**DEMOSTRACIONES**

**Introducción**

En Matemáticas, una de las actividades más importantes consiste en demostrar proposiciones, es decir, a partir de unas afirmaciones iniciales que tomamos como hipótesis, deducir mediante métodos de razonamiento aceptados, otras afirmaciones más complejas.

En la clase de hoy, empezaremos entonces a estudiar los métodos de demostración que se utilizan habitualmente en Matemáticas.

Las proposiciones matemáticas son normalmente enunciados condicionales de la forma P ⇒ Q, donde P normalmente es una conjunción de enunciados a los que llamamos **hipótesis** o **premisas** y Q es la **tesis** o **conclusión** de la proposición.

Hay también proposiciones matemáticas que no tienen hipótesis, por ejemplo, la proposición “√2 no es un número racional”. En este caso, hay que demostrar la proposición utilizando propiedades básicas ya sabidas de los números racionales.

**Ejemplos**

1. “Si f y g son funciones reales continuas, entonces f + g es una función real continua.”

Hipótesis: f es una función real continua y g es una función real continua.

Conclusión: f + g es una función real continua.

1. “La suma de dos números enteros impares es un número entero par”

Hipótesis: m es un número entero impar y n es un número entero impar.

Conclusión: m + n es un número entero par.

1. “Si T es un triángulo rectángulo cuyos lados tienen longitudes a, b y c donde c es la longitud de la hipotenusa, entonces a2 + b2 = c2”

Hipótesis: T es un triángulo rectángulo, a, b son las longitudes de los catetos y c es la longitud de la hipotenusa.

Conclusión: a2 + b2 = c2.

**Observación**

A partir de ahora, nos centraremos en proposiciones matemáticas que sabemos que son verdaderas, es decir, en proposiciones para las cuales hay una demostración.

Cuando hagamos una demostración de una proposición matemática, utilizaremos el símbolo ❏ para indicar el final de la demostración.

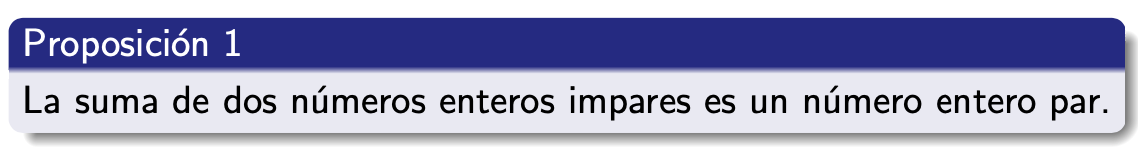
**Demostraciones directas**

Queremos demostrar un enunciado condicional A ⇒ B (hipótesis, tesis; suponemos A para llegar a. B), donde A y B son proposiciones matemáticas. Tenemos que deducir entonces proposiciones intermedias C1, . . ., Cn de manera que

A⇒C1 ⇒C2 ⇒···⇒Cn ⇒B.

Antes de hacer la demostración, tenemos que entender bien el enunciado, entendiendo claramente los conceptos que aparecen en A y en B.Veamos a continuación algunos ejemplos.

**Ejemplos**



Para demostrar esta proposición, tenemos que tener claro qué significa que un número sea **par** y que un número sea **impar**. Consideramos entonces las siguientes definiciones.

Sea n un número entero. Decimos que n es par, si existe un k ∈ Z tal que n = 2k. Y decimos que n es impar, si existe un k ∈ Z tal que n = 2k + 1.

**Demostración de la Proposición 1**

Sean n y m números enteros impares. Como n es impar, tenemos que existe un k ∈ Z tal que n = 2k + 1. Análogamente, como m es impar, existe un l ∈ Z tal que n = 2l+1. Por tanto,

n + m = 2k + 1 + 2l + 1 = 2k + 2l + 2 = 2(k + l + 1).

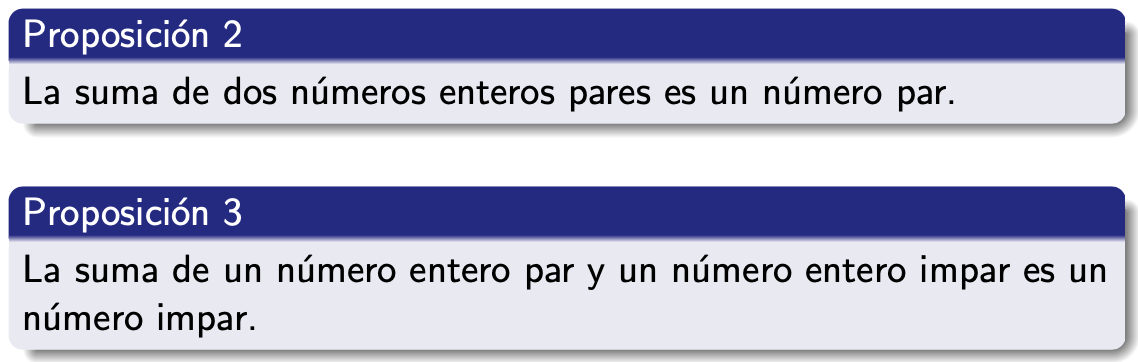
Sea r = k + l +1. Como k y l son números enteros, r es también un número entero. Tenemos entonces que n + m = 2r y r es un número entero. Por tanto, n + m es par. ❏

**Observación**

Obsérvese que en la demostración de la Proposición 1 hemos utilizado “hipótesis implícitas”, como son la propiedad conmutativa de la suma en los enteros, la propiedad distributiva del producto respecto de la suma en los enteros y el hecho de que la suma de enteros es también un entero.

Las “hipótesis implícitas” se utilizan habitualmente en las demostraciones de proposiciones matemáticas y corresponden a propiedades básicas conocidas de los números u objetos matemáticos que estemos considerando.

**Ejemplos**

Las siguientes proposiciones se demuestran de manera análoga a la Proposición 1.

Asimismo, se puede demostrar el siguiente enunciado.

**Demostración de la Proposición 4**

Sea x un número impar. Por tanto, existe un k ∈ Z tal que x = 2k + 1. Tenemos entonces:

(2k+1)3 = 8k3 +12k2 + 6k + 1 = 2(4k3 + 6k + 3k) + 1.

Sea l = 4k3 + 6k + 3k. Como k es un número entero, l es también un número entero.

Entonces, como x3 = 2l + 1, deducimos que x3 es impar. ❏

Obsérvese que en la demostración de la Proposición 4, hemos utilizado la fórmula que conocemos para calcular el cubo de la suma de dos números a y b:

(a + b)3 =a3 + 3a2b + 3ab2 + b3.

**Ejemplos**

Para demostrar la siguiente proposición, necesitamos definir el siguiente concepto.

Un entero a es un **divisor** de un entero b, si b es múltiplo de a, es decir si existe un entero c tal que b = ac.

Si a es un divisor de b, escribiremos a|b.



**Demostración de la Proposición 5**

Como a|b, existe un q1 ∈ Z tal que b = a·q1. Y como b|c, existe un q2 ∈ Z tal que c = b·q2

Por tanto,

c = b · q2 = a · q1 · q2.

Sea q = q1 · q2. Como q1 y q2 son números enteros, q es también un número entero. Por tanto, como c = a · q, deducimos que a|c. ❏

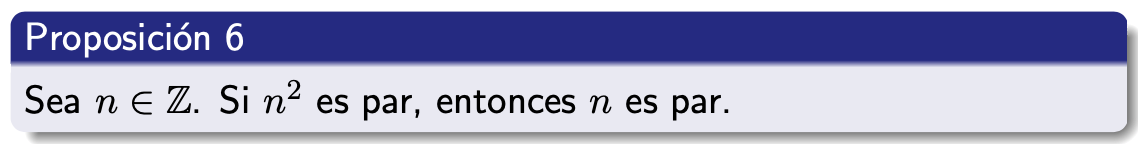
**Demostraciones por contrarrecíproco o contraposición**

Se basa en la equivalencia lógica P ⇒ Q ≡ ¬Q ⇒ ¬P, que es una de las leyes lógicas que vimos en la penúltima clase. Así pues, si P y Q son proposiciones matemáticas, demostrar por contraposición que P ⇒ Q significa demostrar que ¬Q ⇒ ¬P (suponer ¬Q para llegar a ¬P).

En muchas demostraciones matemáticas es más fácil demostrar que ¬Q ⇒ ¬P en lugar de demostrar de manera directa que P ⇒ Q.

A continuación, veremos algunos ejemplos de demostraciones por contraposición.

**Ejemplos**



En este caso, tenemos

P = n2 es par y Q = n es par.

Para demostrar entonces P ⇒ Q por contraposición, tenemos que demostrar que ¬Q ⇒ ¬P. Supongamos entonces que Q es falso. Por tanto, n es impar. Así pues, existe un entero k tal quen = 2k + 1. Tenemos entonces:

n2 = (2k+1)2 = 4k2 + 4k +1 = 2(2k2 +2k) + 1.

Sea l = 2k2 + 2k. Como k es un número entero, l es también un entero. Entonces, como n2 = 2l + 1, deducimos que n2 es impar. Por tanto, P es falso. Así pues, hemos demostrado ¬Q ⇒ ¬P. ❏

****

En este caso, tenemos

P = 7n es par y Q = n es par.

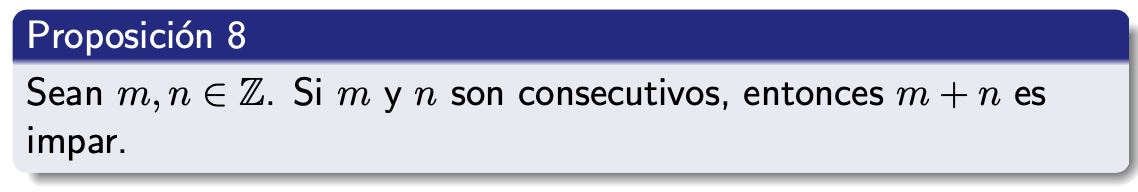
Para demostrar entonces P ⇒ Q por contraposición, tenemos que demostrar que ¬Q ⇒ ¬P. Supongamos entonces que Q es falso. Por tanto, n es impar. Así pues, existe un entero t tal que n = 2t + 1. Tenemos entonces:

7n + 4 = 7(2t + 1) + 4 = 14t + 11 = 14t + 10 + 1 = 2(7t + 5) + 1.

Sea p = 2t + 5. Como t es un número entero, p es también un entero. Entonces, como 7n + 4 = 2p + 1, deducimos que 7n + 4 es impar. Por tanto, P es falso. Así pues, hemos

demostrado ¬Q⇒¬P. ❏

Veamos a continuación otro ejemplo de una demostración por contraposición.



En este caso, tenemos

P = m y n son números enteros consecutivos,

Q = m + n es impar.

Para demostrar entonces P ⇒ Q por contraposición, tenemos que demostrar que ¬Q ⇒ ¬P. Supongamos entonces que Q es falso. Por tanto, m + n es par. Así pues, existe un entero k tal que m + n = 2k. Por tanto, m = 2k − n. Así pues, tenemos:

m − n = (2k − n) − n = 2k − 2n = 2(k − n).

Sea l = k − n. Entonces, como l es un número entero y m − n = 2l, deducimos que m − n es un número par, y por tanto m y n no son consecutivos.

Por consiguiente, P es falso. Así pues, hemos demostrado ¬Q⇒¬P. ❏

Veamos a continuación otro método de demostración.

**Demostraciones por reducción al absurdo**

El método de reducción al absurdo consiste en negar la proposición que se quiere demostrar y llegar entonces a una contradicción. Este método está basado en la ley de reducción al absurdo que vimos en la parte de Lógica y Razonamientos, la cual afirma que para toda proposición P, (¬P → 0) ≡ P. ¬(P⇒Q) =

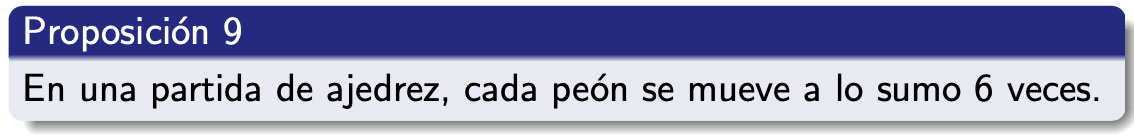
🡪Si el enunciado no es un condicional A. Suponemos que A es falso y llegamos a una contradicción.

🡪Si el enunciado es un condicional P ⇒ Q, tenemos ¬(P⇒Q) ≡ P ∧ ¬Q. Suponemos ¬Q y P, y llegamos a una contradicción

Así pues, si queremos demostrar una proposición P por reducción al absurdo, tendremos que suponer que P es falsa y llegar entonces a una contradicción.

Veamos a continuación algunos ejemplos.

**Ejemplos**



Supongamos, por el contrario, que hemos movido un peón 7 o más veces.

Tras el primer movimiento, el peón se encuentra al menos en la tercera fila del tablero.

Tras el segundo movimiento, el peón se encuentra al menos en la cuarta fila del tablero.

.

.

.

Tras el séptimo movimiento, el peón se encuentra fuera del tablero.

Hemos llegado entonces a una situación absurda. Por tanto, se cumple la proposición. ❏



Supongamos, por el contrario, que √2 es un número racional.

Entonces, podemos expresar √2 como una fracción irreducible, es decir, existen n, m ∈ N tales que m>0, √2 = n / m y el máximo común divisor de n y m es 1. Por tanto, 2 = n2 / m2, y, por consiguiente:

n2 = 2m2.

Así pues, n2 es par. Entonces, por la Proposición 6, n es par. Por tanto, existe un k ∈ N tal que n = 2k. Así pues:

n2 = 4k2 = 2m2.

Por consiguiente, m2 = 2k2. Como k2 ∈ N, tenemos que m2 es par. Aplicando entonces de nuevo la Proposición 6, deducimos que m es par.

Así pues, hemos demostrado que m y n son pares. Por tanto, 2 es un divisor de m y n, lo cual contradice que la fracción n / m es irreducible. Hemos llegado entonces a una contradicción. Por tanto, √2 es un número irracional. ❏

**Introducción (clase 5)**

En la última clase, vimos cómo se pueden hacer demostraciones directas, cómo se pueden hacer demostraciones por contraposición (o por contrarrecíproco) y cómo se pueden hacer demostraciones por reducción al absurdo.

En la clase de hoy, estudiaremos dos nuevos métodos de demostración, que son los llamados “método de demostración por distinción de casos” y “método de demostración por contraejemplo”.

Además, veremos cómo se puede demostrar que varias proposiciones matemáticas son equivalentes.

**Demostraciones por casos**

Para demostrar una proposición P por distinción de casos, se consideran proposiciones A1, . . ., An de manera que A1 ∨ . . . ∨ An es una tautología, y entonces se demuestran:

1. A1 ⇒P.

.

.

.

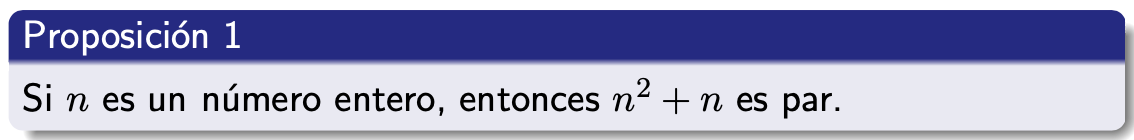
n. An ⇒P.

Este método está basado en la ley de distinción de casos, que vimos en la segunda clase del curso, que afirma que si A1, . . ., An, P son proposiciones de manera que A1 ∨ . . . ∨ An es una tautología, entonces ((A1 ⇒P) ∧...∧ (An ⇒P)) ⇒P es una tautología.

Intuitivamente, los A*i* son los casos que consideramos para la demostración de P. La idea entonces es dividir la demostración de P en una serie de casos. Y el que A1 ∨...∨ An sea una tautología significa que los casos A1, . . ., An son exhaustivos.

**Ejemplos**

Veamos a continuación algunos ejemplos.



Para demostrar la Proposición 1, supongamos que n es un entero genérico. Distinguimos entonces los siguientes casos:

**Caso 1**. n es par.

Como n es par, existe un k ∈ Z tal que n = 2k. Tenemos entonces:

n2 + n = (2k)2 + 2k = 4k2 + 2k = 2(2k2 + k).

Como 2k2 + k ∈ Z, deducimos que n2 + n es par.

**Caso 2**. n es impar.

Como n es impar, existe un k ∈ Z tal que n = 2k+1. Tenemos entonces:

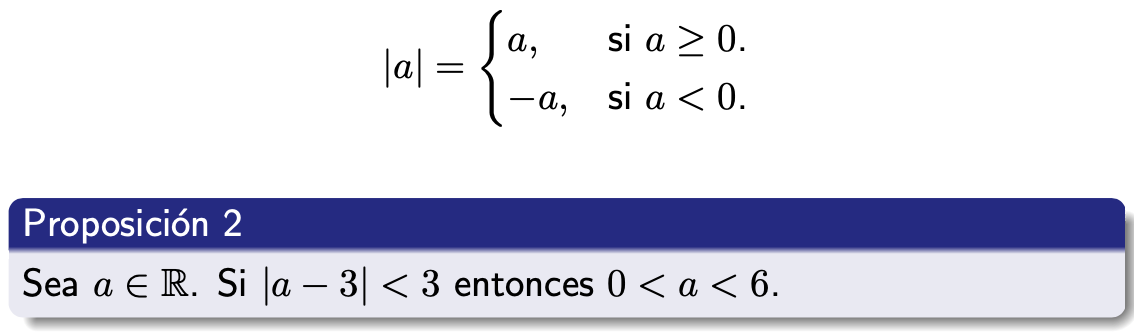
n2 +n = (2k+1)2 + 2k + 1 = 4k2 + 4k + 1 + 2k + 1 = 4k2 + 6k + 2 = 2(2k2 + 3k+1).

Como 2k2 + 3k + 1 ∈ Z, deducimos que n2 + n es par.

Entonces, como para todo número entero n, siempre se cumple que “n es par” ∨ “n es impar”, y en los dos casos hemos demostrado que n2 + n es par, hemos demostrado por distinción de casos que n2 + n es par. ❏

**Ejemplo**

Recordemos que si a ∈ R, el **valor absoluto** de a se define como:



Sea a ∈ R tal que |a − 3| < 3. Distinguimos los siguientes casos:

**Caso1**. a−3 ≥ 0.

Entonces, |a−3| = a−3 < 3, y por tanto a < 6. Por otra parte, como tenemos que a − 3 ≥ 0, deducimos que a ≥ 3. Por tanto, tenemos que 0 < a < 6.

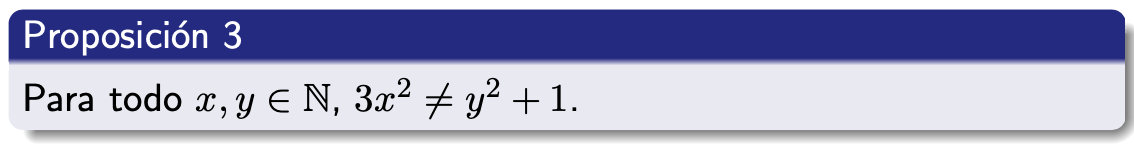
**Caso2**. a−3 < 0.

Entonces, |a−3| = 3−a < 3. Por tanto, a > 0. Por otra parte, como tenemos que a − 3 < 0, inferimos que a < 3, y por tanto a < 6. Así pues, tenemos que 0 < a < 6.

Como para todo a ∈ R, siempre se cumple que a − 3 ≥ 0 o a − 3 < 0, y en los dos casos hemos demostrado que 0 < a < 6 bajo la hipótesis de que |a − 3| < 3, hemos demostrado por distinción de casos la proposición. ❏

**Ejemplo**

En la demostración de la siguiente proposición, combinamos el método de reducción al absurdo con el método de distinción de casos.



Para demostrar la Proposición 3, procedemos por reducción al absurdo. Supongamos entonces que existen x, y ∈ N tales que 3x2 = y2 + 1. Como 3x2 = y2 + 1, deducimos que y2 + 1 es un múltiplo de 3. Distinguimos entonces los siguientes casos:

**Caso1**. y = 3k para algún k ∈ N

Entonces,

y2 +1 = (3k)2 +1 = 9k2 + 1 = 3(3k2) + 1.

Por tanto, y2 + 1 no es un múltiplo de 3, y por consiguiente llegamos a una contradicción.

**Caso2**. y = 3k + 1 para algún k ∈ N.

Entonces,

y2 + 1 = (3k + 1)2 + 1 = 9k2 + 6k + 2 = 3(3k2 + 2k) + 2.

Por tanto, y2 + 1 no es un múltiplo de 3, y por consiguiente llegamos a una contradicción.

**Caso3**. y = 3k + 2 para algún k ∈ N.

Entonces,

y2 + 1 = (3k + 2)2 + 1 = 9k2 + 12k + 5 == 9k2 + 12k + 3 + 2 = 3(3k2 + 4k + 1) + 2.

Por tanto, y2 + 1 no es un múltiplo de 3, y por consiguiente llegamos a una contradicción.

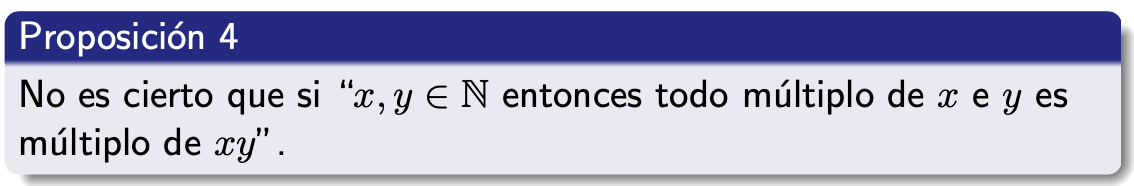
Así pues, como los tres casos que hemos considerado son exhaustivos, y en cada uno de ellos hemos llegado a una contradicción, queda demostrada la proposición. ❏

**El método de demostración por contraejemplo**

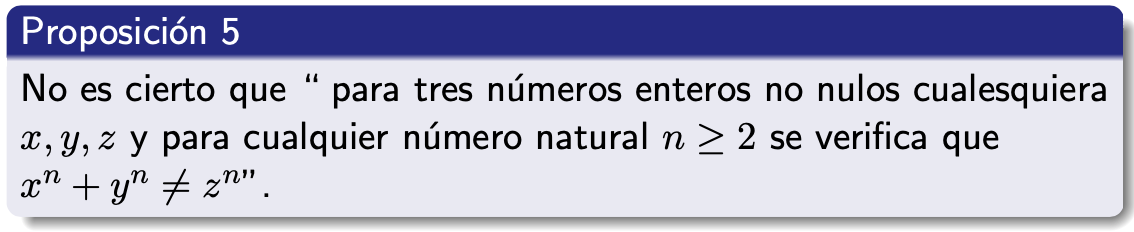
Se utiliza para demostrar la falsedad de una proposición, cuya hipótesis está constituida por una cuantificación universal. Veamos algunos ejemplos.

**Ex**: Proposiciones existenciales; la ecuación x2 + 5 = 0 tiene solución en R. Demostrar que para todo x ∈ R, la ecuación es falsa.

**Ex**: Sea n (n ∈ N). Si n es múltiplo de 5, es múltiplo de 25; n es múltiplo de 5 pero no lo es de 25. Contraejemplo: n = 5 (no satisface el enunciado).



Para demostrar esta proposición, tenemos que dar un contraejemplo. Tomamos x = 2 e y = 6. Se tiene entonces que 6 es un múltiplo de *x* e *y*, pero 6 no es un múltiplo de 12.



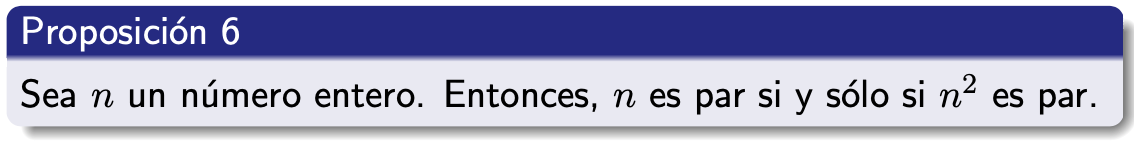
Para demostrar la Proposición 5, tomamos los números x = 3, y = 4, z = 5 y n = 2. Tenemos entonces que

32 + 42 = 52.

**Demostración de proposiciones bicondicionales**

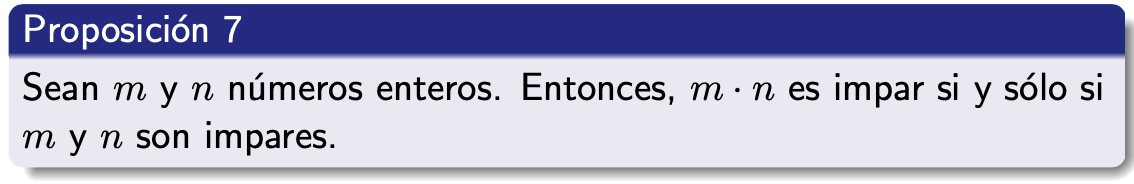
Hay muchas proposiciones matemáticas que tienen la forma P ⇔ Q, es decir, P si y sólo si Q. En estos casos, demostraremos lo dos implicaciones: P ⇒ Q y Q ⇒ P. Este método de demostración esta basado en la ley lógica:

P ⇔ Q ≡ P ⇒ Q ∧ Q ⇒ P.

Veamos a continuación algunos ejemplos:

En la última clase, demostramos por contraposición que si n2 es par entonces n es par. Por tanto, ya tenemos demostrada la implicación de derecha a izquierda de la Proposición 6. Para demostrar la implicación de izquierda a derecha, supongamos que n es un número entero par. Entonces, existe un k ∈ Z tal que n = 2k. Por tanto, n2 = (2k)2 = 4k2 = 2(2k2). Como 2k2 es un entero, deducimos que n2 es par. ❏

Veamos otro ejemplo a continuación.



En primer lugar, demostramos la implicación de izquierda a derecha. Para ello, procedemos por contraposición. Supongamos entonces que no es verdad que m y n son impares. Esto significa que m es par o n es par. Tenemos que demostrar que m \* n es par. Para ello, procedemos por distinción de casos.

🡪Si m es par, existe un entero j tal que m = 2j. Entonces, m\*n = 2jn, y por consiguiente m\*n es par.

🡪Y si n es par, existe un entero i tal que n = 2i. Entonces, m\*n = 2im, y por consiguiente m\*n es par.

De esta forma, queda demostrada la implicación de izquierda a derecha.

Demostramos ahora la implicación de derecha a izquierda. Supongamos que m y n son impares. Existen entonces enteros j y k tales que m = 2j + 1 y n = 2k + 1. Por tanto,

m\*n = (2j + 1) (2k + 1) = 4jk + 2j + 2k + 1 = 2(2jk + j + k) + 1.

Como j y k son enteros, también lo es 2jk + j + k. Por tanto, m\*n es impar. De esta forma, queda demostrada la implicación de derecha a izquierda. ❏

**Demostración de la equivalencia de varias proposiciones**

En ocasiones, queremos demostrar que tres o más proposiciones matemáticas son equivalentes. Entonces, para demostrar que n proposiciones P1, . . ., Pn donde n ≥ 3 son equivalentes se demuestra lo siguiente:

P1 ⇒ P2,

P2 ⇒ P3,

.

.

.

Pn−1 ⇒ Pn,

Pn ⇒ P1.

Es decir, se hace una demostración “circular” de la equivalencia de las n proposiciones.

El caso más frecuente es cuando se quiere demostrar la equivalencia de tres proposiciones P1, P2 y P3. En este caso, demostraremos lo siguiente:

**(1)** P1 ⇒ P2.

**(2)** P2 ⇒ P3.

**(3)** P3 ⇒ P1.

Obsérvese que de (1), (2) y (3), se deduce que las tres proposiciones P1, P2 y P3 son equivalentes. Es decir, de (1), (2) y (3), deducimos:

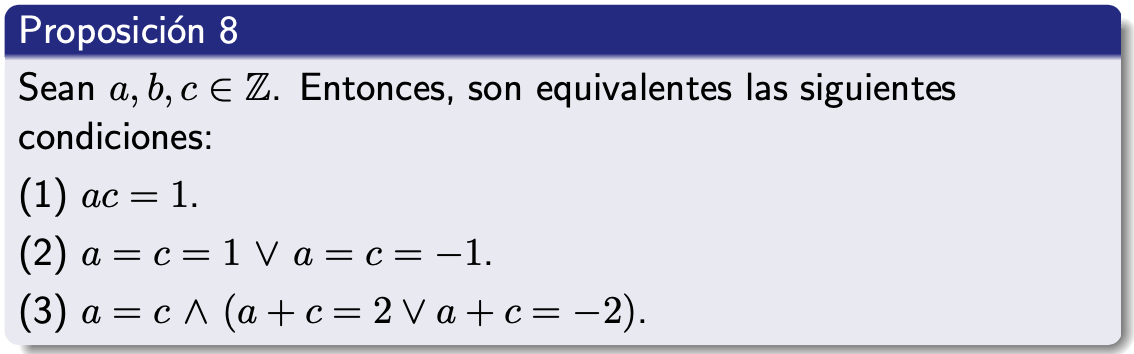
**(4)** P2 ⇒ P1.

**(5)** P3 ⇒ P2.

**(6)** P1 ⇒ P3.

Y esto es así, porque (4) se deduce de (2) y (3); (5) se deduce de (3) y (1); y (6) se deduce de (1) y (2).

Así pues, se deduce de (1)-(6) que P1 ⇔ P2 ⇔ P3.

Veamos a continuación el siguiente ejemplo.

Supongamos que a, b, c ∈ Z. Tenemos que demostrar que (1) ⇒ (2), (2) ⇒ (3) y (3) ⇒ (1).

En primer lugar, demostramos que (1) ⇒ (2). Supongamos que a\*c = 1. Como a y c son números enteros, deducimos que o bien a = c = 1 o bien a = c = −1. Por tanto, se cumple (2).

Demostramos ahora que (2) ⇒ (3). Supongamos entonces que a = c = 1 o a = c = −1. Claramente, a = c. Tenemos que demostrar entonces que a + c = 2 o a + c = −2. Para ello, procedemos por distinción de casos. Tenemos que a = c = 1 o a = c = −1. Entonces, si a = c = 1, tenemos que a + c = 2. Y si a = c = −1, tenemos que a + c = −2. Por tanto, es cierto que (a + c = 2 ∨ a + c = −2), y por consiguiente se cumple (3).

Por último, demostramos que (3) ⇒ (1). Supongamos entonces que a = c ∧ (a + c = 2 ∨ a + c = −2). Demostramos (1) por distinción de casos. Tenemos que a + c = 2 ∨ a + c = −2. Entonces, si a + c = 2, como tenemos que a = c, deducimos que a = c = 1, y por tanto a\*c = 1. Y si a + c = −2, como tenemos que a = c, deducimos que a = c = −1, y por tanto a\*c = 1. As ́ı pues, hemos demostrado (1). ❏

**Introducción (clase 6)**

En la clase de hoy, empezaremos viendo otro ejemplo de una demostración de la equivalencia de tres proposiciones matemáticas.

A continuación, introduciremos los conceptos de teorema, lema, corolario y axioma.

Por último, trataremos las demostraciones de existencia y unicidad, que aparecen frecuentemente en Matemáticas.

Empezamos recordando el método “circular” que vimos al final de la última clase para demostrar que varias proposiciones matemáticas son equivalentes.

**Demostración de la equivalencia de varias proposiciones**

En ocasiones, queremos demostrar que tres o más proposiciones matemáticas son equivalentes. Entonces, para demostrar que n proposiciones P1, . . ., Pn donde n ≥ 3 son equivalentes se demuestra lo siguiente:

P1 ⇒ P2,

P2 ⇒ P3,

.

.

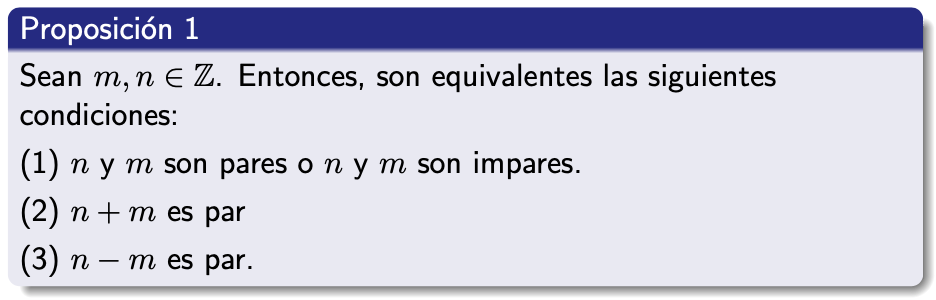
.

Pn−1 ⇒ Pn,

Pn ⇒ P1.

Es decir, se hace una demostración “circular” de la equivalencia de las n proposiciones.

**Ejemplo**



Supongamos que m, n ∈ Z. Tenemos que demostrar que (1) ⇒ (2), (2) ⇒ (3) y (3) ⇒ (1).

En primer lugar, demostramos que (1) ⇒ (2). Supongamos que o bien n y m son pares o bien n y m son impares.

**Caso 1**. n y m son pares.

Entonces, existen k, l ∈ Z tales que n = 2k y m = 2l. Por tanto,

n + m = 2k + 2l = 2(k + l).

Entonces, como k + l ∈ Z, tenemos que n + m es par.

**Caso 2**. n y m son impares.

Entonces, existen k, l ∈ Z tales que n = 2k + 1 y m = 2l + 1. Por tanto,

n + m = 2k + 2l + 2 = 2(k + l + 1).

Entonces, como k + l + 1 ∈ Z, tenemos que n + m es par.

A continuación, demostramos que (2) ⇒ (3). Supongamos que n + m es par. Existe entonces k ∈ Z tal que n + m = 2k. Por tanto,

n − m = n + m − 2m = 2k − 2m = 2(k − m).

Por tanto, n − m es par.

Por último, demostramos que (3) ⇒ (1). Supongamos que n − m es par. Entonces, existe un k ∈ Z tal que n – m = 2k. Distinguimos entonces los siguientes casos:

**Caso 1**. n es par.

Sea l ∈ Z tal que n = 2l. Por tanto:

m = n − (n − m) = 2l − 2k = 2(l − k).

Por consiguiente, m es par. En consecuencia, m y n son pares, y por tanto se cumple (1).

**Caso 2**. n es impar.

Sea l ∈ Z tal que n = 2l + 1. Por tanto:

m = n − (n − m) = 2l + 1 − 2k = 2(l − k) + 1.

Por consiguiente, m es impar. En consecuencia, m y n son impares, y por tanto si cumple (1). ❏

**Teoremas, lemas, corolarios y axiomas**

A las proposiciones verdaderas que son relevantes en Matemáticas se les llama **teoremas**. El término “teorema” se reserva para los resultados matemáticos de mayor interés.

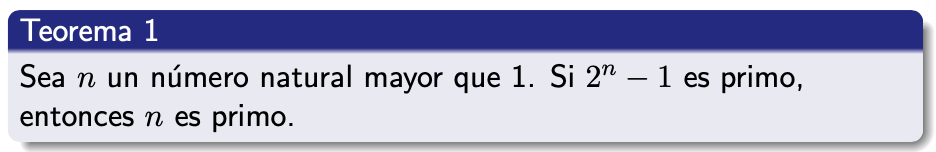
Un **lema** es un resultado auxiliar en el proceso de una demostración de un teorema o de una proposición. Hay ocasiones en las que la demostración de un teorema es muy extensa, en cuyo caso es conveniente dividir dicha demostración en una serie de lemas.

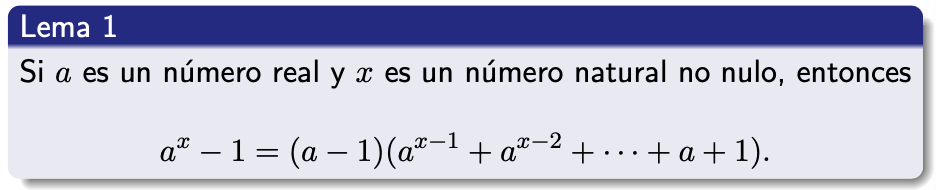
Un **corolario** es una proposición que se deduce con facilidad de un teorema. En muchas ocasiones, los corolarios son casos particulares importantes de los teoremas.

Por último, un **axioma** es una proposición verdadera evidente, que se considera que no necesita demostración. Un ejemplo de un axioma es la proposición “por dos puntos distintos del plano pasa exactamente una recta”.

**Un teorema sobre números primos**

Recordemos que un número natural n es **primo**, si tiene exactamente dos divisores.



Para demostrar este teorema, utilizaremos el siguiente lema:

Tenemos que:

(a − 1) (ax−1 +ax−2 + ··· + a + 1) = a · (ax−1 +ax−2 + ··· + a + 1) − (ax−1 +ax−2 + ··· + a + 1) =

ax + ax−1 + ax−2 ··· + a − ax−1 − ax−2 − ··· − a − 1 = ax − 1. ❏

Demostramos el Teorema 1 por el contrarrecíproco. Es decir, vamos a demostrar que

n no es primo ⇒ 2n – 1 no es primo.

Supongamos entonces que n no es primo. Por tanto, existen números naturales p y q tales que p, q > 1 y p, q < n de manera que n = p · q. Tenemos entonces que

2n – 1 = 2p·q − 1 = (2p)q − 1.

Aplicamos ahora el Lema 1, tomando a = 2p y x = q. Obtenemos entonces:

2n – 1 = (2p)q − 1 = aq −1 = (a − 1) (aq−1 + aq−2 + ··· + a + 1) =

(2p −1) ((2p) q−1 +(2p)q−2 + ··· + 2p + 1).

Ahora, nos fijamos en el factor 2p − 1 de la expresión anterior. Por un lado, como tenemos que n = p · q y q > 1, deducimos que p < n, y por tanto 2p < 2n, y por consiguiente 2p −1 < 2n − 1.

Por otra parte, como p > 1, inferimos que 3 < 2p, y por tanto 1 < 2p − 1.

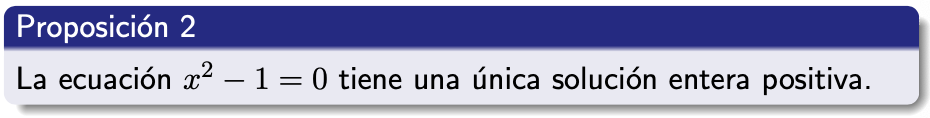
Así pues, hemos demostrado que 1 < 2p − 1 < 2n − 1. Entonces, como 2p −1 es un divisor de 2n −1, deducimos que 2n −1 no es primo. ❏

**Demostraciones de existencia y unicidad**

En muchas ocasiones queremos demostrar proposiciones del tipo “existe un único elemento de un dominio D que satisface una propiedad P(x)”, lo cual formalmente se escribe como ∃!x ∈ D P(x). Obsérvese que esta última expresión la podemos escribir como:

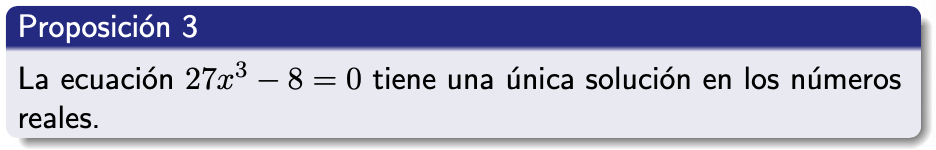
(∃x ∈ D P(x)) ∧ (∀x ∈ D∀y ∈ D(P(x) ∧ P(y) → x = y)).

Para demostrar la existencia, tenemos que encontrar un elemento del dominio que estemos considerando que satisfaga la propiedad. Y para demostrar la unicidad, o bien demostramos de manera directa que si tenemos dos elementos que cumplen la propiedad, entonces esos dos elementos han de ser iguales; o bien procedemos por reducción al absurdo, suponiendo que existen dos elementos distintos que cumplen la propiedad, y entonces llegamos a una contradicción.

**Ejemplos**

**Demostración de la existencia**. Tomemos x = 1. Como 1 ∈ Z, 1 > 0 y 12 − 1 = 0, queda demostrada la existencia

**Demostración de la unicidad**. Sean m, n ∈ Z tales que m, n > 0. Supongamos que m2 – 1 = 0 y n2 – 1 = 0. Entonces, m2 − 1= n2 − 1. Por tanto, m2 = n2. Como m2 = n2, deducimos que m = n o m = −n. El caso m = −n es imposible, ya que m y n son números positivos. Por tanto, m = n. Así pues, hemos demostrado la unicidad. ❏



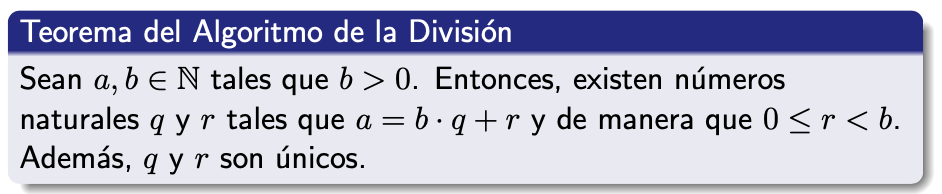
En este caso, podemos demostrar la existencia y unicidad de la siguiente manera. Sea **a** un número real arbitrario. Tenemos entonces:

27a3 – 8 = 0 ⇔ 27a3 = 8 ⇔ a3 = 8 / 27 ⇔ a = 2 / 3.

Por tanto:

27a3 – 8 = 0 ⇔ a = 2 / 3.

Obsérvese que la implicación de derecha a izquierda demuestra la existencia, y la implicación de izquierda a derecha demuestra la unicidad. ❏



**Demostración de la existencia**. Sea b\*q el mayor múltiplo de b que es menor o igual que a. Entonces,

b\*q ≤ a < b (q + 1).

Sea r = a – b\*q. Como b\*q ≤ a, deducimos que r ≥ 0. Por otra parte, tenemos:

r = a – b\*q < b (q + 1) – b\*q = b.

Por tanto, r < b. Y como antes hemos demostrado que r ≥ 0, tenemos que 0 ≤ r < b.

Por otra parte, como tenemos que r = a – b\*q, deducimos que a = b\*q + r. Así pues, queda demostrada la existencia.

Para demostrar la unicidad, procedemos por reducción al absurdo. Supongamos entonces que existen r1, q1, r2, q2 ∈ N tales que se cumplen las siguientes condiciones:

**(1)** a = b\*q1 + r1 = bq2 + r2.

**(2)** 0 ≤ r1 < b y 0 ≤ r2 < b.

**(3)** r1 ≠ r2.

Obsérvese que, como b\*q1 + r1 = b\*q2 + r2, tenemos que r1−r2 = b (q2 − q1). Vamos a demostrar que b ≤ |r1−r2|. Para ello, consideramos los siguientes dos casos:

**Caso 1**. r2 < r1.

Como b (q2 − q1) = r1 − r2, b > 0 y r1 − r2 > 0, deducimos que q2 − q1 > 0. Por tanto, b es un divisor de r1 − r2. Así pues, b ≤ r1 − r2 = |r1 − r2|.

**Caso 2**. r1 < r2.

Obsérvese que como b (q2 − q1) = r1 − r2, b > 0 y r1 − r2 < 0, tenemos que q2 − q1 < 0. Entonces como b (q2 − q1) = r1 − r2, deducimos que b (q1 − q2) = r2 − r1. Por tanto, b es un divisor de r2 − r1. Así pues, b ≤ r2 − r1 =|r1−r2|.

Así pues, hemos demostrado por casos que b ≤ |r1 − r2|.

Sin embargo, como tenemos que 0 ≤ r1 < b y 0 ≤ r2 < b, podemos deducir que |r1 − r2| < b considerando otra vez los dos casos de antes:

**Caso 1**. r2 < r1.

Tenemos que |r1 −r2| = r1 −r2. Entonces, como r1 < b y r2 ≥ 0, deducimos que |r1−r2|= r1 − r2 < b.

**Caso 2**. r1 < r2.

Tenemos que |r1 − r2| = r2 − r1. Entonces, como r2 < b y r1 ≥ 0, deducimos que |r1 − r2|= r2 − r1 <b.

Así pues, hemos demostrado por casos que |r1 − r2| < b.

Entonces, hemos demostrado que b ≤ |r1 − r2| y que |r1 − r2| < b, y por tanto hemos llegado a una contradicción. ❏