.

25. Si un triángulo tiene área numéricamente igual al perímetro, encuentre el radio del círculo inscrito.

26. Si los puntos A, B, Q, D y C están el círculo como se muestra en el dibujo y las medidas de los arcos $\widehat{BQ}$ y $\widehat{QD}$ son 42^0 y 35^0 respectivamente. Encuentre la suma de los ángulos en P y Q.



27. En un triángulo ABC, el punto F divide al lado AC en la razón $1:2$. Si G es el punto medio de BF y E es el punto de intersección de BC y AG, ¿en qué razón divide E al segmento BC.

Bibliografía

[1] E. Antoniano "Geometría ¿para qué?". Editorial Limusa, 1984.

[2] C.T. Salkind and J.M. Earl "The contest problem book III, annual high school contests 1966-1972". The Mathematical Association of America, 1973.

[3] L.S. Shively "Introducción a la Geometría Moderna". CECSA, 1963.

Capítulo 2

Divisibilidad

2.1 Introducción[1]

Estas notas están hechas para acompañar uno de los cursos introductorios diseñados para profesores interesados en las materias que suelen ser el tema de las Olimpiadas de Matemáticas, el curso de Teoría de Números.

Su contenido esencial es la divisibilidad de los números enteros, que desde la época de los griegos ha sido materia de estudio y un campo vasto para aquellos que quieren probar su ingenio.

Las notas no pretenden cubrir el tema completo ni mucho menos, son solamente una guía para poder seguir el curso; el lector interesado podrá encontrar muchos textos excelentes para adentrarse en la materia.

2.2 Divisibilidad

2.2.1 El algoritmo de la división

En esta sección trataremos el tema de divisibilidad de los números enteros

$$\{..., -3, -2, -1, 0, 1, 2, 3, ...\}$$

y más en particular de los números naturales

$$\{1, 2, 3, ...\}.$$

[1]Notas de Helga Fetter Nathansky

Definición 2.1 *Sean a y b dos números enteros con $a \neq 0$.. Diremos que a* ***divide*** *a b si $\frac{b}{a}$ es un número entero c ó equivalentemente si podemos escribir $b = a \cdot c$. Decimos que b es un* ***múltiplo*** *de a y también que a es un* ***divisor*** *de b. Usaremos la notación a/b.*

De esta definición inmediatamente podemos obtener los resultados siguientes:

Teorema 2.2 *Sea $a \neq 0$.*

1. *a/b implica que a/bc para cualquier entero c.*
2. *Si $b \neq 0$ entonces a/b y b/c implican a/c.*
3. *Si $a \neq 0$, entonces a/b y b/a implican $a = \pm b$.*
4. *Si $a/b, a > 0, b > 0$ entonces $a \leq b$.*

Demostración: 1. Si a/b entonces existe un entero d tal que $b = a \cdot d$. Luego $bc = (a \cdot d) \cdot c = a \cdot (d \cdot c)$, es decir a/bc.

2. Como a/b y b/c existen enteros d y e tales que $b = a \cdot d$ y $c = b \cdot e$. Consecuentemente $c = (a \cdot d) \cdot e = a \cdot (d \cdot e)$ de lo cual se concluye que a/c.

3. Existen enteros d y e tales que $b = a \cdot d$ y $a = b \cdot e$. Luego $a = (a \cdot d) \cdot e = a \cdot (d \cdot e)$. Dividiendo ambos lados por a obtenemos $1 = d \cdot e$, es decir ó $d = e = 1$ ó $d = e = -1$. En el primer caso $a = b$ y en el segundo $a = -b$.

4. Existe un entero $d > 0$ tal que $b = d \cdot a$. Por lo tanto $d \geq 1$ ó equivalentemente $b \geq a$.

De aquí en adelante $a, b, c, ..., x, y, ...$ siempre denotarán números enteros y si escribimos a/b siempre daremos por sentado que $a \neq 0$. Además, cuando no se preste a confusión, escribiremos ab en lugar de $a \cdot b$ para indicar la multiplicación de a por b.

Ejercicios

1. Demuestre que si a/b y a/c, entonces $a/(bx + cy)$ para cualesquiera enteros x y y.

2. Demuestre que si a/b y $a > 0, b > 0$, entonces $a \leq b$.

Teorema 2.3 (Algoritmo de la división) *Dados dos enteros cualesquiera a y b con $a > 0$ existen dos enteros q y r con $0 \leq r < a$ tales que*

$$b = qa + r. \tag{2.1}$$

Demostración: Fijémonos en la sucesión

$$....b - 3a, b - 2a, b - a, 0, b + a, b + 2a, b + 3a, ...$$

Como $a > 0$, los números de la forma na tienden a infinito cuando n recorre los valores $1, 2, 3, ...$y de aquí vemos los números de la forma $b - na$ tienden a menos infinito y los de la forma $b + na$ tienden a infinito. Por esta razón y observando que $b + na = b - (-n)\, a$ debe haber algún entero q tal que

$$b - (q + 1)\, a < 0 \leq b - qa = r.$$

Por definición se satisfacen 2.2 y $0 \leq r$. Además de $b - (q + 1)\, a < 0$, se deduce que

$$0 > b - qa - a = r - a,$$

es decir, $r < a$.

2.2.2 Máximo común divisor

Definición 2.4 *Sean a y b números enteros. Diremos que un número entero d es un **divisor común** de a y b si d/a y d/b.*

Si $|a|$ denota el valor absoluto de a, como tanto $d \leq |a|$ como $d \leq |b|$, resulta que el número de divisores comunes de a y b es finito, lo cual nos permite hacer la siguiente definición:

Definición 2.5 *El **máximo común divisor** de a y b denotado por (a, b) es el mayor de los divisores positivos comunes de a y b. Si $(a, b) = 1$ se dice que a y b son **primos entre sí**.*

De esta definición se deduce de inmediato que

$$(a, b) = (a, -b) = (-a, b) = (-a, -b)\,.$$

Para calcular el máximo común divisor entre a y b bastará listar los divisores positivos de cada uno de ellos y ver cuál es el número mayor que aparece en la lista.

Ejemplos

- Encontrar el máximo común divisor entre -124 y 310.

  Los divisores positivos de -124 son: $1, 2, 4, 31, 62, 124$ y los de 230 son $1, 2, 5, 10, 31, 62, 165, 310$.

  Entonces los divisores comunes positivos de -124 y 310 son $1, 2, 31$ y 62 y por lo tanto $(124, 310) = 62$.

- Demuestre que si $a = bq + r$, entonces $(a, b) = (b, r)$.

  Si d/a y d/b. por el ejercicio 1 de la página 46, $d/(a - bq)$ y también si f/b y f/r entonces $f/(bq + r)$ ó dicho de otro modo, si d/a y d/b entonces d/r, y si f/b y f/r entonces f/a. Hemos probado que el conjunto de los divisores comunes de a y b es el mismo que el conjunto de divisores comunes de b y r. Consecuentemente $(a, b) = (b, r)$.

Sin embargo para calcular el máximo común divisor entre a y b podemos proceder de otra manera, aplicando el algoritmo de la división repetidas veces como veremos enseguida:

Teorema 2.6 (Algoritmo de Euclides) *Sean a y b naturales. Consideremos la lista siguiente:*

$a = bq_1 + r_1$ *donde* $0 \leq r_1 < b$.

$b = r_1q_2 + r_2$ *donde* $0 \leq r_2 < r_1$.

$r_1 = r_2q_3 + r_3$ *donde* $0 \leq r_3 < r_2$.

.....

$r_{m_0-3} = r_{m_0-2}q_{m_1} + r_{m1}$.

$r_{m_0-2} = r_{m_0-1}q_{m_0} + r_{m_0}$.

$r_{m_0-1} = r_{m_0}q_{m_0+1} + 0$.

En esta lista obtenemos el emésimo miembro mediante el algoritmo de la división, encontrando el residuo que se obtiene al dividir r_{m-2} por r_{m-1}. Como en este proceso se tiene que $r_1 > r_2 > \ldots$ y todos los residuos son no negativos, hay un momento en el que $r_{m_0+1} = 0$. Entonces se tiene que $(a, b) = r_{m_0}$.

Demostración: Aplicando el segundo ejemplo de la página 48 repetidas veces tenemos que

$$(a,b) = (b,r_1) = (r_1,r_2) = \ldots (r_{m_0-1}, r_{m_0}) = r_{m_0}$$

donde la última igualdad se obtiene de que r_{m_0-1} es múltiplo de r_{m_0}.

Del teorema anterior de inmediato podemos sacar la siguiente consecuencia:

Lema 2.7 *Sea a un número natural. Entonces $(a, a+1) = 1$.*

Demostración: Usando el algoritmo de Euclides tenemos que

$$a+1 = a \cdot 1 + 1, a = 1 \cdot a + 0,$$

y de aquí tenemos el resultado que queremos.

A continuación daremos una caracterización del máximo común divisor, que si bien no es de mucha ayuda para hallarlo, sí es muy útil para aplicaciones teóricas.

Teorema 2.8 *Si $d = (a,b)$, entonces existen enteros x_0 y y_0 (que pueden ser negativos), tales que*

$$d = ax_0 + by_0.$$

Es más, d es el mínimo valor positivo de las expresiones $ax + by$ cuando x y y recorren todos los números enteros.

Demostración: Despejando en las últimas ecuaciones del teorema anterior y sustituyendo, se tiene

$d = r_{m_0} = r_{m_0-2} - r_{m_0-1}q_{m_0}$ y como

$r_{m_0-1} = r_{m_0-3} - r_{m_0-2}q_{m_0-1}$,

$d = r_{m_0-2} - (r_{m_0-3} - r_{m_0-2}q_{m_0-1})\, q_{m_0} = r_{m_0-2}\,(1 + q_{m_0-1}q_{m_0}) - r_{m_0-3}$.

Siguiendo este método repetidas veces, obtenemos que

$d = x_m r_m + y_m r_{m-1}$ para $m = m_0, m_0 - 1, ..., 2, 1$

donde cada x_m y cada y_m es un entero que depende de las q_i.

Finalmente llegamos a que

$d = x_1 r_1 + y_1 r_2$ y como

$r_2 = b - r_1 q_2$ y

$r_1 = a - bq_1$, combinando todo esto se tiene que

$$d = x_1 r_1 + y_1 (b - r_1 q_2) = y_1 b + r_1 (x_1 - y_1 q_2) =$$
$$= y_1 b + (a - bq_1)(x_1 - y_1 q_2),$$
$$d = a(x_1 - y_1 q_2) + b(y_1 + y_1 q_2 - q_1 x_1).$$

Si $x_0 = x_1 - y_1 q_2$ y $y_0 = y_1 (1 + q_2) - q_1 x_1$, podemos escribir

$$d = ax_0 + by_0.$$

Si ahora $e = ax + by$ y $e > 0$; como $a = dA$ y $b = dB$ para ciertos enteros A y B, obtenemos que $e = dAx + dBy = d(Ax + By)$, o sea que d/e y como $e > 0$, esto significa que $d \leq e$ (ver ejercicio 2 de la página 47), es decir que d es la mínima expresión positiva de la forma $ax + by$.

También se puede proceder al revés: Sea $l = ax_0 + by_0$ la mínima expresión positiva de la forma $ax + by$. Veremos que l/a y l/b.

Usando el algoritmo de la división supongamos que $a = lu + r$ con $0 \leq r < l$. Entonces

$$r = a - lu = a - (ax_0 + by_0) = a(1 - x_0) - by_0.$$

Como $r < l$, y l es la mínima expresión positiva de la forma $ax + by$, r no puede ser positivo, de manera que $r = 0$, $a = lu$ y l/a. De la misma forma se ve que l/b. Con esto queda establecido que l es un divisor común positivo de a y b. Comprobaremos ahora que es el mínimo. Sea $d = (a, b)$ y supongamos que $a = dA$ y $b = dB$. Entonces $l = dAx_0 + dBy_0 = d(Ax_0 + By_0)$. Consecuentemente d/l de lo cual se deduce que $d \leq l$. Por otro lado tanto l como d son divisores comunes de a y b y d es el máximo de los divisores comunes; entonces $l \leq d$ y por lo tanto $l = d$.

Ejemplo

- Calcule $d = (238, 117)$ y exprese a d como combinación de la forma $238x + 117y$.

  $238 = 117 \cdot 2 + 4$

  $117 = 4 \cdot 29 + 1$

  $4 = 4 \cdot 1 + 0.$

  Consecuentemente $(238, 117) = 1$. Además tenemos que

  $1 = 117 - 4 \cdot 29$

  $4 = 238 - 117 \cdot 2$ y de aquí

  $1 = 117 - (238 - 117 \cdot 2)\, 29 = 238 \cdot (-29) + 117 \cdot (59)\,.$

2.2.3 Propiedades del máximo común divisor

Veremos algunas características del máximo común divisor que pueden sernos útiles para calcular más expeditamente este número.

Teorema 2.9 *Sean a, b números enteros.*

(a) Si $d = (a, b)$ y e es cualquier divisor común de a y b, entonces d/e.

(b) Sea $k > 0$ un número natural y a y b enteros. Entonces

$$(ka, kb) = k\,(a, b)\,.$$

(c) Si h/a y h/b y $h > 0$, entonces

$$\left(\frac{a}{h}, \frac{b}{h}\right) = \frac{1}{h}\,(a, b)\,.$$

Demostración: (a) Por el teorema 2.8, $d = ax_0 + by_0$ y por el ejercicio 1 de la página 46, si e/a y e/b, entonces $e/\,(ax_0 + by_0) = d$ y esto finaliza la prueba de (a).

(b) (ka, kb) es el mínimo número positivo de la forma $kax + kby$ que a su vez es k veces el mínimo número positivo de la forma $ax + by$, o sea es igual a $k\,(a, b)$, con lo cual queda probado (b).

Para demostrar (c) usamos (b):

$$(a,b) = \left(h\frac{a}{h}, h\frac{b}{h}\right) = h\left(\frac{a}{h}, \frac{b}{h}\right)$$

y dividiendo ambos lados por h tenemos el resultado deseado.

A continuación daremos uno de los resultados más importantes en la teoría de la divisibilidad:

Teorema 2.10 *Sean a, b y c enteros. Supongamos que c divide a ab y que $(b,c) = 1$. Entonces c divide a a.*

Demostración: Por el teorema anterior parte (b) tenemos

$$(ab, ac) = a\,(b,c) = a.$$

Como c es un divisor común de ab y de ac por el teorema anterior parte (a), resulta que $c/\,(ab, ac) = a$.

Corolario 2.11 *Sean $a_1, a_2, ..., a_n$ y c enteros. Supongamos que c divide a $a_1 \cdot a_2 \cdot ... \cdot a_n$, que $r \leq n$ y que $(a_i, c) = 1$, $i = 1, 2, ..., n$, $n \neq r$. Entonces c/a_r.*

Ejemplo

- Muestre que para cualquier natural n, los números $n^2 + n - 1$ y $n^2 + 2n$ son primos entre sí.

  Usando el algoritmo de Euclides obtenemos que

  $n^2 + 2n = (n^2 + n - 1) \cdot 1 + (n + 1)\,,$

  $n^2 + n - 1 = (n + 1)\,(n - 1) + n,$

  $n + 1 = n \cdot 1 + 1.$

Ejercicios

1. Usando el algoritmo de Euclides encuentre el máximo común divisor de

   (a) 2689 y 4001

   (b) 2947 y 3997

2. Encuentre los valores de x y y que satisfagan

   (a) $486x + 198y = 18$

   (b) $27x - 66y = 3$

3. Demuestre el corolario 2.11.

4. Si definimos a (a, b, c) como el máximo común divisor de a,b y c demuestre que $(a, b.c) = ((a, b), c)$.

5. Pruebe que si $(a, 4) = 2$ y $(b, 4) = 2$ entonces $(a + b, 4) = 2$.

2.2.4 El mínimo común múltiplo y sus propiedades

Muy ligado al concepto de máximo común divisor está el de mínimo común múltiplo de dos enteros. Es claro que si a y b son dos números enteros, $a \cdot b$ es múltiplo tanto de a como de b, es decir $a \cdot b$ es múltiplo común de a y b. Con esto en mente formulamos la siguiente definición:

Definición 2.12 *Si a y b son números enteros, el menor de los múltiplos positivos de a y b se llama el* ***mínimo común múltiplo de*** *a y b y se denota por m.c.m de a y b ó por $[a, b]$.*

Tenemos un resultado semejante para el mínimo común múltiplo al que se obtuvo en el teorema 2.9 para el máximo común divisor.

Teorema 2.13 *Sean a y b enteros. Entonces*

(a) *Si h es cualquier múltiplo común de a y b, y $m = [a, b]$, entonces m/h. Como es claro que si h es tal que m/h entonces h es múltiplo común de a y b, resulta que el conjunto de múltiplos comunes de a y b es el que consta de los números*

$$, ..., -3m, -2m, -m, 0, m, 2m, 3m, ...$$

(b) *Si* $k > 0$, *entonces* $[ka, kb] = k\,[a, b]$.

Demostración: (a) Sea h un múltiplo común de a y b. Entonces, por el algoritmo de la división,

$$h = qm + r$$

donde $0 \leq r < m$. Como a/h y también a/m, por el ejercicio 1 de la página 46 resulta que a/r. De la misma manera obtenemos que b/r, de lo cual resulta que r es múltiplo común de a y b. Como m es el mínimo común múltiplo positivo y $0 \leq r < m$, a r no le queda más que ser igual a 0 y consecuentemente $h = qm$.

(b) Sean $k > 0$, $m = [a, b]$ y $l = [ka, kb]$. Como a/m y b/m resulta que ka/km y kb/km lo cual nos dice que km es un múltiplo común de ka y kb. por (a) deducimos que l/km. Como l es múltiplo de ka en particular lo es de k y podemos escribir $l = kc$ donde c es un número natural. Entonces como l es múltiplo común de ka y de kb, tenemos que ka/kc y kb/kc, es decir a/c y b/c. Por (a) resulta que m/c, o sea que $km/kc = l$. De aquí concluimos que $km = l$.

Ejercicio

1. Calcule (a, b) y $[a, b]$ si a y b son números naturales tales que a/b.

2.3 Los números primos

Uno de los conceptos más importantes relacionados con la divisibilidad de los números enteros es el de número primo. De hecho, como veremos en esta sección, los números primos son los ladrillos a partir de los cuales se pueden construir todos los números enteros.

Definición 2.14 *Un entero* $p > 1$ *se llama número* ***primo*** *si sus únicos divisores son* ± 1 *y* $\pm p$. *A los números de la forma* $-p$ *con* p *primo se les llama primos negativos. y los enteros distintos de* ± 1 *que no son ni primos ni primos negativos se llaman* ***números compuestos***.

Como vemos, un número p natural mayor que 1 es primo si no se puede expresar de la forma $a \cdot b$ con a, b naturales ambos distintos de 1, es decir p no es múltiplo de ningún natural menor que p que no sea 1.

Supongamos ahora que $p/a_1a_2...a_n$. Si p no divide a a_1, por el argumento anterior $p/a_2...a_n$; si p tampoco divide a a_2 entonces, nuevamente por el argumento anterior, $p/a_3...a_n$. Proseguimos así hasta hallar una $i \leq n$ tal que p/a_i. Esta i siempre existe, pues si en el peor de los casos obtuvimos que p no divide ni a a_1 ni a a_2 ... ni a a_{n-1} resulta que entonces p/a_n.

A continuación probaremos el resultado principal de esta sección que nos asegura que todo entero m se puede expresar de manera única de la forma

$$m = \pm p_1p_2...p_r$$

donde cada p_i es un número primo no necesariamente distinto de los demás y la unicidad se interpreta en el sentido de que en cualquier otra expresión de m como producto de primos aparecen exactamente los mismos primos que en la primera y con la misma multiplicidad (es decir se repiten el mismo número de veces); la única diferencia puede ser el orden en que aparecen estos primos.

Ejemplo

- $225 = 5 \cdot 5 \cdot 3 \cdot 3 = 3 \cdot 5 \cdot 3 \cdot 5$.

Teorema 2.16 (fundamental de la aritmética) *Todo número natural distinto de* 1 *se puede factorizar de manera única como producto de primos.*

Demostración: Primero veremos que todo natural se puede factorizar en primos, después nos ocuparemos de la unicidad.

Sea n un natural cualquiera distinto de 1. Como los números de la forma $2^m = 2 \cdot 2 \cdot ... \cdot 2$ (m factores) tienden a infinito, existe algún natural m tal que $n \leq 2^m$.

Si n es primo ya está descompuesto como producto de primos con un solo factor. Si no es primo, $n = a \cdot b$ donde a y b son dos naturales mayores o iguales a 2; es decir $n \geq 2 \cdot 2$. Si a y b son primos ya terminamos; si alguno de los dos no lo es entonces podemos escribir a n como un producto de 3 enteros c, d y e todos ellos mayores ó iguales a 2, lo cual significa que $n = c \cdot d \cdot e \geq 2 \cdot 2 \cdot 2$.

Si c, d y e son primos si no alguno de ellos se puede expresar como un producto de dos factores mayores ó iguales a 2 y así n es un producto de 4 factores todos mayores ó iguales a 2 lo cual significa que $n \geq 2^4$.

2.3.1 La criba de Eratóstenes

¿Cómo podríamos proceder para hallar todos los primos? Esta pregunta ya ocupaba a los antiguos griegos y de hecho fue resuelta por el matemático griego Eratóstenes hacia el año 200 A.C.

El procedimiento es como sigue:

Escribimos en una lista de corrido todos los números naturales:

$$1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, ...$$

Nos fijamos en el primer número primo de la lista que según nuestra definición es 2. Acto seguido quitamos de la lista a todos los múltiplos de 2 mayores que $2 : 4, 6, 8, 10, 12, 14, 16, 18, ...$ y nos quedamos con $1, 2, 3, 5, 7, 9, 11, 13, 15, 17, ...$

El segundo primo será entonces el primer número mayor que 2 que no quitamos, es decir 3, pues 3 no es divisible por 2. Quitamos ahora los múltiplos de 3 mayores que 3 que quedan en la lista: $9, 15, 21, 27, .$ y nos quedamos con, $1, 2, 3, 5, 7, 11, 13, 17, 19, 23, 25, ...$

El siguiente primo es el primer número mayor que 3. que no hemos tachado, a saber 5 ya que 5 no es ni múltiplo de 2 ni de 3. Quitamos ahora los múltiplos de 5 mayores que 5 de la lista anterior quedándonos con $1, 2, 3, 5, 7, 11, 13, 17, 19, 23, ...$ y razonando como antes vemos que el siguiente primo es 7 ya que no es divisible ni por 2, ni por 3, ni por 5.

Siguiendo con este procedimiento puede uno hallar la lista consecutiva de primos. Afortunadamente hoy en día contamos con potentes computadoras para facilitarnos la tarea.

2.3.2 El teorema fundamental de la aritmética

Veremos ahora por qué es tan importante conocer a los números primos, pero para esto necesitamos primero el siguiente resultado:

Teorema 2.15 *Sean $a, b, a_1, a_2, ..., a_n$ números enteros. Si p es un número primo y p/ab entonces ó p/a ó p/b; más generalmente, si $p/a_1a_2...a_n$ entonces p/a_i para alguna $1 \leq i \leq n$ ó dicho con palabras, si un primo divide aun producto, forzosamente divide a uno de los factores.*

Demostración: Como p es primo, si p no divide a a, entonces p y a no pueden tener divisores comunes, es decir $(a, p) = 1$. Como sin embargo p/ab, aplicando el teorema 2.10 concluimos que p/b.

Y así continuamos hasta que n finalmente queda expresado como un producto de primos. Que esto se logra en a lo más m pasos está garantizado por el hecho de que $n \leq 2^m$.

Respecto a la unicidad:

Sea n un natural y supongamos que tenemos dos maneras de escribir a n como producto de primos. Dividiendo entre los primos comunes llegamos, una igualdad de la forma

$$p_1 p_2 ... p_r = q_1 q_2 ... q_s.$$

Si suponemos que el producto anterior no vale 1, entonces existe alguna $p_i \neq 1$ que no aparece en el lado derecho, lo cual es imposible ya que por el teorema 2.15 se tendría que como $p_i / q_1 q_2 ... q_s$ entonces p_i / q_j para alguna j pero q_j es primo. De aquí se deduce que al cancelar los primos que aparecen en ambas expresiones llegamos a que $1 = 1$ y que n tiene una única manera de descomponerse como producto de primos.

Corolario 2.17 *Si n es un número natural mayor que 1, existe una manera única de escribir n de la forma*

$$n = p_1^{m_1} \cdot p_2^{m_2} \cdot ... \cdot p_r^{m_r}$$

con $p_1 < p_2 < ... < p_r$, $r \geq 1$ y $m_i \geq 1$ para $i = 1, ..., r$.

Llamamos a esta descomposición la ***descomposición única como producto de potencias de primos de*** *n.*

Demostración: Simplemente ordenamos los primos que se obtienen en la descomposición de n en el teorema anterior según su magnitud y en lugar de $p \cdot p \cdot ... \cdot p$ (k factores) escribimos p^k en cada instancia.

Corolario 2.18 *Si n es un número natural mayor que 1, n se puede escribir de la forma*

$$n = q_1^{m_1} \cdot q_2^{m_2} \cdot ... \cdot q_l^{m_l}$$

donde $q_1, q_2, ..., q_l$ son los primeros l primos, ordenados por su tamaño y $0 \leq m_i$ para $i = 1, 2, ..., l$.

Demostración: Simplemente tomamos la representación obtenida en el corolario anterior y añadimos los términos de la forma $q_{r_i}^0$, si es que q_{r_i} no aparece en dicha representación.

Observemos que la representación obtenida en el corolario 2.18 no es única pues podemos agregar tantos términos de la forma q_s^0 como queramos.

Del teorema fundamental de la aritmética obtenemos de inmediato la forma de los divisores de un número natural dado.

Lema 2.19 *Sea n un natural distinto de 1 y $n = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$ su factorización única en producto de potencias de primos. Entonces cualquier divisor de n es de la forma $p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_r^{s_r}$ con $0 \leq s_i \leq m_i$ para $i = 1, 2, ..., r$; es más, cualquier divisor de n es de esa forma.*

Demostración: Sea d un divisor de n y supongamos que la descomposición única en producto de potencias de primos de d es $d = q_1^{l_1} \cdot q_2^{l_2} \cdot \ldots q_j^{l_j}$ con $q_1 < \ldots < q_j$. Como d/n, del teorema 2.15 tenemos que q_1 debe de dividir a alguno de los factores de n, es decir que $q_1 = p_{r_1}$ para algún índice $r_1 \geq 1$. Como entonces $\left(q_1^{l_1}, p_i^{m_i}\right) = 1$ si $1 \leq i \leq r, i \neq r_1$, por el corolario 2.11 tenemos que $q_1^{l_1} / p_{r_1}^{m_1}$ lo cual implica que $q_1^{l_1} = p_{r_1}^{l_1}$ y $l_1 \leq m_1$. De la misma manera obtenemos que existe $r_2 > r_1$ tal que $q_2^{l_2} = p_{r_2}^{l_2}$, $l_2 \leq m_2$ y así sucesivamente hasta que llegamos a que $d = p_{r_1}^{l_1} \cdot p_{r_2}^{l_2} \cdot \ldots p_{r_j}^{l_j}$ es la descomposición única de d en producto de potencias de primos. Si tomamos ahora como 0 los exponentes de los p_i que no aparecen en la descomposición anterior, hemos probado la primera afirmación del lema.

La segunda es clara, pues si $d = p_1^{s_1} \cdot p_2^{s_2} \cdot \ldots \cdot p_r^{s_r}$ con $0 \leq s_i \leq m_i$ para $i = 1, 2, ..., r$ entonces $n = d \cdot \left(p_1^{m_1 - s_1} \cdot p_2^{m_2 - s_2} \cdot \ldots \cdot p_r^{m_r - s_r}\right)$ con $m_i - s_i \geq 0$ para $i = 1, 2, ..., r$.

Corolario 2.20 *Si $a = p_1^{m_1} \cdot p_2^{m_2} \cdot \ldots \cdot p_r^{m_r}$ y $b = p_1^{l_1} \cdot p_2^{l_2} \cdot \ldots \cdot p_r^{l_r}$ donde $p_1 < p_2 < \ldots < p_r$ y $m_i, l_i \geq 0$. entonces*

(a) $(a, b) = p_1^{\min\{m_1, l_1\}} \cdot p_2^{\min\{m_2, l_2\}} \cdot \ldots \cdot p_r^{\min\{m_r, l_r\}}$ *donde* $\min\{m_i, l_i\}$ *significa el mínimo de los números m_i y l_i.*

(b) $[a, b] = p_1^{\max\{m_1, l_1\}} \cdot p_2^{\max\{m_2, l_2\}} \cdot \ldots \cdot p_r^{\max\{m_r, l_r\}}$ *donde* $\max\{m_i, l_i\}$ *significa el máximo de los números m_i y l_i.*

Corolario 2.21 *Si a y b son números enteros distintos de 0, entonces $(a, b) \cdot [a, b] = |a \cdot b|$*

Demostración: (c) Como

$$[a, b] = [a, -b] = [-a, b] = [-a, -b]$$

y de la misma manera

$$(a, b) = (a, -b) = (-a, b) = (-a, -b)$$

basta probar esta afirmación para $a > 0$ y $b > 0$.

Pero en este caso el resultado es claro por el corolario anterior, ya que si $\max\{m_i, l_i\} = m_i$, entonces $\min\{m_i.l_i\} = l_i$ y viceversa, si $\max\{m_i, l_i\} = l_i$, entonces $\min\{m_i.l_i\} = m_i$ y consecuentemente $\max\{m_i, l_i\} \cdot \min\{m_i, l_i\} = m_i + l_i$, pero

$$a \cdot b = p_1^{m_1+l_1} \cdot \ldots p_r^{m_r+l_r}.$$

Ejemplo

- Encuentre el mínimo común múltiplo y el máximo común divisor de 482 y 1687.

  Observamos que $482 = 2 \cdot 241$ y que $1687 = 7 \cdot 241$.

  De aquí se concluye que

  $$(482, 1687) = 241y\,[482, 1687] = 2 \cdot 7 \cdot 241 = 3374.$$

- Sean a y b números naturales tales que $(a, b) = 1$ y ab es un cuadrado perfecto. Entonces a y b a su vez son cuadrados perfectos.

  Escribimos a a y b en su expresión única como producto de potencias de primos

  $$a = p_1^{\alpha_1} \ldots p_m^{\alpha_m} \text{ y } b = q_1^{\beta_1} \ldots q_r^{\beta_r}.$$

  Entonces, puesto que a y b son primos entre sí, todas las p_i son distintas de todas las q_j de manera que la expresión única como producto de potencias de primos de ab está dada por

  $$ab = p_1^{\alpha_1} \ldots p_m^{\alpha_m}\ q_1^{\beta_1} \ldots q_r^{\beta_r}.$$

  Como ab es un cuadrado, todos los primos en su descomposición deben de aparecer con potencias pares y esto resuelve el problema.

El resultado siguiente nos muestra que hay una infinidad de primos, lo cual no es obvio a priori, pues si bien la cantidad de números naturales es infinita, también lo es la de cualquier conjunto de la forma $p, p^2, p^3, ...$ donde p es primo y podría darse el caso que cualquier número natural fuera producto de potencias de primos que pertenecieran a un conjunto finito.

Teorema 2.22 (Euclides) *El número de primos es infinito.*

Demostración: Para probar esta afirmación veremos que dada una colección finita de primos siempre podemos hallar un primo que no está en la colección.

Supongamos que tenemos el conjunto de primos $\{p_1, p_2, .., .p_r\}$. Nos fijamos en el número

$$n = p_1 \cdot p_2 \cdot ... \cdot p_r + 1.$$

Por el lema 2.7, $(n, p_1 \cdot p_2 \cdot ... \cdot p_r) = 1$, y de aquí inferimos que ninguno de los primos de la colección divide a n. pero por el corolario 2.17, n se expresa de manera única como

$$n = q_1^{\alpha_1} \cdot ...q_s^{\alpha_s}$$

con $s, \alpha_1 \geq 1$. Entonces q_1 es un primo que no pertenece al conjunto inicial.

Ejercicios

1. Calcule (a, b) y $[a, b]$ si a y b son números naturales tales que a/b.

2. Si $[a, b, c]$ denota al mínimo común múltiplo de a, b y c encuentre todas las ternas de números naturales a, b y c tales que se satisfagan a la vez $(a, b, c) = 10$ y $[a, b, c] = 100$.

3. Si p y q son primos distintos de 2 pruebe que $p^2 + q^2$ no puede ser un cuadrado perfecto.

2.4 Congruencias

El concepto de congruencia surgió originalmente como una especie de taquigrafía para la divisibilidad, la cual ha facilitado enormemente algunas de las tareas de esta área.

Definición 2.23 *Diremos que dos números enteros a y b son* ***congruentes módulo*** *el entero m si $a - b$ es divisible por m y en ese caso escribimos*

$$a \equiv b \,(\mathrm{mod}\, m.)$$

Ejemplo

- Los números de la forma $7, 17, 27, 107, 2347$ todos son congruentes entre sí módulo 10 ya que la diferencia de cualesquiera dos de ellos es un múltiplo de 10.

Lema 2.24 *Sean a, b, c, m números enteros. Entonces*

(a) $a \equiv a \,(\mathrm{mod}\, m)$.

(b) *Si* $a \equiv b \,(\mathrm{mod}\, m)$ *entonces* $b \equiv a \,(\mathrm{mod}\, m)$.

(c) *Si* $a \equiv b \,(\mathrm{mod}\, m)$ *y* $b \equiv c \,(\mathrm{mod}\, m)$ *entonces* $a \equiv c \,(\mathrm{mod}\, m)$.

Demostración: Se le deja al lector.

2.4.1 Propiedades de las congruencias

Las congruencias tienen varias propiedades que son compatible con las de la suma y producto. Con esto lo que queremos decir es lo siguiente:

Teorema 2.25 *Sean a, b, c, d, m números enteros.*

(a) *Si* $0 \leq b < m$ *y* $a \equiv b \,(\mathrm{mod}\, m)$ *entonces b es el residuo que se obtiene al dividir a entre m.*

(b) $a \equiv 0 \,(\mathrm{mod}\, m)$ *si y sólo si* m/a.

(c) *Si* $a \equiv b \,(\mathrm{mod}\, m)$ *y* $c \equiv d \,(\mathrm{mod}\, m)$ *entonces* $a + c \equiv b + d \,(\mathrm{mod}\, m)$ *y* $a - c \equiv b - d \,(\mathrm{mod}\, m)$.

(d) *Si* $a \equiv b \,(\mathrm{mod}\, m)$ *y* $c \equiv d \,(\mathrm{mod}\, m)$ *entonces* $ac \equiv bd \,(\mathrm{mod}\, m)$.

(e) *Si* $a \equiv b \,(\mathrm{mod}\, m)$ *entonces* $a^n \equiv b^n \,(\mathrm{mod}\, m)$.

Demostración: (a) $a \equiv b \pmod{m}$ significa que existe un entero x tal que $a - b = mx$, o lo que es lo mismo, $a = mx + b$ y como $0 \leq b < m$, esto nos indica que b es el residuo que se obtiene al dividir a entre m.

(b) Sale inmediatamente de (a).

(c) $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ implica $m/(a-b)$ y $m/(c-d)$ y por el ejercicio 1 de la página 46, $m/(a+c-(b+d))$ y $m/(a-c-(b-d))$.

(d) Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces existen enteros x y y tales que

$$a = b + mx \text{ y } c = d + my.$$

De aquí tenemos que $ac = bd + m(by + dx + mxy)$, es decir $ac \equiv bd \pmod{m}$.

(d) Esto se obtiene al aplicar el inciso (c) a $a \equiv b \pmod{m}$, obteniendo así $a^2 \equiv b^2 \pmod{m}$, luego se aplica (c) a $a \equiv b \pmod{m}$ y a $a^2 \equiv b^2 \pmod{m}$ lo cual da $a^3 \equiv b^3 \pmod{m}$ y así sucesivamente.

Observemos que en el teorema anterior no mencionamos nada acerca de la división, pues en general **no** es cierto que si $ac \equiv bc \pmod{m}$ entonces $a \equiv b \pmod{m}$, es decir, aunque al dividir entre c dos números e y f congruentes módulo m obtengamos sendos enteros, éstos no tienen que ser congruentes módulo m.

Ejemplo

- $16 \equiv 4 \pmod{12}$, pero $4 \not\equiv 1 \pmod{12}$ pues 12 no divide a $4 - 1$.

Sin embargo, si se satisface una hipótesis adicional sí podemos dividir de ambos lados de la congruencia:

Teorema 2.26 *Sean a, b, c, m números enteros. Si $(c, m) = 1$ entonces de $ac \equiv bc \pmod{m}$ se puede concluir que $a \equiv b \pmod{m}$.*

Demostración: Como $ac \equiv bc \pmod{m}$, tenemos que $m/c(a-b)$. Pero como $(c, m) = 1$ del teorema 2.10 obtenemos que $m/(a-b)$, es decir $a \equiv b \pmod{m}$.

Después de haber analizado algunas de las propiedades de las congruencias, es hora de ver para qué sirven, lo cual mostraremos con unos ejemplos.

Ejemplos

- Calcule el residuo que se obtiene al dividir 7^{52} entre 13.

  $7^2 \equiv 10 \pmod{13}$, consecuentemente

  $$7^4 \equiv 10^2 \pmod{13} \equiv 9 \pmod{13} \tag{2.2}$$

  Por otro lado $9^2 \equiv 3 \pmod{13}$ y

  $$9^3 \equiv 27 \pmod{13} \equiv 1 \pmod{13}, \tag{2.3}$$

  así que $(7^4)^2 = 7^8 \equiv 3 \pmod{13}$ y

  $$7^{16} \equiv 9 \pmod{13}. \tag{2.4}$$

  Por lo tanto usando 2.2, 2.3 y 2.4 obtenemos

  $$7^{52} = \left(7^{16}\right)^3 \cdot 7^4 \equiv 9^3 \cdot 9 \pmod{13} \equiv 1 \cdot 9 \pmod{13} = 9 \pmod{13},$$

  es decir el residuo buscado es 9.

- Pruebe que $10^n \equiv 1 \pmod{3}$ para cualquier número natural n.

  Claramente $10 \equiv 1 \pmod{3}$ y de aquí la conclusión se obtiene de inmediato aplicando el inciso (e) del teorema 2.25 .

- Pruebe que un número natural m es divisible entre 3 si y sólo si la suma de sus cifras es a su vez divisible entre 3.

  La expresión decimal de m está dada de la forma:

  $$m = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0.$$

  Por el ejemplo anterior $10^n \equiv 1 \pmod{3}$ y consecuentemente de (c) y (d) del teorema 2.25 obtenemos que

  $$m \equiv a_n \cdot 1 + ... + a_1 \cdot 1 + a_0 \pmod{3} = a_n + a_{n-1} + ... + a_0 \pmod{3},$$

  de manera que $m \equiv 0 \pmod{3}$ si y sólo si

  $$a_n + a_{n-1} + ... + a_0 \equiv \pmod{3}.$$

- Pruebe que $n^6 - 1$ es divisible entre 7 si $(n, 7) = 1$.

  Si $n \equiv 0 \pmod 7$, $n^6 \equiv 0 \pmod 7$

  Si $n \equiv 1 \pmod 7$, $n^6 \equiv 1 \pmod 7$

  Si $n \equiv 2 \pmod 7$, $n^6 \equiv 1 \pmod 7$

  Si $n \equiv 3 \pmod 7$, $n^3 \equiv 6 \pmod 7 \equiv -1 \pmod 7$ y $n^6 \equiv 1 \pmod 7$

  Si $n \equiv 4 \pmod 7$, $n^3 \equiv 1 \pmod 7$ y $n^6 \equiv 1 \pmod 7$

  Si $n \equiv 5 \pmod 7$, $n^2 \equiv 4 \pmod 7$ y $n^6 \equiv 1 \pmod 7$

  Si $n \equiv 6 \pmod 7$, $n^2 \equiv 1 \pmod 7$ y $n^6 \equiv 1 \pmod 7$

  De aquí observamos que cualquier número que no es divisible entre 7 satisface que $n^6 \equiv 1 \pmod 7$ o, equivalentemente

$$n^6 - 1 \equiv 0 \pmod 7.$$

Ejercicios

1. Pruebe el lema 2.24.
2. Pruebe que $n^3 - n$ es divisible entre 6, y $n^5 - n$ es divisible entre 30.
3. Pruebe que un número $m = a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + ... + a_1 \cdot 10 + a_0$ es divisible entre 11 si y sólo si $\sum_i a_{2i} - \sum_i a_{2i+1}$ es divisible por 11.
4. Encuentre todos los números naturales tales que $2^n + 1$ es divisible entre 3.

Bibliografía

[1] Illanes Mejía Alejandro, "Primeros Pasos en las Olimpiadas de Matemáticas". Revista del Seminario de Titulación y Enseñanza, Vol. IX, Num.76, (1993).

[2] Niven y Zuckerman, "Teoría de los Números". Limusa -Wiley, México (1969).

[3] Oystein Ore, " Invitation to Number Theory". Mathematical Association of America (1967).

Capítulo 3

Combinatoria

3.1 Prefacio[1]

La combinatoria estudia ciertos aspectos enumerativos (o de "conteo") de conjuntos finitos de objetos. Puede por tanto considerarse como una rama, o un conjunto de técnicas, ancladas a la vez en la aritmética y en la teoría de conjuntos (finitos).

Sin embargo, esta descripción es demasiado parca, pues en realidad la combinatoria nos ayuda a resolver una enorme variedad de problemas en muchas ramas, tanto de las matemáticas mismas como de sus aplicaciones. En cierto modo, ese es el objetivo de estas notas: describir el origen y la aplicación de esas técnicas combinatorias, pero más que nada ilustrarlas mediante ejemplos.

Ahora bien, las notas están dirigidas a profesores de enseñanza media superior y no a estudiantes propiamente. Por ello, están escritas en un estilo que quizá no sea el más ortodoxo matemáticamente hablando, ni el más apropiado para la enseñanza directa del conocimiento, pero que me parece un buen compromiso para que se pueda entender la **esencia** de las ideas: es decir, no me dirijo a profesionales de las matemáticas, pero además he incluido material que normalmente no se daría a un estudiante de preparatoria, mas puede ayudar al instructor a responder a algunas de las inquietudes que, en mi opinión, pudieran surgir en la mente de un estudiante inquisitivo.

Por supuesto, una comprensión cabal de cualquier teoría o método matemático sólo se adquiere mediante la práctica, y por ello se incluyen bastantes

[1]Notas de Fausto Ongay Larios

ejercicios, algunos de ellos con solución. Es importante enfatizar aquí que la solución de un problema matemático dado casi nunca es automática y que, en general, no existe un único método de solución, ni siquiera un método óptimo: sólo existen métodos correctos e incorrectos para resolver un problema dado. Por ello, las respuestas que se dan deben considerarse como un referencia, y es conveniente que el lector intente sus propias respuestas

Y aquí, aunque en teoría el número de posibilidades es ilimitado, la imaginación del autor no lo es, y muchos de ellos están extraidos de las fuentes que citamos en la bibliografía (anotada), con cuyos autores estoy en clara deuda.

3.2 Conjuntos finitos

Recordemos ante todo algunas nociones elementales de la teoría de conjuntos:

Primeramente, la propiedad más básica es que los conjuntos están caracterizados por sus elementos. La notación usual para un conjunto es

$$A = \{x \mid x \text{ satisface P}\}$$

donde la variable x denota a los elementos del conjunto A, y P es alguna propiedad que caracteriza a los elementos de A. Por ejemplo, si queremos describir al conjunto P de los números enteros positivos y pares, podemos escribir

$$P = \{x \mid x \text{ es un entero positivo y par}\}$$

(la raya vertical se lee "tales que"). Como hemos dicho, esta relación entre un conjunto y sus elementos es la más fundamental en la teoría de conjuntos; se llama **relación de pertenencia**, y se denota por $\in$. Así por ejemplo, escribimos $2 \in P$.

Conviene señalar que a veces se puede remplazar la escritura explícita de la propiedad P por alguna descripción de otro tipo, pero siempre y cuando ésta sea perfectamente clara: Por ejemplo, si está completamente claro que hablamos de los pares positivos, podemos escribir

$$P = \{x \mid x = 2, 4, 6, 8, ...\};$$

o incluso podemos suprimir la referencia a la variable x y escribir algo como $P = \{2, 4, 6, ...\}$, pero siempre hay que tener cuidado de que no vayamos incurrir en ambigüedades.

Otras nociones básicas de teoría de conjuntos que necesitaremos son las de subconjunto, función y cardinalidad:

Decimos que el conjunto A es subconjunto del conjunto B si todo elemento de A lo es también de B. En tal caso escribimos $A \subset B$. Nótese que por definición, $A \subset B$ si y sólo si para todo $x \in A$ se tiene también $x \in B$.

Intuitivamente hablando, una función f es una relación, o *regla de correspondencia*, entre los elementos de dos conjuntos, digamos A y B, llamados *dominio* y *codominio*, respectivamente, de modo que a cada elemento del dominio A corresponde **uno y sólo un** elemento del codominio B. Más precisamente, una función consta de los tres elementos: dominio, codominio y regla de correspondencia, aunque usualmente se tiene el caso que dominio y codominio quedan claros del contexto, de modo que la única información relevante es la regla de correspondencia (aunque hay que tener presente que la definición involucra a las tres partes).

Hay varias notaciones para una función; la más común es escribir sólo la regla de correspondencia como $y = f(x)$ o simplemente $f(x)$, aunque nosotros utilizaremos también la notación $x \longmapsto f(x)$.

Sin duda, en las aplicaciones el tipo de funciones que más comunmente aparecen son las *funciones reales de variable real,* es decir funciones con dominio y codominio los números reales $\mathbb{R}$, o en otras palabras, que asocian números reales a números reales, como por ejemplo $f(x) = x^2$ ó $f(x) = \ln x$; pero es importante tener siempre presente que la definición es mucho más amplia.

En el caso de una función *biyectiva,* o *correspondencia biunívoca,* se usa la notación $x \leftrightarrow f(x)$. Hagamos una pausa para explicar esta idea: aunque para una función arbitraria f se cumple que $y = f(x)$ está totalmente determinado por x, en general no es cierto que todo y en el codominio esté determinado por x en el dominio, ni que cada y esté determinado por un único x. Cuando la primera condición se cumple, es decir, que todo y está determinado por un x, decimos que la función es *suprayectiva* (o *sobre*); cuando la segunda condición se cumple, es decir, que cada x tiene asociado un único y, decimos que la función es *inyectiva* (ó 1 *a* 1). Es cuando **ambas** condiciones se cumplen que decimos que la función es biyectiva, o que es una *biyección.*

Demos ejemplos de funciones reales de variable real que cumplen una de las condiciones, pero no las dos: por un lado, tenemos la función, $f(x) = x^3 - x$, que es suprayectiva pero no inyectiva, ya que a los dos números distintos 1 y -1 les asocia el mismo valor 0; como ejemplo de una función

inyectiva que no es suprayectiva tenemos la función $f(x) = x/|x+1|$, cuyos valores están en el intervalo $(-1, 1)$.

Ejercicio: Justificar esta última afirmación.

Vagamente hablando, la cardinalidad de un conjunto A, denotada $\sharp A$, es el número de elementos de ese conjunto. La razón por la que esta definición es imprecisa es porque no es *a priori* obvio lo que es el 'número de elementos de un conjunto' para un conjunto arbitrario. Una manera de remediar esto es escoger 'conjuntos tipo', o 'conjuntos representativos', que llamamos *números cardinales*; determinamos entonces la cardinalidad mediante la existencia de una correspondencia biunívoca (o dicho en otras palabras más llanas, un apareamiento) entre un conjunto y algún número cardinal. Aunque se puede argumentar que esta es en efecto la manera en que contamos, y que así puesto no parece que hayamos ganado mayor cosa, pero la ventaja real es que todas estas nociones se pueden definir con precisión dentro de la teoría de conjuntos y, aunque no entraremos en detalle sobre estas construcciones, el resultado neto es que cada conjunto tiene un único cardinal asociado, de modo que su cardinalidad está bien definida. (Conviene sin embargo señalar que, en general, las biyecciones que se pueden encontrar no son únicas; de hecho, como veremos más adelante, en general existen muchas.)

Pero por otro lado y entrando más en materia, algo que es más importante para nosotros es que en particular cada número natural n define uno de estos cardinales, que es justamente el conjunto de todos los números naturales menores o iguales que n. Con esta noción a la mano, podemos definir un conjunto finito como un conjunto cuyo cardinal corresponde a algún número natural n. De acuerdo con nuestra discusión anterior, esto lo que significa es que podemos escoger una correspondencia biyectiva entre los elementos del conjunto y los números del 1 al n.

Sin duda, una propiedad útil de los conjuntos finitos es que en este caso, *al menos en principio*, siempre podemos describir al conjunto de manera explícita listando sus elementos; por ejemplo si $\sharp A = n$, podemos escribir algo como:

$$A = \{a_1, a_2, a_3, ..., a_n\}$$

y notemos que aquí se está describiendo explícitamente un apareamiento entre A y $\{1, 2, ..., n\}$, que podemos representar simbólicamente como sigue:

$$1 \longleftrightarrow a_1, 2 \longleftrightarrow a_2, ..., n \longleftrightarrow a_n,$$

como requiere la definición de cardinalidad.

3.3 Permutaciones (ordenaciones) de un conjunto

Entremos ahora en materia:

La primera propiedad combinatoria de un conjunto que analizaremos son las *permutaciones*, o más precisamente, el *número* de permutaciones de los elementos de ese conjunto. Esta noción, aunque no es la más inmediata que se le ocurre a uno, es ciertamente la más simple de describir y aparecerá con frecuencia en todo lo que sigue.

Sea entonces $A = \{a_1, a_2, a_3, ..., a_n\}$ un conjunto con n elementos. Decimos que las permutaciones de A (o de los elementos de A) son las distintas maneras en que podemos ordenar los elementos de A. En otras palabras, cada permutación es una manera específica (un "*ordenamiento*") en que escribimos los elementos del conjunto A. Cada permutación de los elementos del conjunto A se puede pensar como una forma de aparear los elementos de A con los de su cardinal, es decir, es una manera de establecer una función biyectiva entre A y el conjunto $\{1, 2, ..., n\}$. Esto muestra en efecto que en general hay muchos apareamientos posibles entre dos conjuntos.

Es bastante claro que para determinar uno de estos ordenamientos tenemos n posibilidades para elegir al primer elemento en el orden dado; enseguida, habiendo escogido un primer elemento, tenemos $n - 1$ posibilidades para el segundo, ya que ahora podemos elegir entre $n - 1$ elementos, después $n - 2$ para el tercero, y así sucesivamente hasta el último, que queda automáticamente determinado. Cada una de estas elecciones no impone ninguna restricción adicional en la que sigue, y por consiguiente (¿por qué?), el número total de posibles ordenamientos es

$$n \cdot (n-1) \cdot (n-2) \cdot ... \cdot 2 \cdot 1 = n!.$$

Aquí el símbolo $n!$ se lee "n factorial" o "factorial de n"; y así por ejemplo, tenemos los primeros factoriales: $1! = 1$, $2! = 2 \times 1 = 2$, $3! = 3 \times 2 \times 1 = 6$, $4! = 4 \times 3 \times 2 \times 1 = 24$, $5! = 5 \times 4 \times 3 \times 2 \times 1 = 120$, etc. (Por lo anterior, $n!$ es también el número de funciones biyectivas de un conjunto A de cardinalidad n en sí mismo, ¿por qué?)

Una primera observación que se puede hacer es que el factorial de un número define una función, entre números naturales. Pero además, es una función que crece **muy** rápidamente al aumentar n; de hecho, no sólo crece más rápidamente que cualquier potencia de n, sino que también crece más

rápido que cualquier exponencial de n, como 2^n. (Aunque nosotros no haremos mayor uso de esta propiedad, pienso que es conveniente recalcarla a los estudiantes; por ejemplo, $6! = 720$, $8! = 40320$, pero $20!$ es un número con 18 cifras.)

Otra observación es que haremos es que $n! = n \cdot (n-1)!$, que es evidente de la definición. Esta igualdad es por supuesto válida si $n > 1$, pero conviene extenderla al caso $n = 1$, **definiendo** $0! = 1$; esta convención nos resultará también útil para evitar tener que dividir algunas afirmaciones en dos casos.

Ejemplos:

i) ¿Cuántas 'palabras' de 10 letras (es decir, listas de letras, aunque no tengan sentido idiomático) se pueden formar con 10 letras?

Solución: Hay $10!$ palabras.

(¡Usualmente, por supuesto, la solución no es tan directa como en este ejemplo!)

ii) ¿Cuántos números de 10 cifras, con todas los dígitos distintos hay?

Solución: La respuesta **no** es $10!$, como podría pensarse de primera impresión, ya que el 0 no puede ocupar la primera posición, debemos por tanto descartar estas permutaciones. Sin embargo, si consideramos todas las posibles permutaciones que tienen al 0 como primer dígito, éstas son exactamente $9!$ ya que podemos permutar los restantes 9 elementos arbitrariamente. De este modo, la solución es $10! - 9! = 9 \times 9!$.

Una útil generalización de la idea de permutación ocurre cuando permutamos k elementos de un conjunto de n objetos distintos (sin restricciones adicionales). Igual que antes, para el primer objeto que permutamos tenemos n opciones, para el segundo $n-1$, para el tercero $n-2$, y así hasta llegar al k-ésimo, para el que tendremos $n-k+1$ (¡atención, **no** $n-k$!). Aunque en este caso no hay una notación universalmente aceptada, al número de permutaciones resultante se le denota a veces por $P(n,k)$, que es la notación que adoptaremos aquí, y como hemos visto está dado por

$$P(n,k) = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) = \frac{n!}{(n-k)!};$$

la última igualdad es clara de la definición del factorial. Notemos que es claro que $P(n,n) = n!$.

Ejemplo: ¿Cuántos números de 3 cifras con dígitos distintos hay?

Solución: Igual que antes, debemos excluir de nuestra respuesta aquellos que empiecen con 0. Por la fórmula anterior, las permutaciones de tres

dígitos distintos son $P(10,3)$, en tanto que aquellos que empiezan con 0 son las permutaciones de pares de números de los restantes 9 números distintos de 0, por lo la respuesta es

$$P(10,3) - P(9,2) = 720 - 72 = 648$$

La noción de permutaciones de k elementos de un conjunto de n elementos se puede también interpretar diciendo que $P(n,k)$ es el número de funciones inyectivas de un conjunto de k elementos en uno de n elementos (por supuesto, esto exige que $k < n$).

Ejercicios.

i) De los 648 números del problema anterior, ¿cuántos son impares?

ii) ¿Cuántas placas de vehículos sin letras ni números repetidos hay?

iii) Probar la siguiente identidad:

$$P(n,1) + P(m,1) = P(n+m,1).$$

3.4 Repeticiones

Otra útil generalización de la noción anterior ocurre cuando permitimos que algunos de los elementos del conjunto sean idénticos (o al menos indistinguibles en algún sentido); en tal caso, al considerar una permutación de esos elementos, ésta resultará indistinguible de la anterior. Por ejemplo, si consideremos el conjunto $A = \{a, a, b\}$ (dos elementos iguales), entonces, de acuerdo a la definición, las permutaciones de A son $3! = 6$ en total, que podemos escribir como:

$$aab; aab; aba; aba; baa; baa;$$

aquí las primeras dos permutaciones sólo intercambian las a, en la tercera y cuarta lo mismo, y en la quinta y sexta lo mismo; es claro que con éstas obtenemos idénticas listas, de modo que el número de permutaciones **distintas** es sólo $6/2 = 3 = 3!/2!$. En general, si tenemos n elementos con k repetidos, el número de permutaciones distintas, también llamadas *permutaciones con repetición*, será $n!/k!$.

Esta construcción se generaliza sin dificultad al caso en que haya más subconjuntos de elementos indistinguibles como sigue: Si en un conjunto de n elementos tenemos r subconjuntos con $k_1, k_2, k_3, ..., k_r$, elementos repetidos

respectivamente, de modo que las permutaciones de estos elementos no sean distinguibles, entonces el número de permutaciones con repetición es

$$\frac{n!}{k_1!k_2!\cdots k_r!}.$$

Por supuesto, para que esta fórmula tenga sentido debe de cumplirse la restricción

$$k_1 + k_2 + \cdots + k_r \leq n$$

Aunque no es muy importante para nosotros, podemos señalar que desde el punto de vista de la teoría de conjuntos, agregando unos si es necesario, de modo que se cumpla que $k_1+k_2+\cdots+k_r = n$, este tipo de permutaciones con repetición también pueden interpretarse como el número de funciones entre ciertos conjuntos, en este caso entre un conjunto de n elementos pero *dividido en r clases de equivalencia*, cada una de las cuales tiene k_i elementos, en el conjunto de sus *clases de equivalencia*. Lo que sí es importante, es que la división en clases no tiene que ser en clases de objetos idénticos, basta que los consideremos como equivalentes. Pero recordemos ahora que significa relación de equivalencia:

Una relación de equivalencia entre elementos de un conjunto, usualmente denotada por $\sim$, es una relación que tiene las tres propiedades siguientes:

i) La relación es reflexiva; es decir, cada elemento está realcionado consigo mismo: $\forall x; x \sim x$.

ii) La relación es simétrica; es decir, si x está relacionado con y, entonces y está relacionado con x. En símbolos, $x \sim y \Longleftrightarrow y \sim x$.

iii) La relación es transitiva; es decir, si x está relacionado con y y y está relacionado con z, entonces x está relacionado con z.

Por supuesto, la relación de equivalencia más inmediata que se ocurre es la de identidad, donde dos elementos de un conjunto son equivalentes si y sólo si son iguales; pero hay muchas otras relaciones de equivalencia que ocurren de manera natural; por ejemplo, 'tener la misma nacionalidad' determina una relación de equivalencia en el conjunto de las personas (ejercicio: ¿por qué?). En general, una relación de equivalencia se puede identificar con una *partición del conjunto en subconjuntos ajenos dos a dos.* Cada uno de los subconjuntos corresponde a los elementos del conjunto que son equivalentes entre sí.

Ejemplo: se tienen 10 puestos en una delegación internacional, y hay dos ingleses, tres chinos, dos alemanes, un ruso y un polaco para ocuparlas;

¿de cuántas maneras pueden distribuirse las distintas nacionalidades de las personas en esos puestos?

Solución: el número pedido es el número de permutaciones con repetición de los 10 puestos, pero hay treschinos, dos ingleses y dos alemanes que al ser permutados entre ellos dejan la misma distribución de nacionalidades en los puestos. Por consiguiente, el total es

$$\frac{10!}{2!2!3!} = 151200.$$

3.5 Combinaciones (sin repetición) y subconjuntos

Probablemente la noción más importante que aparece en combinatoria es la de las *combinaciones de n elementos, tomados de r en r*; dicho de otro modo, de cuantas maneras se pueden escoger r elementos de un conjunto con n elementos. Cada una de estas combinaciones divide al conjunto de n elementos en dos clases: la del conjunto con r elementos que estamos seleccionando, y su complemento, que evidentemente tiene $n - r$ elementos; por lo visto en la sección anterior, el número total de combinaciones posibles es

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

En la ecuación anterior se introdujo la notación más habitual para las combinaciones, aunque existen otras como ${}_nC_r$ ó $C(n,r)$; en cualquier caso esto se lee 'las combinaciones de n en r'.

Una primera observación, evidente de la definición, es que

$$\binom{n}{r} = \binom{n}{n-r},$$

que simplemente expresa que cada subconjunto de r elementos está determinado por su complemento, que tiene $n - r$ elementos.

El número de combinaciones $\binom{n}{r}$ se llama también coeficiente binomial, ya que ocurren como coeficientes de los monomios en el desarrollo de un binomio elevado a la n. En efecto, si consideramos el binomio $(a+b)^n$, el número total de veces que el monomio $a^r b^{(n-r)}$ aparece en el desarrollo de éste, es exactamente $\binom{n}{r}$. Para probar esto notemos que si efectuamos todos

los posibles productos de r 'a's con $(n-r)$ 'b's, pero no conmutamos los elementos del resultado, sino que dejamos la lista de n factores en el orden en que salen, entonces podemos exactamente dar un acomodo de las 'a's por cada subconjunto de r elementos de las n distintas posiciones que puede ocupar una letra de la lista.

Una sencilla pero útil propiedad de los coeficientes binomiales está dada en la siguiente proposición:

Proposición 3.1 *Los coeficientes binomiales satisfacen la relación*

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}.$$

Dem: ejercicio.

Una consecuencia interesante de esta proposición es la construcción del llamado triángulo de Pascal, que es una representación gráfica de los coeficientes binomiales para los distintos valores de n; para $n \leq 5$ el triángulo de Pascal se ve así:

$$\begin{array}{ccccccc} 1 & & & & & & \\ 1 & 2 & 1 & & & & \\ 1 & 3 & 3 & 1 & & & \\ 1 & 4 & 6 & 4 & 1 & & \\ 1 & 5 & 10 & 10 & 5 & 1 \end{array}$$

y el resultado anterior dice que el elemento i del renglón j se obtiene sumando los elementos $i-1$ e i del renglón $j-1$.

Otra consecuencia importante, que sale directamente de la relación entre subconjuntos y coeficientes binomiales, es que el número de subconjuntos de un conjunto de n elementos es exactamente $(1+1)^n = 2^n$ (¿por qué?).

3.5.1 Productos cartesianos y funciones de A en B

Dados dos conjuntos A y B, el conjunto de todas las *parejas (o pares) ordenadas* (a, b), donde $a \in A$ y $b \in B$, es otro conjunto, llamado el *producto cartesiano* de A y B, denotado $A \times B$:

$$A \times B = \{(a, b) \mid a \in A; b \in B\}.$$

El punto fundamental que hay que retener es que en la escrtiura de un par ordenado es importante, y que la igualdad de dos parejas ordenadas se da si y sólo si las entradas correspondientes son iguales:

$$(a,b) = (c,d) \Longleftrightarrow a = c \text{ y } b = d$$

Si A y B son conjuntos finitos, que es el caso que nos interesa aquí, entonces $A \times B$ también lo es; más aún, si $\sharp A = n; \sharp B = m$, entonces $\sharp(A \times B) = nm$. Para ver esto, basta con observar que para los elementos de un par ordenado se tienen n elecciones posibles para el primer elemento, y para cada una de estas, se tienen m elecciones posibles del segundo.

La definición de producto cartesiano se extiende fácilmente para el caso de un número finito de factores (incluso se puede extender a un número infinito, pero eso no nos interesa ahora): Si $A_1, A_2, ..., A_k$, son conjuntos, entonces el producto cartesiano de ellos es

$$A_1 \times A_2 \times \cdots \times A_k = \{(a_1, a_2, ...a_k) \mid a_i \in A_i;\ i = 1, 2, ..., k\}.$$

Y por el mismo tipo de argumentos, si $\sharp A_i = n_i$, entonces $\sharp(A_1 \times \cdots \times A_k) = n_1 \cdots n_k$.

En particular, los conjuntos que aparecen en un producto cartesiano pueden ser todos iguales, en tal caso, si tenemos n copias del conjunto A, denotamos su producto cartesiano por A^n.

Una importante interpretación del producto cartesiano A^n de un conjunto consigo mismo se obtiene como sigue: cada elemento del producto es, por definición, una lista ordenada $(a_1, a_2, ...a_n)$ de elementos de A; esto determina una función del conjunto $\{1, 2, ..., n\}$ en el conjunto A, dada por $i \longmapsto a_i$. Recíprocamente, cada función de este tipo determina, de manera obvia, un elemento de A^n; vemos así que el producto cartesiano es equivalente al conjunto de funciones de $\{1, 2, ..., n\}$ en A.

Más en general, si tenemos dos conjuntos, denotamos por A^B al conjunto de todas las funciones de B en A (obsérvese el orden). Por lo dicho anteriormente, es claro que si A y B son conjuntos finitos, de cardinalidades m y n respectivamente, entonces la cardinalidad del conjunto A^B es mn.

Ejemplo: Si A es un conjunto arbitrario (finito o no), y $B \subset A$, entonces B está completamente determinado por su función característica, usualmente denotada por χ_B, definida por

$$\chi_B(x) = \begin{cases} 1 \text{ si } x \in B \\ 0 \text{ si } x \notin B \end{cases}$$

(por ejemplo, la función cracterística del vacío es la función idénticamente cero, en tanto que la función característica del conjunto total A es la función idénticamente 1).

De esta manera, vemos que el conjunto de todos los subconjuntos de A es equivalente al conjunto de todas las funciones de A en $\{0, 1\}$. Esto comprueba de una manera distinta nuestro cálculo de que el número de subconjuntos, para el caso de conjuntos finitos, es 2^n, y por ello a veces al conjunto de subconjuntos se le denota por 2^A y se le llama el *conjunto potencia* de A.

3.6 Algo de herramienta

Vamos a considerar ahora dos importantes herramientas de trabajo:

i) Principio de las casillas

La primera herramienta es un resultado muy sencillo, pero de gran utilidad: el llamado *principio de las casillas* (*pigeon-hole principle*, en inglés), que dice que si se tienen n elementos u objetos que se van a distribuir en k casillas, y $n > k$, entonces en alguna de las casillas hay al menos dos elementos. Para demostrar esto, simplemente basta con observar que si no fuera así, entonces el número de elementos acomodados sería $\leq k < n$. Evidentemente, este principio se puede generalizar como sigue: si tenemos n objetos y k casillas, y $n > rk$ para algún entero r, entonces alguna casilla tiene al menos $r + 1$ objetos.

Ejemplo: si se sabe que el número máximo de cabellos en la cabeza de un ser humano no excede 300,000, entonces, ya que 300,000 es menor que el número de habitantes en la Ciudad de México, se puede afirmar que en esa área hay al menos dos personas que tienen exactamente el mismo número de cabellos.

Problema: si se supone que hay 15,000,000 de habitantes en el área de la Ciudad de México, ¿cuál es el máximo número de gentes en esa zona que se puede afirmar tienen el mismo número de cabellos?

ii) Inducción matemática

Nuestra segunda herramienta es la técnica **no elemental** más poderosa cuando se trabaja con números naturales: el *principio de inducción matemática*. Podemos enunciarlo como sigue:

Principio de inducción matemática:

Sea P una propiedad de los números naturales, tal que:

i) Un primer número la posee.

ii) Si un número la posee, entonces el siguiente número también la posee.

Entonces, **todos** los números naturales, a partir del primero considerado en *i)*, la poseen.

En símbolos, si $P(n)$ es una propiedad de los números naturales tal que $P(i_0)$ es válida y, si $P(k)$ es válida para $k > i_0$ entonces $P(k+1)$ también lo es, entonces $P(n)$ es válida para todos los números naturales $> i_0$.

La afirmación para i_0 se llama el *pie de inducción*, y hemos enunciado así el principio de inducción porque es importante que quede claro que el **primer** elemento no tiene que ser 1 ó 0, que es una dificultad que suelen encontrar los principiantes, basta con que haya un primer elemento en el razonamiento inductivo.

Ejemplos:

i) Una fórmula sencilla, pero muy útil, que se puede probar por inducción es la siguiente:

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

La demostración es como sigue:

Si $k = 1$ la fórmula es obviamente cierta, ya que sólo dice que $1 = \frac{1\times 2}{2}$, que es trivialmente cierto.

Si suponemos ahora que la relación es cierta para $n = k$, lo que necesitamos es probar que vale para $n = k + 1$. Pero

$$\sum_{i=1}^{k+1} i = (k+1) + \sum_{i=1}^{k} i = (k+1) + \frac{k(k+1)}{2} = (k+1)\left(1 + \frac{k}{2}\right) = \frac{(k+1)(k+2)}{2}$$

como queríamos demostrar; de acuerdo con el principio de inducción, esto muestra que la afirmación es cierta para toda n.

ii) Un sencillo ejemplo que muestra que no siempre el pie de inducción i_0 tiene que ser 1 ó 0 es el siguiente:

Probar que $2^n > n$ si $n > 1$.

Solución: Si $n = 2$ (que es el primer natural para el que $2^n > n$) entonces la afirmación es $4 > 2$, que es evidentemente cierta.

Si ahora suponemos que $2^k > k$, para $k > 1$, entonces $2^{k+1} = 2 \times 2^k > 2k > k + 1$, que es lo que queríamos probar.

Ejercicios:

Probar por inducción las siguientes afirmaciones:
i) $\sum_{1=0}^{n} i^2 = \frac{1}{6}n(n+1)(2n+1)$
ii) $\sum_{i=0}^{n} 2^i = 2^{n+1} - 1$

Aunque las demostraciones por inducción son sin lugar a dudas las más útiles cuando se trabaja con número naturales, no hay que perder de vista que hay otra técnicas de demostración:

Ejemplo: Probar que si $r \neq 1$, entonces

$$\sum_{i=0}^{n} r^n = \frac{1 - r^{(n+1)}}{1 - r}$$

(sugerencia: considere el producto $(1 - r)\left(\sum_{i=0}^{n} r^n\right)$).

Ejercicio: Intente demostrar lo anterior por inducción (¡no es demasiado difícil!).

3.7 Teoría de gráficas

Algunas de las aplicaciones más atractivas de la combinatoria ocurren en la teoría de gráficas. Debemos señalar enseguida que, aunque hasta mediados de este siglo se le consideraba como un especie de diversión, en la actualidad la teoría de gráficas es una rama muy vasta de las matemáticas y por ello sólo mencionaremos aquí algunos de sus aspectos más básicos.

Por definición, una gráfica G es un conjunto de puntos, llamados *vértices* de la gráfica, junto con un conjunto de parejas de vértices, llamados *aristas* de la gráfica. Por supuesto, una gráfica puede pensarse intuitivamente como un conjunto de puntos -los vértices-, pintados en un papel junto con una serie de líneas -las aristas- que los unen; pero la definición anterior **enfatiza** el hecho que no es importante si la podemos dibujar o no. Si a es un vértice de una gráfica, su *valencia* es el número de aristas que lo contienen (o que *inciden* en él).

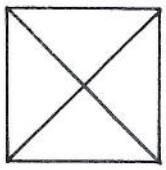
Para dar una idea de la utilidad de la teoría de gráficas, consideremos el siguiente problema, el llamado *problema del cartero*, que en cierto modo es el mismo que el famoso problema de los puentes de Königsberg, que fue el que sugirió al gran matemático suizo L. Euler, alrededor de 1770, la idea de utilizar gráficas para estudiar problemas:

Se tiene una serie de sitios en una ciudad que se deben recorrer **todos**, y la idea es escoger una ruta que nos lleve a todos ellos, **sin andar dos veces por un mismo camino**.

En retrospectiva es bastante claro que el problema se pude traducir a un problema de gráficas, remplazando los sitios por vértices de una gráfica, y los caminos entre dos sitios contiguos por aristas; una ruta o camino es entonces una sucesión de aristas contiguas y, cuando una ruta como la descrita en el problema existe, se le llama una *camino euleriano.*

Para tener una idea el método de solución del problema (sin entrar en detalles), notemos que una condición necesaria para que el problema tenga solución es que, si en un vértice dado tenemos una ruta de llegada, entonces debemos de tener una de salida; en el lenguaje de gráficas, esto dice que la valencia del vértice debe ser *par.*

Una simpática aplicación de este resultado es para responder al acertijo clásico de si es posible trazar el "cuadrado del diablo", ilustrado en la siguiente figura, sin despegar el lápiz del papel:



Ejercicio: Dar los detalles de que no es posible dibujar el "cuadrado del diablo" sin despegar el lápiz del papel. En general, el mismo problema para cualquier polígono de un número par de lados, en el que unimos **todos** los vértices entre sí (lo que se llama la *gráfica completa*), también es imposible. Sin embargo, si el número es impar entonces sí existe un camino euleriano.

Ejercicios:

i) Probar, usando argumentos combinatorios, que en cualquier gráfica el número de vértices es igual a a la mitad de la sumas de las valencias de los vértices.

ii) Si se tiene un grupo de diez gentes, ¿será cierto que puede existir un grupo de siete gentes donde cada una conoce exactamente a tres de las gentes? (Sugerencia: considerar una gráfica que represente, con los vértices a las personas, y con las aristas el hecho de que dos personas se conozcan, y usar el ejercicio anterior.)

3.8 Probabilidad finita

Otro tema donde las aplicaciones de la combinatoria son de enorme utilidad es la *probabilidad finita.* Aquí debemos aclarar también que la teoría de

probabilidad es otra rama muy desarrollada de las matemáticas, y en estas notas sólo tocaremos un aspecto muy particular de ella.

Consideremos entonces un conjunto A, con n elementos, y un subconjunto B de A; nos preguntamos entonces que tan probable es que al escoger *completamente al azar* un elemento de A obtengamos uno de B. Por definición (definición basada en la experiencia, aunque justificar este punto no es importante para nosotros ahora) diremos que esta probabilidad es

$$p = \frac{\sharp B}{\sharp A} = \frac{\sharp B}{n}.$$

Notemos que automáticamente $0 \leq p \leq 1$.

Sin duda, una de las aplicaciones más comunes de esta noción, que se originó en el siglo XVII con trabajos de B. Pascal entre otros, ocurre en los juegos de azar. Por ejemplo, consideremos cual es la probabilidad de ganar una apuesta al arrojar una moneda al aire ("echar un volado"): Si suponemos que sólo hay dos resultados posibles de la acción de arrojar la moneda ('águila o sol', ó 'cara o cruz'), entonces, de dos posibles situaciones hay una que es "favorable" para nosotros (la elección que hayamos hecho) y otra que no lo es. De acuerdo a nuestra definición tenemos entonces que la probabilidad de ganar el volado es $1/2$. Aquí por supuesto la experiencia muestra que esto no es una verdad absoluta; sin embargo, si se efectúa un gran número de volados se verá que, efectivamente, aproximadamente la mitad de las veces sale 'águila', y la mitad de las veces 'sol'. Esta es la explicación "experimental" de nuestra definición de probabilidad que mencionábamos hace un instante. Es también por este tipo de razones que al hablar de probabilidades suele decirse que la probabilidad es "el número de casos favorables entre el número de casos posibles", entendiéndose por favorable simplemente que cae en el conjunto B de la definición dada arriba.

Ejemplo: la probabilidad de obtener dos águilas en dos volados es un cuarto; en efecto, hay cuatro casos posibles: 'águila-águila'; 'águila-sol'; 'sol-águila'; 'sol-sol'; y sólo uno de ellos es favorable.

Observación: Aunque profundizar en ello está fuera del alcance de estas notas, el ejemplo anterior ilustra indirectamente una de las propiedades básicas de la probabilidad, que es el hecho de que la probabilidad de tener dos *eventos independientes* es el producto de las probabilidades de los eventos. En este caso, la probabilidad de obtener un 'águila' en cada volado es $1/2$, y el resultado de cada uno de los volados es independiente del otro,

de este modo, la probabilidad de que salgan dos 'águilas' es $\frac{1}{2} \times \frac{1}{2} = \frac{1}{4}$, en concordancia con nuestro cálculo previo.

Ejemplo: Una ilustración muy clásica del uso de la probabilidad y de las técnicas combinatorias es en la determinación de los valores relativos de las distintas manos de la baraja en el poker.

Recordemos que la baraja (inglesa) consiste de 52 cartas, divididas en cuatro tipos o "palos" (corazones, diamantes, tréboles y picas), y numeradas del 1 (o "as") al 10 y luego la J (el "jack" o "príncipe", y que viene siendo el 11) la Q (la "reina", el 12) y la K (el "rey", el 13). Cada mano consiste en 5 cartas de la baraja.

El tipo de preguntas que nos hacemos ahora es, ¿qué es más fácil de obtener en una mano sacada al azar: una tercia (es decir tres cartas del mismo número y las otras dos de distintos números), o dos pares (es decir dos pares de cartas del mismo número, pero no las cuatro del mismo, y la otra de un tercer número)?

Para calcular el número de manos con tercia podemos argumentar como sigue: En primer lugar, si fijamos el número del que tendremos la tercia (por ejemplo, tercias de ases), entonces podemos tener 4 tercias distintas, que son las combinaciones de 4 en 3, $\binom{4}{3}$. Una vez fija la tercia, para la cuarta carta de la mano podemos escoger entre cualquiera de las 48 cartas que no tienen el número de la tercia. Finalmente la quinta carta debe de escogerse de entre las 44 cartas que no tienen ni el número de la tercia ni el número de la otra carta ya escogidas; Pero como no nos interesa distinguir entre que llamamos la cuarta y la quinta cartas, el resultado debemos todavía dividirlo entre 2: el total de posibilidades para esto es entonces $\frac{4\times48\times44}{2}$. Si hacemos esto con los trece números posibles, vemos que el total de tercias es $13 \times 2 \times 48 \times 44 = 54912$

Calculemos ahora el número de manos con dos pares: el primer par se puede escoger de cualquier número, lo que da 13 opciones; pero si fijamos este número, entonces podemos construir $\binom{4}{2} = 6$ distintos pares, en total 13×6. Para el segundo par tenemos ahora 12 números disponibles, y para cada uno de estos números hay de nuevo 6 pares distintos. Pero una vez más, no debemos distinguir entre que par llamamos el primero y que par el segundo, por lo que el total de posibles pares de parejas es $13 \times 12 \times 6 \times 3$. Finalmente, la quinta carta podemos escogerla de cualquiera de las 44 cartas restantes que no son de ninguno de los dos números ya usados en los pares; de este modo, el número de manos con dos pares es $13\times12\times6\times3\times44 = 123552$.

Podemos describir esto en términos de probabilidades como sigue:

El número total de manos posibles es $\binom{52}{5} = 2598960$. Como el número de casos favorables para el evento "tener una tercia" es 54912, la probabilidad de tener una tercia es aproximadamente .0211. Similarmente, la probabilidad de tener dos pares es .0475. Esto muestra que es un poco más de dos veces más probable obtener dos pares que una tercia.

Ejercicios:

1. Calcular las probabilidades de obtener *a)* un 7 y *b)* un 11, cuando se arrojan dos dados.

2. Si se arrojan 7 dados, cual es la probabilidad de obtener exactamente tres seises.

3. Si se escoge un número de cinco dígitos al azar, ¿cuál es la probabilidad de que

a) la suma de los dígitos sea 20

b) el producto de los dígitos sea 20.

4. Un mecánico limpió las bujías de un motor de 8 cilindros; él hubiera querido dejarlas exactamente en sus mismas posiciones, pero se le cayeron, se revolvieron y ya no las pudo distinguir. ¿Cuál es la probabilidad de que las haya colocado en su orden original? ¿Cuál es la probabilidad de que al menos 2 bujías hayan quedado en su posición original?

3.8.1 Problemas varios

1. Sin expander el producto

$$(a+b+c)(d+e+f)(p+q+r+s)(x+y+u+v+w)$$

¿cuántos términos tiene el resultado?

2. En un examen de opción múltiple, en que cada pregunta tiene cuatro respuestas numeradas de 1 a 4, ¿cuántas formas hay de acomodar las soluciones, de modo que dos problemas consecutivos no tengan el mismo número de respuesta?

3. ¿Cuántas colecciones distintas de 5 monedas mexicanas se pueden hacer, con todas las monedas distintas en cada colección? (Las monedas van de 5 centavos a 50 pesos.)

4. Demuestra por inducción que

$$\sum_{r=1}^{n-1} r(n-r) = \binom{n+1}{3}$$

5. En una ciudad con cuadras totalmente cuadradas, las calles que van de norte a sur están numeradas 1,3,5, etc., en tanto que las que van de este a oeste están numeradas 2,4,6, etc. Alguien que vive en la esquina de 1 y 2 quiere ir a su trabajo en la esquina de 10 y 15. ¿De cuántas maneras puede hacerlo (sin regresar en ningún momento)?

6. Ocho personas se acomodan en una mesa redonda con ocho sillas. De cuantas maneras se pueden acomodar si se desea que cada persona quede siempre entre las mismas personas, aunque la que en un acomodo está a su dercha en otro puede estar a su izquierda, etc.

Bibliografía

[1] 'Primeros pasos en las olimpiadas de matemáticas' Revista del seminario de enseñanza y titulación. Vol. IX, Num. 76 (1993).

Esta referencia es quizá la más básica, parte por estar en español, parte porque va muy al grano y parte porque está escrita por alguien con mucha experiencia en la preparación de "olímpicos matemáticos" mexicanos.

[2] Mathematics of Choice. New Mathematical Library, Vol 15. Editado por la American Mathematical Society (1965).

Esta es probablemente mi referencia favorita para este tema. Es un libro muy bonito y muy bien escrito, con muchos ejemplos y ejercicios de varios de los temas que tratamos en estas notas (y otros más). Quizá su defecto es que está escrito un poco "a la antigüita"

[3] Editado por A.W. Planck y N.H. Williams para el Australian Mathematical Committee y publicado por el Australian International Centre for Mathematics Enrichment, de la Universidad de Canberra (199?)

El Tool Chest, como su nombre lo indica, es literalmente un compendio de resultados, para ser usados como herramienta en la solución de problemas del tipo que aparecen en las olimpiadas de matemáticas. Es un muy buen libro como complemento.