Lo anterior refiere a la tabla de certeza de una fbc. Por ejemplo: para la fbc $(p \vee q) \rightarrow r$ (cada valuación es un renglón):

| $p$ | $q$ | $r$ | $(p \vee q)$ | $(p \vee q) \rightarrow r$ |
|---|---|---|---|---|
| $V$ | $V$ | $V$ | $V$ | $V$ |
| $V$ | $V$ | $F$ | $V$ | $F$ |
| $V$ | $F$ | $V$ | $V$ | $V$ |
| $V$ | $F$ | $F$ | $V$ | $F$ |
| $F$ | $V$ | $V$ | $V$ | $V$ |
| $F$ | $V$ | $V$ | $V$ | $V$ |
| $F$ | $V$ | $F$ | $V$ | $F$ |
| $F$ | $F$ | $V$ | $F$ | $V$ |
| $F$ | $F$ | $F$ | $F$ | $V$ |

Además, se dice que una fbc $\mathcal{A}$ es una *tautología* si para toda valuación $v$, $v(\mathcal{A}) = V$, y que una fbc $\mathcal{A}$ es una *contradicción* si para toda valuación $v$, $v(\mathcal{A}) = F$.

**Ejercicio 3** Comprobar si las siguientes fbc son tautologías:

1. $\neg\neg p \rightarrow p$
2. $p \rightarrow \neg\neg p$
3. $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$
4. $(\neg p \rightarrow \neg q) \rightarrow (q \rightarrow p)$
5. $(p \rightarrow q) \rightarrow ((p \rightarrow \neg q) \rightarrow \neg p)$

**Observación 1**

1. Aunque las fbc anteriores usan solamente proposiciones el resultado obtenido puede generalizarse. Esto es, $p \rightarrow \neg\neg p$ no cambiaría su valor de certeza al sustituir por $p$ cualquier otra fbc, digamos $\mathcal{A}$, $\mathcal{A} \rightarrow \neg\neg\mathcal{A}$. Esto es debido a que en la tabla, finalmente $\mathcal{A}$ sólo podrá, como $p$, tomar uno de dos valores, $V$ o $F$, y obtener el resultado final al igual que con $p$. Así las fbc del ejercicio 3 se cumplen en general: $\neg\neg\mathcal{A} \rightarrow \mathcal{A}$, $\mathcal{A} \rightarrow \neg\neg\mathcal{A}$, etc.
2. Algunas fbc pueden ser reescritas en virtud del *teorema de la deducción*. Por ejemplo: $(p \rightarrow q) \rightarrow (\neg q \rightarrow \neg p)$, como $(p \rightarrow q) \vDash (\neg q \rightarrow \neg p)$: a partir de $(p \rightarrow q)$ podemos inferir $\neg q \rightarrow \neg p$. O bien, $(p \rightarrow q), \neg q \vDash \neg p$: si contamos con las premisas $(p \rightarrow q)$ y $\neg q$, podemos inferir $\neg p$.

La última fbc del ejercicio 3 expresa el esquema conocido como *reducción al absurdo*: Si a partir de $p$ obtenemos $q$, pero también $\neg q$, entonces concluimos $\neg p$, esto es si suponemos $p$ y llegamos a que $q$ y no $q$ entonces $p$ es falso. Esta es justamente la primera técnica de demostración que vamos a presentar.

### 1.1.1. Contradicción

Para ilustrar esta técnica de demostración haremos antes algunas definiciones. Un número $q$ se llama *racional* si hay un múltiplo entero de él que es entero: $\exists a \in \mathbb{Z}, a \neq 0$: $aq = b \in \mathbb{Z}$, es decir $q = b/a$ es una fracción. En caso contrario se dice que $q$ es irracional. Claramente tenemos muchos enteros que cumplen con la definición de racional: si $b = qa$ entonces $mb = qma$, $ma, mb \in \mathbb{Z}$. Convenimos en tomar el múltiplo menor de $q$ que satisfaga la condición antedicha. También se dice que los enteros que definen el racional no tienen factores comunes diferentes a 1 o -1. El siguiente es un ejemplo enunciado por Euclides (hacia 330 a.n.e.).

**Teorema 1** $\sqrt{2}$ es irracional.

**Demostración.** Supongamos que $\sqrt{2}$ es racional. Esto significa $\sqrt{2} = b/a$ con $a, b \in \mathbb{Z}$ sin factores comunes. Entonces, podemos escribir $2 = b^2/a^2$, $2a^2 = b^2$, y $b$ debe ser par. De esta forma, $b = 2c^2$ y, por tanto, $2a^2 = 4c^2$, $a^2 = 2c^2$. Luego, $a$ y $b$ son pares, lo cual es una contradicción. □
En la demostración anterior hemos usado la tautología de reducción al absurdo: $(p \rightarrow q), (p \rightarrow \neg q) \vDash \neg p$, tomando como $p =$"$\sqrt{2}$ es racional", $q =$"$\sqrt{2} = b/a$ con $a$ y $b$ sin factores comunes", $\neg q =$"$a$ y $b$ son pares", y $\neg p =$"$\sqrt{2}$ es irracional".

Antes de ver otro ejemplo recordaremos algunas definiciones. Un número es llamado *primo* si tiene exactamente dos divisores. Para un primo $p$ los divisores aludidos son $p$ y 1, y dicha propiedad se escribe: $p|p$ y $1|p$. Observe que 1 no es primo. Con la relación de *divisibilidad* entre dos enteros $a$ y $b$, $a|b$ estamos indicando que $b \bmod a = 0$. Esta relación tiene las siguientes propiedades: i) si $a|b$ y $a|c$ entonces $a|(b + c)$ y $a|(b - c)$, ii) si $a|b$ y $b|c$ entonces $a|c$.

**Teorema 2** Hay una cantidad infinita de números primos.

**Demostración.** Supongamos que los primos son $P = \{2, 3, 5, \ldots, p_k\}$. Claramente el número $n = (2 \cdot \ldots \cdot p_k) + 1 > p_k$ y, por tanto, debe ser divisible por algún $x > 1$ y $x < n$ (de lo contrario $n$ sería primo y tendríamos una contradicción) . Sea $m$ el menor número tal que $m|n$. $m$ debe ser primo (de no serlo, habría un $p < m$ que divide a $m$ y, por tanto, $m$ no sería el menor divisor de $n$). Como $m \in P$, $m|(n - 1)$, pero esto es imposible puesto que $m|n$. □
La demostración anterior se hace por contradicción y además dentro de ella se hace una construcción que se justifica también por contradicción, las demostraciones referidas aparecen entre paréntesis.

**Ejercicio 4** Demostrar las siguientes afirmaciones:

1. Para todo número primo mayor que dos su antecesor es par.
2. Si $c^3 = 5$ entonces $c$ es irracional.
3. El cubo de el mayor de tres enteros consecutivos no puede ser igual a la suma del cubo de los otros dos.
4. La suma de los cuadrados de tres enteros consecutivos no puede tener residuo -1 al ser dividida por 12.

### 1.1.2. Inducción

El *Principio de Inducción Matemática* (PIM) es una característica de los números naturales. Ésta surge en la construcción intuitiva de tales números, al aprender a contar: "la numeración empieza con 1$\varepsilon$ "siempre podemos obtener un número mayor sumando 1 al que tenemos". Más formalmente se dice que el conjunto de números naturales cumple la propiedad $\mathcal{A}$ si 1 la cumple, y si cualquier $n$ cumple $\mathcal{A}$ también lo hace $n + 1$: $\mathcal{A}(1)$, y $[\mathcal{A}(n) \rightarrow \mathcal{A}(n + 1)]$. Cuando deseamos probar que una propiedad es cumplida por todos los elementos de $\mathbb{N}$, basta demostrar dos cosas: (*base*:) 1 satisface dicha propiedad y, (*paso inductivo*:) suponiendo que $n \in \mathbb{N}$ la satisface (*hipótesis de inducción*), $n + 1$ también satisface la propiedad. Aclaremos lo anterior con un ejemplo.

**Proposición 1** Para todo natural se cumple $\log n < n$.

**Demostrsción.** Por inducción. Base: $\log 1 = 0 < 1$.
Inducción: Debe demostrarse que si $\log n < n$ entonces $\log(n+1) < n + 1$. Puesto que log es una función creciente al igual que su inversa: $n < 2^n$, por tanto, $(n + 1) < 2^n + 1$, pero es también cierto que $2^n + 1 < 2^n + 2^n$. Resumiendo: $(n + 1) < 2^{n+1}$ lo cual equivale a decir que $\log(n + 1) < n + 1$. □
Es común establecer la validez de una propiedad $\mathcal{A}$ solamente para una parte de los números naturales, esto es: $\mathcal{A}(n)$ para todo $n \geq n_0$, lo cual es equivalente a decir que la propiedad $\mathcal{B}(n)$ se cumple para todo $n \in \mathbb{N}$, donde $\mathcal{B}(n) \doteq \mathcal{A}(n + n_0 - 1)$. Así debe demostrarse que $\mathcal{A}(n_0)$ (base) y $\mathcal{A}(n) \rightarrow \mathcal{A}(n + 1)$ para $n \geq n_0$ (inducción). El siguiente ejemplo muestra la utilidad de esta forma del PIM.

**Proposición 2** Para todo $n \geq 5$, $2^n > n^2$.

**Demostración.** Base: $32 > 25$. Inducción: La hipótesis de inducción es $\mathcal{A}(n - 1) = 2^{n-1} > (n - 1)^2$. Parte de $\mathcal{A}(n)$ es: $2^n = 2 \cdot 2^{n-1}$. Por hipótesis de inducción $2^{n-1} > n^2 - 2n + 1$, de aquí $2^n > 2n^2 - 4n + 2 = n^2 + (n - 2)^2 - 2 > n^2$, para $n \geq 5$. □

**Ejercicio 5**

1. Diga para qué valores no se cumple $2^n \leq n^3$.