Teoría de conjuntos

Isaac Ruiz Barrera

June 29, 2025

Teoría de conjuntos

En la Teoría de Conjuntos trabajamos con *conjuntos*, que es un concepto superficialmente simple. Un conjunto es cualquier colección, agrupación o conglomeración de objetos. Por ejemplo, el conjunto de estudiantes del salón 4AM1 de la ESFM, el conjunto de todos los puntos en el plano o el conjunto de todos los gatos que son magos.

Los conjuntos no son objetos del mundo real, como las estrellas o computadoras; más bien son creados por nuestra mente, no usando nuestras manos. Nosotros tenemos la capacidad de abstracción, para pensar en una variedad de objetos que son unidos por una propiedad en común, y así formar un conjunto de objetos que poseen esa propiedad.

En este curso, nuestro enfoque principal, será desarrollar las bases para otras disciplinas matemáticas. Por lo tanto, no nos enfocamos en conjuntos de personas o cosas de la vida cotidiana, sino en objetos matemáticos, como números, puntos en el espacio, funciones o los mismos conjuntos. De hecho, los primeros tres mencionados pueden ser descritos en la teoría de conjuntos como conjuntos con cierta propiedad. Por lo que nuestro enfoque será en solo conjuntos.

Para definir conjuntos, nosotros podemos hacer uso de la lógica proposicional, por ejemplo:

- $(\exists x)(x = 2k, \quad k \in \mathbb{N})$ es el conjunto de los números pares.

Nótese que esto se asemeja a una especie de "formula" lógica. Mas adelante cuando empecemos a definir conjuntos específicos con un nombre, las guardaremos como *macros*.

A lo largo de este texto, nosotros definiremos ciertos axiomas que nos ayudaran a desarrollar la teoría.

Axioma de Existencia

$$(\exists x)(x = x)$$

Informalmente: Existe un conjunto.

Observación: Este axioma, en general, puede ser reemplazado con cualquier tautología.

Axioma de Extensionalidad

$$(\forall x)(\forall y)((\forall z)(z \in x \iff z \in y) \implies x = y)$$

Informalmente: Un conjunto esta determinado por sus elementos.

Axioma de Esquema de Comprensión/Separación

Para cada formula φ del lenguaje de la teoría de conjuntos, con una variable libre x,

$$(\forall x)(\exists y)(\forall z)(z \in y \iff (z \in x \land \varphi(z)))$$

Informalmente: para cada conjunto x, el conjunto $y = \{z \in x \mid \varphi(z)\}$ existe.

Nota: piense φ como cierta propiedad.

Teorema 1

Existe un único conjunto que no tiene elementos.
$(\exists x)(\forall \zeta)(\zeta \notin x)$

Demostración. Por el axioma de la existencia, sea a ese conjunto. Por el esquema de compresión, $\left\{\zeta \in a \middle| \zeta \neq \zeta\right\}$ es un conjunto. Note que este conjunto no tiene elementos.
La unicidad se deduce inmediatamente del axioma de Extensionalidad.

Teorema 2

No existe un conjunto universal.
$\neg(\exists x)(\forall \zeta)(\zeta \in x)$
$(\forall x)(\exists \zeta)(\zeta \notin x)$

Demostración: Supongamos, para llegar a una contradicción, que existe V tal que $\forall x(x \in V)$. Por el esquema de Compresión, existiría el conjunto

$$A := \left\{x \in V \middle| x \notin x\right\}$$

Por lo que consideremos dos casos:

$$\begin{aligned} A \in A &\implies A \notin A \\ A \notin A &\implies A \in A \end{aligned}$$

Lo cual nos lleva a una contradicción.

Conjunto Vacío

Definimos el conjunto vacío como:

$$\varnothing := \exists x(\forall z)(\zeta \notin x)$$

Algunos usos:

$$\begin{aligned} \varnothing \in A &\longrightarrow \forall x(\forall \zeta(\zeta \in x) \land x \in A) \\ \varnothing = B &\longrightarrow \forall x(\forall \zeta(\zeta \notin x) \land x = B) \\ c \in \varnothing &\longrightarrow c \neq c. \end{aligned}$$

Teorema 3

Dados a, b existen y son únicos

1. $a \cap b := \left\{ x \in a \middle| x \in b \right\} = \left\{ x \in b \middle| x \in a \right\}$
2. $a \backslash b := \left\{ x \in a \middle| x \notin b \right\}$

Axioma del par

$\forall a \forall b \exists x (\forall \zeta \in x \iff (\zeta = a \vee \zeta = b))$
Informalmente: Dados a, b el conjunto $\{a, b\}$ existe.

Axioma de Unión

$\forall x \exists y (\forall \zeta (\zeta \in y \iff (\exists w)(\zeta \in w \wedge w \in x)))$
Informalmente: Dado x, existe

$$y = \bigcup_{w \in x} w$$

(Piense a x como familia de conjuntos).

Nótese que ambos conjuntos son únicos por extensionalidad.

Unión de conjuntos

Dados a, b, sea

$$a \cup b = \bigcup_{w \in \{a,b\}} w$$

Proposición

Dado a, no existe c tal que

$$\forall \zeta (\zeta \notin a \implies \zeta \in c)$$

Es decir no existe $a^{\complement}$.

Demostración: Supongamos que existe tal c.
Entonces $a \cup c$ seria un conjunto universal, lo cual es un absurdo.

Proposición

Dados $a_1, \dots, a_n$, existe $\{a_1, \dots, a_n\}$.

Demostración: Por inducción sobre n.
$\underline{n = 1}$: Por el axioma del par existe:

$$\{a_1, a_1\} = \{a_1\}.$$

Supongamos cierto el resultado para n, y sean $a_1, \dots, a_n, a_{n+1}$ conjuntos.
Por hipótesis inductiva, existe $\{a_1, \dots, a_n\}$
Por el caso $n = 1$ $\{a_{n+1}\}$ existe.
Por lo tanto existe

$$\{a_1, \dots, a_n\} \cup \{a_{n+1}\}.$$

Axioma del conjunto potencia

Dado x existe $\mathcal{P}(x) = \left\{ y \middle| y \subseteq x \right\}$

Ejemplo: Dado $\zeta = \{a, b, c\}$, entonces

$$\mathcal{P}(\zeta) = \{\varnothing, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}.$$

Axioma de Infinitud

$(\exists x)(\varnothing \in x \wedge (\forall a \in x)(a \cup \{a\} \in x))$
Informalmente: Existe un conjunto infinito.

Ejemplo: $X = \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}, \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \dots\}$

Axioma de Fundación (Von Neumann)

$(\forall x)(x \neq \varnothing \implies (\exists y)(y \in x) \wedge (x \cap y = \varnothing))$

Proposición

Para todo x, $x \notin x$.

Demostración: Supongamos que x es tal que $x \in x$. Consideremos $\{x\}$, por fundación existe $y \in \{x\}$ tal que $y \cap \{x\} = \varnothing$ Por lo que debe tenerse que $y = x$, además $x \in x \cap \{x\} = y \cap \{x\} = \varnothing$, contradicción.

Proposición

No existen x, y tales que

$$x \in y \ \wedge \ y \in x.$$

Demostración: Supongamos que $x \in y \in x$ consideremos $\{x, y\}$, por fundación existe $\zeta \in \{x, y\}$ tal que $\zeta \cap \{x, y\} = \varnothing$ Entonces tenemos dos casos:

$$\begin{aligned} \zeta = x &\implies y \in \zeta \cap \{x, y\} \\ \zeta = y &\implies x \in \zeta \cap \{x, y\} \end{aligned}$$

Lo cual es un absurdo.

Pares Ordenados (Kuratowski)

Dados a, b definimos

$$(a, b) = \{\{a\}, \{a, b\}\}$$

Proposición

Dados a, b, c, d

$$(a, b) = (c, d) \iff (a = c \ \wedge \ b = d)$$

Demostración: $\Longleftarrow$)Trivial
$\Longrightarrow$) Supongamos que $(a, b) = (c, d)$. Entonces

$$\{\{a\}, \{a, b\}\} = \{\{c\}, \{c, d\}\}$$

en particular $\{a, b\}$ es igual a $\{c\}$ o a $\{c, d\}$, consideremos dos casos.

1. $\{a, b\} = \{c\} \implies a = b = c \therefore \{\{a\}\} = \{\{c\}, \{c, d\}\} \implies \{c, d\} = \{a\} \implies a = c = d$
2. $\{a, b\} = \{c, d\}$ de donde obtenemos dos subcasos:
   (a) $\{a\} = \{c, d\} \implies c = d = a$
   $\implies \{a, b\} = \{a\} \implies b = a$
   (b) $\{a\} = \{c\} \implies a = c$
   además $\{a, b\} = \{a, d\}$: dos subcasos
      i. $b = a \implies \{a\} = \{a, d\} \implies a = d$
      ii. $b = d$.

Notación: "x es una pareja ordenada"$\equiv (\exists a, b)(\exists \alpha, \beta)(\alpha, \beta \in x \wedge \forall \zeta(\zeta \in a \iff \zeta = a) \wedge (\forall \zeta(\zeta \in \beta \iff (\zeta = a \vee \zeta = b)) \wedge \forall \zeta(\zeta \in x \iff (\zeta = \alpha \vee \zeta = \beta)))$

Producto cartesiano

Dados A, B definimos

$$A \times B = \left\{ x \in \wp(\wp(A \cup B)) \middle| (\exists a \in A)(\exists b \in B)(x = (a, b)) \right\}$$

n-tuplas ordenadas

Se definen las $n-$tuplas ordenadas ($n \geq 2$)

- $(a_1, a_2) = \{\{a_1\}, \{a_1, a_2\}\}$
- $(a_1, \ldots, a_n, a_{n+1}) = ((a_1, \ldots, a_n), a_{n+1})$
- $A_1 \times \ldots \times A_n \times A_{n+1} = (A_1 \times \ldots \times A_n) \times A_{n+1}$

Relación Binaria

1. Una relación binaria es un conjunto cuyos elementos son parejas ordenadas.
2. $S : R \subseteq A \times B$, decimos que R es una relación entre A y B.
3. Si R es una relación binaria y $(a, b) \in R$, escribiremos aRb.

Ejemplos:

1. $\leq \subseteq \mathbb{Z} \times \mathbb{Z}$ dada por

$$\leq = \{\ldots, \ldots, (-3, 0), (-2, 0), (-1, 0), (0, 0), \ldots, (-3, 1), (-2, 1), \ldots\}$$

   (a) $\leq \subseteq \{1, \ldots, 6\}$

$$\leq = \{(1, 1), (1, 2), \ldots, (2, 2), (2, 3), \ldots, \ldots, (6, 6)\}$$

2. $\mid \subseteq \{1, \ldots, 6\}$

$$\mid = \{(1, 1), (1, 2), \ldots, (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6)\}$$

Notación: "R es una relación binaria" $\equiv (\forall x \in R)$("x es una pareja ordenada")

Operaciones de Relaciones Binarias

Sea R una relación binaria. Definimos:

1. El dominio de R es:

$$\mathrm{dom}(R) = \left\{ a \in \bigcup_{B \in \bigcup_{A \in R} A} B \,\middle|\, (\exists B)(aRb) \right\}$$

2. El rango de R o la imagen de R es:

$$\mathrm{im}(R) = \mathrm{ran}(R) = \left\{ b \in \bigcup_{B \in \bigcup_{A \in R} A} B \,\middle|\, (\exists a)(aRb) \right\}$$

3. Si $A \subseteq \mathrm{dom}(R)$, definimos:

   (a) La restricción de R a A

$$R \restriction A = \left\{ (a,b) \in R \,\middle|\, a \in A \right\}$$

   (b) La imagen de A bajo R:

$$R[A] = \left\{ b \in \mathrm{ran}(R) \,\middle|\, (\exists a \in A)(aRb) \right\} = \mathrm{ran}(R \restriction A)$$

4. Si $B \subseteq \mathrm{ran}(R)$, entonces:
   La pre-imagen de B bajo R:

$$R^{-1}[B] = \left\{ a \in \mathrm{dom}(R) \,\middle|\, (\exists b \in B)(aRb) \right\}$$

5. La relación inversa de R es:

$$R^{-1} = \left\{ (b,a) \in \mathrm{ran}(R) \times \mathrm{dom}(R) \,\middle|\, (a,b) \in R \right\}$$

6. Si S es otra relación binaria, entonces:

$$R \circ S = \left\{ (a,c) \in \mathrm{dom}(S) \times \mathrm{ran}(R) \,\middle|\, (\exists b)(aSb \ \wedge \ bRc) \right\}$$

Función

Si f es una relación binaria, diremos que es una función si:

$$\forall x \in \mathrm{dom}(f)\ \exists! y \in \mathrm{ran}(f) \big((x,y) \in f \big)$$

Nota: Si f es función y $y \in \mathrm{dom}(f)$, denotamos al único y tal que $(x,y) \in f$ como $f(x)$

Al igual que con las relaciones, podemos definir operaciones en funciones:

Imagen de A bajo f

Suponga que $\text{ran}(f)$ y $\text{dom}(f)$ ya están definidos
Si $A \subseteq \text{dom}(f)$,

$$f[A] = \left\{ b \in \text{ran}(f) \middle| \, a \in A \; (a,b) \in f \right\}$$

$$= \left\{ b \in \text{ran}(f) \middle| \, \exists a \in A, \; b = f(a) \right\}$$

$$= \left\{ f(a) \middle| \, a \in A \right\}$$

Pre-imagen de B bajo f

Si $B \subseteq \text{ran}(f)$,

$$f^{-1}[B] = \left\{ a \in \text{dom}(f) \middle| \, \exists b \in B \; \big((a,b) \in f\big) \right\}$$

$$= \left\{ a \in \text{dom}(f) \middle| \, \exists b \in B \; (f(a) = b) \right\}$$

$$= \left\{ a \in \text{dom}(f) \middle| \, f(a) \in B \right\}$$

Notación: $f : A \to B$ significa:

$$(f \text{ es una función}) \wedge (A = \text{dom}(f)) \wedge (\text{ran}(f) \subseteq B).$$

Inyectiva suprayectiva y biyeccion

Si f es una función, entonces diremos que:

1. f es inyectiva si:

$$\big(\forall a, b \in \text{dom}(f)\big)\big(f(a) = f(b) \implies a = b\big)$$

2. Dado un conjunto B, diremos que f es suprayectiva en B o sobre B si:

$$(\text{ran}(f) \subseteq B) \wedge (\forall b \in B)(\exists a \in \text{dom}(f))(f(a) = b)$$

3. "$f : A \to B$ es biyectiva" significa:

$$(f : A \to B) \wedge (f \text{ es inyectiva}) \wedge (f \text{ es sobre } B).$$

Composición de funciones

Sean f, g funciones

$$g \circ f = \left\{ (a,c) \in \text{dom}(f) \times \text{ran}(g) \,\middle|\, \exists b \, (f(a) = b \ \wedge \ c = g(b)) \right\}$$

$$= \left\{ (a,c) \in \text{dom}(f) \times \text{ran}(g) \,\middle|\, f(a) \in \text{dom}(g) \ \wedge \ c = f\big(g(a)\big) \right\}$$

Ejemplos:

$f : \mathbb{R} \to \mathbb{R}$
$\quad x \mapsto x^2$
$g : \mathbb{C} \to \mathbb{C}$
$\quad z \mapsto e^z$

$$g \circ f = \varnothing$$

Proposición

Si $\underbrace{f : A \to B \text{ y } g : B \to C}_{\text{ran}(f) \subseteq \text{dom}(g)}$ entonces $g \circ f : A \to C$ y $g \circ f(a) = g\big(f(a)\big)$ $\forall a \in A$.

Demostración:

$$g \circ f = \left\{ (a,c) \in \text{dom}(f) \times \text{ran}(g) \,\middle|\, f(a) \in \text{dom}(g) \ \wedge \ c = g\big(f(a)\big) \right\}$$

$$= \left\{ \big(a, f\big(g(a)\big)\big) \,\middle|\, f(a) \in \text{dom}(g) \right\}$$

$$= \left\{ \big(a, g\big(f(a)\big)\big) \,\middle|\, a \in A \right\}$$

$$\therefore g \circ f : A \to C.$$

Función Inversa

Sea $f : A \to B$ función, definimos $f^{-1} : \text{ran}(f) \to A$

$$f^{-1} = \left\{ (b,a) \in \text{ran}(f) \times \text{dom}(f) \,\middle|\, b = f(a) \right\}$$

Proposición

Si f es una función, entonces f^{-1} es también una función $\iff$ f es inyectiva, en cuyo caso $f^{-1} : \text{ran}(f) \to \text{dom}(f)$

Demostración:

$$f^{-1} \text{ es una función} \iff \forall b \in \text{dom}(f^{-1}) \, \exists! a \, (b,a) \in f^{-1}$$

$$\iff \forall b \in \text{ran}(f) \, \exists! a \in \text{dom}(f) \, (a,b) \in f$$

$$\iff \forall b \in \operatorname{ran}(f)\, \forall a, a' \in \operatorname{dom}(f)\ \underbrace{(a,b) \in f}_{b=f(a)} \wedge \underbrace{(a',b) \in f}_{b=f'(a)} \implies a = a'$$

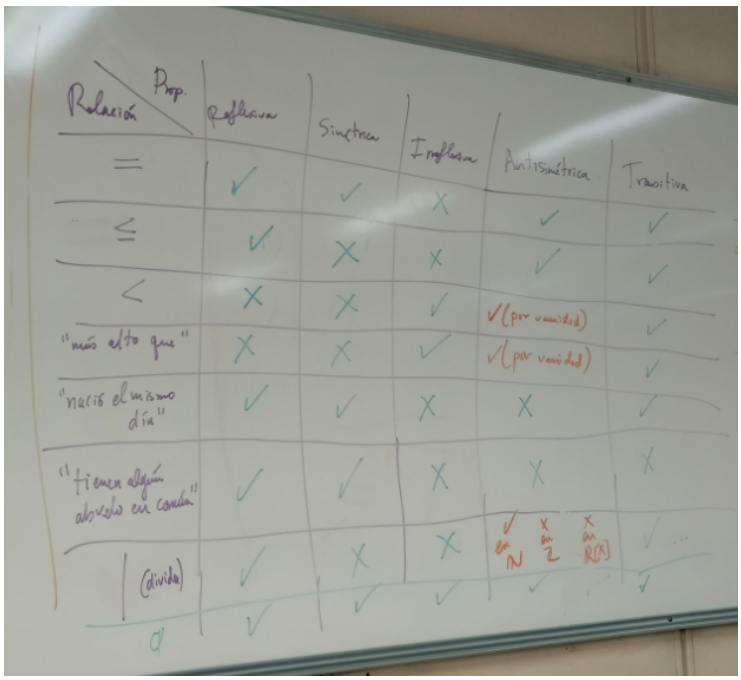
$$\forall a, a' \in \operatorname{dom}(f)(f(a) = f(a') \implies a = a')$$

Tipos de relaciones

Sea R una relación. Diremos que R es:

1. **Reflexiva** si: $\forall a \in \operatorname{dom}(R) \quad aRa$
2. **Simétrica** si: $\forall a \in \operatorname{dom}(R),\ \forall b \in \operatorname{ran}(R) \quad aRb \implies bRa$
3. **Irreflexiva** si: $\forall a \in \operatorname{dom}(R) \quad \underbrace{a \not R a}_{a \not R a \equiv \neg(aRa)}$
4. **Antisimétrica** si: $\forall a, b \in \operatorname{dom}(R) \cup \operatorname{ran}(R) \quad aRb \wedge bRa \implies a = b.$
5. **Transitiva** si: $\forall a, b, c \in \operatorname{dom}(R) \cup \operatorname{ran}(R) \quad aRb \wedge bRc \implies aRc.$

Ejemplos:



Relaciones de Equivalencia.

Sea A. Una relación binaria $E \subseteq A \times A$ se llamará de equivalencia si satisface las siguientes tres propiedades.

1. E es reflexiva: $[\forall a \in A\ (aEa)]$
2. E es simétrica: $[\forall a, b \in A\ (aEb \implies bEa)]$
3. E es transitiva: $[\forall a, b, c \in A\ (aEb \wedge bEc) \implies aEc]$

Ejemplos:

1. "Tener la misma estatura"
2. "Tener el mismo cumpleaños"
3. Dado $m \in \mathbb{N}\backslash\{1\}$, "Dejan el mismo residuo al dividir entre m"
   Congruencia módulo m
4. En $\left\{ T \subseteq \mathbb{R}^2 \middle| \ T \text{ es un triangulo} \right\}$
   (a) "Ser congruente."
   (b) "Ser similar."

Clases de equivalencia

Sea A, y sea $E \subseteq A \times A$ una relación de equivalencia.

1. Para cada $a \in A$, definimos la clase de equivalencia de a como
$$[a]_E = \left\{ b \in A \middle| \ aEb \right\}$$
2. El conjunto cociente de A módulo E es
$$A/E = \left\{ [a]_E \middle| \ a \in A \right\}$$
$$= \left\{ x \in \mathcal{P}(A) \middle| \ \exists a \in A\ x = [a]_E \right\}$$

Ejemplo: Si la relación de equivalencia es "congruencia módulo 2" en $\mathbb{N}$ entonces:

$[8]_E$ = Conjunto de los números pares = $\mathbb{P}$
$[13]_E$ = Conjunto de los números impares = $\mathbb{I}$
$N/E = \{\mathbb{P}, \mathbb{I}\}$

Partición

Dado X una partición de X es un conjunto $\mathcal{P} \subseteq \mathscr{P}(X)$ tal que:

1. $\emptyset \notin \mathcal{P}$
2. $\forall A, B \in \mathcal{P}\ (A \neq B \implies A \cap B = \emptyset)$
3. $$X = \bigcup_{A \in \mathcal{P}} A \qquad (\forall x \in X)(\exists A \in \mathcal{P})(x \in A)$$

Ejemplos:

1. $\{\mathbb{P}, \mathbb{I}\}$ es una partición de $\mathbb{N}$
2. {1A, 1B, 2A, 2B, 3A, 3B} es una partición de la escuela "Benito Juarez".
3. $\{Q_1, Q_2, Q_3, Q_4\}$ en donde

$$Q_1 = \left\{ (x, y) \in \mathbb{R}^2 \,\middle|\, x \geq 0 \text{ y } y \geq 0 \right\}$$
$$Q_2 = \left\{ (x, y) \in \mathbb{R}^2 \,\middle|\, x < 0 \text{ y } y \geq 0 \right\}$$
$$Q_3 = \left\{ (x, y) \in \mathbb{R}^2 \,\middle|\, x \leq 0 \text{ y } y < 0 \right\}$$
$$Q_4 = \left\{ (x, y) \in \mathbb{R}^2 \,\middle|\, x > 0 \text{ y } y < 0 \right\}$$

   es una partición de $\mathbb{R}^2$

4. $\left\{ \{2n-1, 2n\} \,\middle|\, n \in \mathbb{N} \right\}$ es una partición de $\mathbb{N}$

Observación: Si $\mathcal{P}$ es una partición de X, entonces se cumple:

$$(\forall x \in X)(\exists! A \in \mathcal{P})(x \in A)$$

Teorema

Si E es una relación de equivalencia sobre X entonces

$$X/E = \left\{ [a]_E \,\middle|\, a \in X \right\} \text{ es una partición de } X$$

Demostración: Verificaremos que X/E satisface los tres puntos de la definición de partición:

1. Si $[a]_E \in X/E$ es arbitrario, entonces:

$$aEa \quad \text{(por reflexividad)}$$

2. Sean $[a]_E, [b]_E \in X/E$ y supongamos (por contra-positiva) que $[a]_E \cap [b]_E \neq \emptyset$, es decir, existe $c \in X$ tal que $\underbrace{c \in [a]_E}_{cEa}$ y $\underbrace{c \in [b]_E}_{cEb}$.

Sea $x \in [a]_E$. Entonces, por xEa. Como aEc entonces por transitividad xEc. Como además cEb, por transitividad $xEb \therefore x \in [b]_E$

$$\implies [a]_E \subseteq [b]_E.$$

Recíprocamente sea $y \in [b]_E$. Entonces yEb; como además $bEc \underset{\text{(transitiva)}}{\implies} yEc$; como además $cEa \underset{\text{(transitiva)}}{\implies} yEa \therefore y \in [a]_E$

$$\implies [b]_E \subseteq [a]_E \therefore [b]_E = [a]_E$$

3. Dado $a \in X$, como $aEa \implies a \in [a]_E$

$$\therefore a \in \bigcup_{a \in A} [a]_E = \bigcup_{x \in X/E} x.$$

Un ejemplo importante: Si A es, y $f : A \to B$.
Sea $E_f = \left\{ (a,b) \in A \times A \,\middle|\, f(A) = f(B) \right\}$

E_f es "Tener el mismo valor bajo f "

Observación: E_f es una relación de equivalencia sobre A.

1. Para cada $a \in A$, $f(a) = f(a) \therefore aE_f a$
2. Supongamos que $a, b \in A$ son tales que $aE_f b$

$$\implies f(a) = f(b) \implies f(b) = f(a) \implies bE_f a$$

$\therefore$ Es simétrica.

3. Si $a, b, c \in A$ son tales que $aE_f b$ y $bE_f c$, entonces:

$$f(a) = f(b) \text{ y } f(b) = f(c) \therefore f(a) = f(c)$$

$\implies aE_f c \implies E_f$ es transitiva.

Teorema

Sea A y sea E relación binaria. Entonces las siguientes proposiciones son equivalentes:

1. E es de equivalencia
2. Existe una partición $\mathcal{P}$ de A tal que

$$\forall a, b \in A \; (aEb \iff \exists z \in \mathcal{P}) \quad a, b \in z$$

3. Existe un B y existe $f : A \to B$ tal que $E = E_f$, i.e.

$$\forall a, b \in A \; (aEb \iff f(a) = f(b))$$

Demostración:

1. $\implies$ 2. Si E es de equivalencia, basta tomar

$$\mathcal{P} = A/E$$

3. $\implies$ 1. Se demostró en el "ejemplo importante".

2. $\implies$ 3. Si $\mathcal{P}$ es una partición de A, entonces sea $f = \left\{ (x, y) \in A \times \mathcal{P} \middle| \, x \in z \right\}$. Dado que $\mathcal{P}$ es una partición, $\forall x \, \exists! z \, (x, z) \in f$, por lo tanto

$$\begin{aligned} f &: A \to \mathcal{P} \\ a &\mapsto \text{único } z \in \mathcal{P} \text{ tal que } a \in z. \end{aligned}$$

Entonces, dados $a, b \in A$, tenemos que:

$$\begin{aligned} aEb &\iff \exists z \in \mathcal{P} \text{ tal que } a, b \in z \\ &\iff f(a) = f(b). \end{aligned}$$

Proyección canónica

Si $E \subseteq A \times A$ es una relación de equivalencia, se define la proyección canónica:

$$\begin{aligned} \pi_E &: A \to A/E \\ a &\mapsto [a]_E. \end{aligned}$$

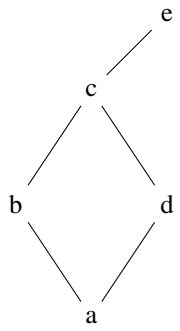
Relaciones de Orden Parcial

Una relación $R \subseteq A \times A$ es de orden parcial en A si es

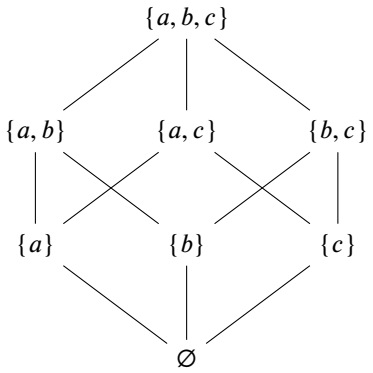
1. Reflexiva $\quad \forall a \in A \, (aRa)$
2. Antisimetrica $\quad \forall a, b \in A \, (aRb \, \wedge \, bRa) \implies a = b$
3. Transitiva $\quad \forall a, b, c \in A \, (aRb \, \wedge \, bRc) \implies aRc$

Ejemplos:

1. En $\mathbb{R}$,
$$\left\{ (a, b) \in \mathbb{R} \times \mathbb{R} \middle| \, a \leq b \right\}$$
2. En $\mathbb{N}$,
$$\left\{ (a, b) \in \mathbb{N} \times \mathbb{N} \middle| \, a \middle| b \right\}$$
3. Dado X, la relación:
$$\left\{ (A, B) \in \mathcal{P}(X) \times \mathcal{P}(X) \middle| \, A \subseteq B \right\}$$
en $\mathcal{P}(X)$.
4. En $\{a, b, c, d, e\}$:
$$\{(a,a), (b,b), (c,c), (d,d), (e,e), (a,b), (b,c), (a,c), (a,d), (d,c), (a,c)\}$$



En el ejemplo 3, si $X = \{a, b, c\}$ entonces su diagrama de Hasse es:



Notación: Para relaciones de orden parcial usaremos los símbolos:

$$\leq, \lesssim, \preceq, \sqsupseteq$$

Observaciones: Sea A un conjunto y $\leq$ una relación de orden parcial en A.

1. Si $a_1, \ldots, a_n \in A$ son tales que $a_1 \leq a_2 \leq \ldots \leq a_n \leq a_1$ entonces:

$$a_1 = a_2 = \ldots = a_n$$

   Demostración:
   Por inducción sobre n
   $n = 1$ Inmediata
   $n = 2$ Por simetría
   Considere

$$a_1 \leq a_2 \leq \ldots \leq a_n \leq a_{n+1} \leq a_1$$

   por hipótesis de inducción

$$a_1 = \ldots = a_n \quad \text{y} \quad a_1 \leq a_{n+1} \leq a_1$$

$$\Longrightarrow \text{ Por simetría, } a_{n+1} = a_1.$$

2. (Ejercicio) Si R es una relación de orden parcial, entonces R^{-1} también lo es.
   Demostración: Sea $\leq$ relación de orden parcial en A denotaremos a $\leq^{-1}$ como $\geq$. Si $\leq$ es una relación de orden parcial, entonces

(a) $\leq$ es reflexiva $\quad (\forall a \in A)(a,a) \in \leq$

(b) $\leq$ es antisimétrica $\quad (\forall a,b \in A)(a,b) \in \leq \ \wedge (b,a) \in \leq \implies a = b$

(c) $\leq$ es transitiva $\quad (\forall a,b,c \in A)(a,b) \in \leq \ \wedge (b,c) \in \leq \implies (a,c) \in \leq$

Luego definimos $\geq$ como:

$$\geq := \left\{ (b,a) \middle| \ (a,b) \in \leq \right\}$$

Es claro que $\geq$ es reflexiva. Luego, si $(a,b) \in \geq$ y $(b,a) \in \geq$ por definición de $\geq$ si $(b,a) \in \geq$, entonces $(a,b) \in \leq$ a su vez, si $(a,b) \in \geq$, entonces $(b,a) \in \leq$, puesto que $\leq$ es antisimétrica, entonces $a = b$.
Finalmente, si $(b,a) \in \geq$, entonces $(a,b) \in \leq$, si $(c,a) \in \geq$, entonces, $(a,c) \in \leq$, puesto que $\leq$ es transitiva $(a,c) \in \leq$ y por definición de $\geq$, entonces $(c,a) \in \geq$ por lo que $\geq$ es transitiva.

Relaciones de Orden estricto

Una relación $R \subseteq A \times A$ es de orden estricto en A si es

1. Irreflexiva $\quad \forall a \in A \ (a \not R a)$
2. Transitiva $\quad \forall a,b,c \in A \ (aRb \ \wedge \ bRc) \implies aRc$

Ejemplos:

1. En $\mathbb{R}$,
$$\left\{ (a,b) \in \mathbb{R} \times \mathbb{R} \middle| \ a < b \right\}$$
2. En $\mathbb{N}$,
$$\left\{ (a,b) \in \mathbb{N} \times \mathbb{N} \middle| \ a \middle| b \ \wedge a \neq b \right\}$$
3. Dado X, la relación:
$$\left\{ (A,B) \in \mathcal{P}(X) \times \mathcal{P}(X) \middle| \ A \subsetneq B \right\}$$
en $\mathcal{P}(X)$.
4. En $\{a,b,c,d,e\}$:
$$\{(a,b),\ (b,c),\ (a,c),\ (a,d),\ (d,c),\ (a,c)\}$$

Notación: Para relaciones de orden estricto usaremos los símbolos:

$$<, \lesssim, \prec, \sqsubset$$

Teorema

1. Si $\preceq \subseteq A \times A$ es una relación de orden parcial en A, entonces

$$\prec = \left\{ (a,b) \in A \times A \,\middle|\, a \preceq b \text{ y } a \neq b \right\}$$

es una relación de orden estricto.

2. Si $< \subseteq A \times A$ es una relación de orden estricto en A, entonces

$$\leq = \left\{ (a,b) \in A \times A \,\middle|\, a < b \text{ o } a = b \right\}$$

es una relación de orden parcial.

Demostración:

1. **Irreflexividad:** Dado $a \in A$, $\quad a = a \implies \neg(a \neq b) \therefore a \not\prec a$
Transitividad: Supongamos que $a, b, c \in A$ son tales que

$$\underbrace{a \prec b}_{a \preceq b \text{ y } a \neq b} \text{ y } \underbrace{b \prec c}_{b \preceq c \text{ y } b \neq c}$$

$$\implies a \preceq c$$

además si $a = c$, entonces $a \preceq b$ y $b \preceq c \implies a = b$ contradicción.

$$\therefore a \neq c \implies a \prec c$$

2. **Reflexividad:** Dado $a \in A$, $a = a \implies a \leq a$
Antisimetria: Supongamos que $a, b \in A$ son tales que $a \leq b$ y $b \leq a$. Entonces, como $a \leq b$, significa que o bien $a < b$ o bien $a = b$; en este ultimo caso hemos terminado $\therefore$ sin perdida de generalidad $a < b$. además, o bien $b < a$ o bien $b = a$; en este ultimo caso hemos terminado $\therefore$ sin perdida de generalidad, suponemos que $b < a$. Entonces $a < b$ y $b < a$, por transitividad $a < a$ lo que contradice la irreflexividad.
Transitividad: Supongamos $a, b, c \in A$ tales que $a \leq b$ y $b \leq c$. Tenemos 4 casos si $a < b$ y $b < c \implies a < c$ por transitividad, si $a < b$ y $b = c \implies a < c$, si $a = b$ y $b < c$ entonces $a < c$, por ultimo, si $a = b$ y $b = c$ entonces $a = c$. En cada caso, podemos concluir que $a \leq c$.

Comparables Ordenes Totales o Lineales

Sea A, sean $\precsim \subseteq A \times A$ relación de orden parcial
$< \subseteq A \times A$ relación de orden estricto

1. Decimos que $a, b \in A$ son comparables si

$$(a \precsim b) \vee (b \precsim a)$$
$$(a < b) \vee (b < a) \vee (a = b)$$

2. Decimos que $\lesssim$ Es un orden total o lineal
$\leq$ Es un orden estricto total o lineal
si

$$(\forall a, b \in A)(a \text{ y } b \text{ son comparables}).$$

Ejemplos:

- En el ejemplo de divisibilidad en $\mathbb{N}$, 2 y 4 son comparables, pero 2 y 17 no son comparables.
- $\leq$ en $\mathbb{R}$ es un orden total/lineal.
- $\mid$ en $\mathbb{N}$ no es un orden total/lineal.
- $\subseteq$ en $\mathcal{P}(X)$ no es un orden total/lineal.

Minimal, Maximal, Cota Superior, Cota Inferior, Mínimo, Máximo, Supremo e Ínfimo

Sea $\begin{matrix}\precsim\\ <\end{matrix}$ una relación de orden $\begin{matrix}\text{parcial}\\ \text{estricto}\end{matrix}$ en A:

1. $a \in A$ es minimal si $\begin{matrix}\forall b \in A\ (b \precsim a \implies a = b)\\ \forall b \in A\ \neg(a < b)\end{matrix}$

2. $a \in A$ es maximal si $\begin{matrix}\forall b \in A\ (a \precsim b \implies a = b)\\ \forall b \in A\ \neg(b < a)\end{matrix}$

3. Si $X \subseteq A$, $a \in A$ es una cota superior de X si

$$\forall x \in X\ (x \precsim a) \quad \forall x \in X (x \prec a \text{ o } x = a)$$

4. Si $X \subseteq A$, $a \in A$ es una cota inferior de X si

$$\forall x \in X\ (a \precsim x) \quad \forall x \in X (a \prec x \text{ o } a = x)$$

5. Si $X \subseteq A$ y $a \in X$, a es un mínimo de X si

$$(\forall x \in X)\,(a \underset{x \prec a \text{ o } a = x}{\preceq} x)$$

6. Si $X \subseteq A$ y $a \in X$, a es un máximo de X si

$$(\forall x \in X)\,(x \underset{x \prec a \text{ o } x = a}{\preceq} a)$$

7. Si $X \subseteq A$, $a \in X$ es un supremo para X si es un mínimo para

$$\left\{ b \in A \,\middle|\, b \text{ es cota superior de } X \right\}$$

8. Si $X \subseteq A$, $a \in X$ es un supremo para X si es un máximo para

$$\left\{ b \in A \,\middle|\, b \text{ es cota inferior de } X \right\}.$$

Ejemplos.

- En $\mathbb{R}$ con $\leq$

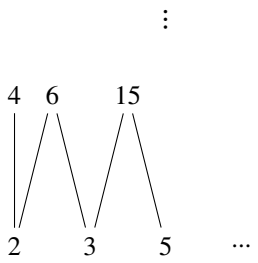
$-1, -2, -5, -\pi$ son cotas inferiores para $(0, 1)$

0 es un ínfimo para $(0, 1)$

$3, \dfrac{9}{2}, 10^6$ son cotas superiores para $[0, 1]$

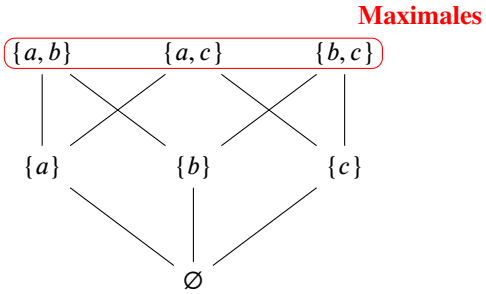
1 es un máximo y también un supremo para $[0, 1]$.

- En $\mathbb{N}\backslash\{1\}$ con $\mid$



  Los números primos son elementos minimales. No hay elemento mínimo.

- En $\wp(X)\backslash\{X\}$ con $\subseteq$



Teorema

Sea A, sea $\lesssim$ relación de orden parcial en A.

1. Si existe un mínimo para $X \subseteq A \implies$ es único. $\min(X)$
2. Si existe un máximo para $X \subseteq A \implies$ es único. $\max(X)$
3. Si existe un supremo para $X \subseteq A \implies$ es único. $\sup(X)$
4. Si existe un ínfimo para $X \subseteq A \implies$ es único. $\inf(X)$
5. Si $\lesssim$ es lineal, entonces minimal $\implies$ mínimo.
6. Si $\lesssim$ es lineal, entonces maximal $\implies$ máximo.

Demostración:

1. Si a, a' son mínimos para X entonces: $a, a' \in X$

$$\implies \begin{array}{ll} a \lesssim a' & (a \text{ es mínimo}) \\ a' \lesssim a & (a' \text{ es mínimo}) \end{array}$$

   $\implies a = a'$.

2. Sean a, a' máximos para X entonces:

$$\implies \begin{array}{ll} a \gtrsim a' & a \text{ es máximo} \\ a' \gtrsim a & a' \text{ es máximo} \end{array}$$

$\implies a = a'$.

3. Se sigue inmediato de 2.

4. Se sigue inmediato de 1.

5. Sea $a \in A$ un elemento minimal, y sea $b \in A$ arbitrario.
   Al ser $\lesssim$ lineal o bien $a \lesssim b$ o bien $b \lesssim a \implies a = b$ por minimalidad $\therefore a \lesssim b$.

6. Sea $a \in A$ un elemento maximal, y sea $b \in A$ arbitrario.
   Al ser $\lesssim$ lineal o bien $a \gtrsim b$ o bien $b \gtrsim a \implies a = b$ por maximalidad $\therefore a \gtrsim b$.

Relaciones de Buen Orden

Una relación $\leq \subseteq A \times A$ de orden parcial en A es un buen orden si:

$$(\forall X \subseteq A)(X \neq \varnothing \implies \exists a \in X(a \text{ es un mínimo para } X))$$

Ejemplos:

1. $\mathbb{N}$ equipados con $\mid$ no es un buen orden.

2. $\mathbb{R}$ equipado con $\leq$ no es un buen orden. $\big((0,1)$ no tiene mínimo$\big)$

3. $\mathbb{N}$ equipados con $\leq$, si son un buen orden.

4. $\mathbb{Z}$, equipados con la relación

$$\sqsubseteq = \left\{ (n,m) \,\middle|\, \text{o bien: } \begin{array}{l} n, m < 0 \text{ y } m \leq n \\ n, m \geq 0 \text{ y } m \geq n \\ n < 0 \text{ y } m \geq 0 \end{array} \right\}$$

   también es un buen orden.

5. En $\mathbb{R}$, los siguientes subconjuntos:

$$\left\{ 1 - \frac{1}{n} \,\middle|\, n \in \mathbb{N} \right\}$$

$$\left\{ 1 - \frac{1}{n} \,\middle|\, n \in \mathbb{N} \right\} \cup \{1\}$$

$$\left\{ 1 - \frac{1}{n} \,\middle|\, n \in \mathbb{N} \right\} \cup \left\{ 2 - \frac{1}{n} \,\middle|\, n \in \mathbb{N} \right\}$$

$$\left\{ m - \frac{1}{n} \,\middle|\, n, m \in \mathbb{N} \right\}$$

Proposición

Si $\leq$ es una relación de buen orden en A, entonces $\leq$ es una relación de orden total (lineal).

Demostración: Sean $a, b \in A$ arbitrarios. Como $\{a, b\} \neq \emptyset$, entonces hay un $c \in \{a, b\}$ que es un mínimo para ese conjunto,

$$\left.\begin{array}{l} \text{si } c = a \implies a \leq b \\ \text{si } c = b \implies b \leq a \end{array}\right\} \implies a, b \text{ son comparables.}$$

Segmento

Si $\leq$ es una relación de orden parcial en A, y $a \in A$, definimos:

$$\text{seg}(a) = \left\{ x \in a \,\middle|\, x < a \right\}$$

Teorema (Principio de Inducción Transfinita)

Sea $\leq$ una relación de buen orden en A. Sea $X \subseteq A$.
Si para todo $a \in A$ se cumple

$$\text{seg}(a) \subseteq X \implies a \in X,$$

entonces $X = A$.

Demostración: Supongamos que no, entonces

$$\forall a \in A \, (\text{seg}(A) \subset X \implies a \in X)$$

pero $X \neq A$, i.e. $X \subsetneq A$.
Entonces $A \backslash X$ es un subconjunto no vacío de A y $\therefore$ existe $a \in A \backslash X$ tal que $a = \min(A \backslash X)$. Entonces, si $b \in \text{seg}(a) \implies b < a \implies b \notin A \backslash X$ por minimalidad de a, $\therefore b \in X$. De esta forma, $\text{seg}(a) \subseteq X$. $\therefore$ Por hipótesis, $a \in X \implies a \notin A \backslash X$, una contradicción.

Teorema

Sea $\leq$ una relación de orden lineal en A tal que,

$$\forall y \subseteq A \left(\forall a \in A \, (\text{seg}(A) \subseteq y \implies a \in y) \implies y = A \right).$$

Entonces $\leq$ es un buen orden.

Demostración: Sea $X \subseteq A$ no vacío arbitrario.
Sea

$$Z = \left\{ \zeta \in A \,\middle|\, \forall x \in X \, (\zeta < x) \right\}.$$

Sabemos que $Z \neq A$ (pues $X \neq \emptyset$) $\therefore$ por hipótesis, $\exists a \in A$ tal que $\text{seg}(a) \subseteq Z$ pero $a \notin Z$.
Notemos que a es cota inferior de X:

Si $x \in X$ es arbitrario, entonces: $\begin{cases} a < x \\ a = x \\ x < a \end{cases}$

Si $x < a$, entonces $x \in \text{seg}(a) \subseteq Z \implies x$ es cota inferior estricta para X, una contradicción.
$\therefore a \leq x$ y $\therefore a$ es cota inferior para X.
$\therefore \forall x \in X, \, a \leq x$

Afirmación: No es el caso que $\forall x \in X,\ a < x$, pues si lo fuera, tendríamos $a \in Z$, contradicción.

$$\therefore \exists x \in X \text{ tal que } a = x \implies a \in X \therefore a = \min(X).$$

Construcción de $\mathbb{N}$

Sistema de Peano

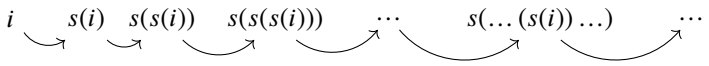
Un sistema de Peano es una terna (N, s, i) tal que:

1. $i \in N$
2. $s : N \to N$
3. $i \notin \text{ran}(s)$ (i no es sucesor de nadie)
4. s es inyectiva
5. (Propiedad de Inducción)

$$\forall A \subseteq N\ (i \in A \ \wedge\ (\forall a \in A)(s(a) \in A)) \implies A = N$$

Nota: Piense a s como "tomar el sucesor inmediato" y a i como "elemento inicial".

Intuitivamente, un sistema de Peano se ve:



No puede ser un cíclico o pseudo-cíclico.

Proposición

Sea (N, s, i) un sistema de Peano. Entonces:

$$\big(\forall a \in N)(a = i \ \vee\ (\exists b \in N)(a = s(b))\big).$$

Demostración: Sea $A = \left\{ a \in N \,\middle|\, a = i \ \vee\ (\exists b \in N)(a = s(b)) \right\}$
Como $i = i \implies i \in A$.
Supongamos que $a \in A$, entonces $s(a)$ satisface $(\exists b \in N)(s(a) = s(b)) \quad \therefore s(a) \in A$
así, por la propiedad de inducción $A = N$

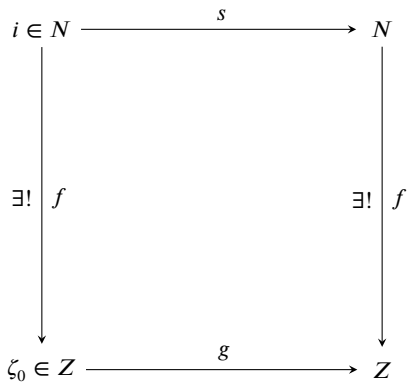
Teorema (Recursivo para sistemas de Peano)

Sea (N, s, i) un sistema de Peano, para todo Z, para todo $\zeta_0 \in Z$, y para toda $g : Z \to Z$, existe una única $f : N \to Z$ tal que:

$$f(i) = \zeta_0$$

$$\forall a \in N \quad f(s(a)) = g(f(a))$$

Bajo un diagrama conmutativo:



Aclaración: La demostración es muy larga, pues la expresión es auto-referencial:

$$\boxed{f} = \left\{ (a,b) \in N \times Z \,\middle|\, (a = i \ \wedge \ b = \zeta_0) \vee (a = s(c)) \wedge (b = g(\boxed{f(c)})) \right\}$$

Demostración: Diremos que "h es aceptable" si:
"(h es función)$\wedge$(dom$(h) \subseteq N$)$\wedge$ (ran$(h) \subseteq Z$) $\wedge$ $\underset{i \in \mathrm{dom}(h) \wedge h(i) = \zeta_0}{((i, \zeta_0) \in h)}$ $\wedge (\forall a \in N)\big(s(a) \in$ dom$(h) \implies a \in \mathrm{dom}(h) \wedge \ h(s(a)) = g(h(a))\big)$".
Sea

$$A = \left\{ a \in N \,\middle|\, (\exists h)(h \text{ es aceptable}) \wedge \ a \in \mathrm{dom}(h) \right\}$$

Note que $i \in A$: Pues $\{(i, \zeta_0)\}$ es aceptable y tiene a i en su dominio.
Ahora suponga que $a \in A$, y sea h aceptable tal que $a \in \mathrm{dom}(h)$.

$$\text{Dos casos} \begin{cases} s(a) \in \mathrm{dom}(h) \implies s(a) \in A. \\ s(a) \notin \mathrm{dom}(h), \text{entonces:} \end{cases}$$

$h \ \cup \{(s(a), g(h(a)))\}$ es una función aceptable que contiene a $f(a)$ en su dominio $\implies s(a) \in A$.
Por el principio de inducción,

$$A = N$$

Sea

$$f = \left\{ (a, \zeta) \in N \times Z \,\middle|\, (\exists h)(h \text{ es aceptable } \ \wedge \ a \in \mathrm{dom}(h) \wedge \zeta = h(a)) \right\}$$

f es una relación binaria de N a Z, y $\text{dom}(f) = N$, $\text{ran}(f) \subseteq Z$.
Sea

$$B = \left\{ a \in N \,\middle|\, \exists!\zeta\big((a,\zeta) \in f\big) \right\}$$

$$= \left\{ a \in N \,\middle|\, \forall h, h'\big(h, h' \text{ son aceptables} \wedge a \in \text{dom}(h) \wedge a \in \text{dom}(h')\big) \implies h(a) = h'(a) \right\}.$$

$i \in B$: Pues si h, h' son aceptables y $i \in \text{dom}(h),\ i \in \text{dom}(h')$ entonces:

$$h(i) = \zeta_0 = h'(i).$$

Supongamos que $a \in B$ y sean h, h' funciones aceptables con $s(a) \in \text{dom}(h),\ s(a) \in \text{dom}(h')$.
Entonces,

$$h(s(a)) = g(h(a)) \underset{\text{Hip. Ind.}}{=} g(h'(a)) = h'(s(a))$$

Por el principio de inducción, $b = N$

$$\therefore f \text{ es función y } f : N \to Z$$

Note además que:

$$f(i) \underset{h \text{ aceptable}}{=} h(i) = \zeta_0,$$

y si $a \in N$, entonces

$$f(s(a)) \underset{h \text{ aceptable } s(a) \in \text{dom}(h)}{=} h(s(a)) = g(h(a)) = g(f(a)).$$

Esto finaliza la existencia de f.
Para la unicidad, supongamos que existe $f' : N \to Z$ tal que $f'(i) = \zeta_0$ y $\forall a \in N \quad f'(s(a)) = g(f'(a))$.
Sea $C = \left\{ a \in N \,\middle|\, f(a) = f'(a) \right\}$, $i \in C$ pues $f(i) = \zeta_0 = f'(i)$.
Supongamos que $a \in C$, entonces

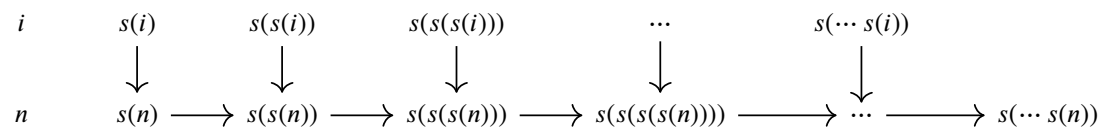
$$f(s(a)) = g(f(a)) \underset{H.I.}{=} g(f'(a)) = f'(s(a))$$

Por el principio de inducción, $C = N$

$$\therefore f = f'.$$

Adición: Sea (N, s, i) un sistema de Peano.
Sea $n \in N$. Por el teorema de recursión existe una única $A_n : N \to N$ tal que:

$$A_n(i) = s(n)$$
$$A_n(s(a)) = s(A_n(a))$$



Suma en sistemas de Peano

Se define la suma en el sistema de Peano (N, s, i) como:

$$+ : N \times N \to N$$

dada por:

$$+ = \left\{ ((n,m),k) \in (N \times N) \times N \;\middle|\; A_n(m) \right\}$$

$$n + m = A_n(m)$$

Proposición

$+$ es asociativa.

Demostración: Demostraremos que $(a+b)+c = a+(b+c)$ por inducción sobre c.

$$(a+b)+i = s(a+b) = a+s(b) = a+(b+i)$$

Suponemos que $(a+b)+c = a+(b+c)$, entonces

$$(a+b)+s(c) = s((a+b)+c) \underset{\text{H.I.}}{=} s(a+(b+c)) = a+s(b+c) = a+(b+s(c)).$$

Proposición

$+$ es conmutativa.

Demostración: Demostraremos que:

$$a+b = b+a \quad \forall a, b \in N$$

Por inducción sobre b
Base de inducción 1: $b = i$ [Por demostrar $a+i = i+a$]
Por inducción sobre a
Base de inducción 2: $a = i$

$$i+i = i+i$$

Paso inductivo 1: Supongamos que $a+i = i+a \quad \forall a \in N$, entonces:

$$i+s(a) = s(i+a) = s(a+i) = a+s(i) = a+(i+i) = (a+i)+i = s(a)+i$$

Paso inductivo 2: Supongamos que $a+b = b+a \quad \forall a \in N$ [Por demostrar $a+s(b) = s(b)+a$], entonces:

$$a+s(b) = s(a+b) \underset{\text{H.I.}}{=} s(b+a) = b+s(a) = b+(a+i) = b+(i+a) = (b+i)+a = s(b)+a$$

Proposición (Ejercicio)

$a + c = b + c \implies a = b \quad \forall a, b \in N$

Demostración: Por inducción sobre c:
Base de inducción: $c = i$ [Por demostrar $a + i = b + i \implies a = b$]

$$a + i = b + i \iff s(a) = s(b)$$

como s es inyectiva, entonces:

$$a = b$$

Paso inductivo: Supongamos que $a + c = b + c \implies a = b$ [Por demostrar: $a + s(c) = b + s(c) \implies a = b$], entonces:

$$a + s(c) = b + s(c) \iff s(a + c) = s(b + c)$$

Como s es inyectiva, entonces:

$$a + c = b + c \underset{\text{H.I.}}{\implies} a = b$$

Producto en sistemas de Peano

Se define el producto en el sistema de Peano (N, s, i) como:

$$\cdot = \begin{cases} a \cdot i = a \\ a \cdot s(b) = a \cdot b + a \end{cases}$$

Proposición (Ejercicio)

$a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in N$

Demostración: Por inducción sobre c:
Base de inducción: $c = i$ [Por demostrar $a \cdot (b + i) = a \cdot b + a \cdot i$]

$$a \cdot (b + i) = a \cdot s(b) = a \cdot b + a = a \cdot b + a \cdot i$$

Paso inductivo: Supongamos que $a \cdot (b+c) = a \cdot b + a \cdot c$ [Por demostrar: $a \cdot (b + s(c)) = a \cdot b + a \cdot s(c)$], entonces:

$$a \cdot (b+s(c)) = a \cdot s(b+c) = a \cdot (b+c) + a \underset{\text{H.I.}}{=} (a \cdot b + a \cdot c) + a = a \cdot b + (a \cdot c + a) = a \cdot b + a \cdot s(c)$$

Proposición (Ejercicio)

$a \cdot (b \cdot c) = (a \cdot b) \cdot c \quad \forall a, b, c \in N$

Demostración: Por inducción sobre c:
Base de inducción: $c = i$ [Por demostrar $a \cdot (b \cdot i) = (a \cdot b) \cdot i$], entonces:

$$a \cdot (b \cdot i) = a \cdot b = (a \cdot b) \cdot i$$

Paso inductivo: Supongamos que $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ [Por demostrar $a \cdot (b \cdot s(c)) = (a \cdot b) \cdot s(c)$], entonces:

$$a{\cdot}(b{\cdot}s(c)) = a{\cdot}(b{\cdot}(c{+}i)) = a{\cdot}(b{\cdot}c{+}b{\cdot}i) = a{\cdot}(b{\cdot}c){+}a{\cdot}(b{\cdot}i) \underset{\text{H.I.}}{=} (a{\cdot}b){\cdot}c{+}(a{\cdot}b){\cdot}i = (a{\cdot}b){\cdot}(c{+}i) = a{\cdot}(b{\cdot}s(c))$$

Proposición (Ejercicio)

$(a + b) \cdot c = a \cdot c + b \cdot c \quad \forall a, b, c \in N$

Demostración: Por inducción sobre c:
Base de Inducción: $c = i$ [Por demostrar $(a + b) \cdot i = a \cdot i + b \cdot i$], entonces:

$$(a + b) \cdot i = a + b = a \cdot i + b \cdot i$$

Paso inductivo: Supongamos que $(a+b) \cdot c = a \cdot c + b \cdot c$ [Por demostrar $(a+b) \cdot s(c) = a \cdot s(c) + b \cdot s(c)$], entonces:

$$(a{+}b){\cdot}s(c) = (a{+}b){\cdot}(c{+}i) = (a{+}b){\cdot}c{+}(a{+}b){\cdot}i = a{\cdot}c{+}b{\cdot}c{+}(a{+}b) \underset{\text{H.I.}}{=} (a{+}b){\cdot}c{+}(a{+}b) = (a{+}b){\cdot}s(c)$$

Proposición (Ejercicio)

$a \cdot b = b \cdot a$

Demostración: Por inducción sobre b:
Base de Inducción 1: $b = i$ [Por demostrar $a \cdot i = i \cdot a$]
Por inducción sobre a
Base de Inducción 2: $a = i$

$$i \cdot i = i = i \cdot i$$

Paso inductivo: Supongamos $a \cdot i = i \cdot a$, [Por demostrar $i \cdot s(a) = s(a) \cdot i$], entonces:

$$i \cdot s(a) = i \cdot (a + i) = i \cdot a + i = s(a) \cdot i$$

Paso inductivo: Supongamos que $a \cdot b = b \cdot a$ [Por demostrar: $a \cdot s(b) = s(b) \cdot a$], entonces:

$$a \cdot s(b) = a \cdot (b + i) = a \cdot b + i \cdot a \underset{\text{H.I.}}{=} b \cdot a + a = (b + i)a = s(b) \cdot a$$

$<$ en sistemas de Peano

Sea (N, s, i) un sistema de Peano. Dados $a, b \in N$ decimos que $a < b$ si

$$\exists c \in N \ (a + c = b)$$

Proposición

La relación $<$ es un orden estricto en N, y además es lineal.

Demostración:

- **Transitividad:** Supongamos que $a < b$ y $b < c$ entonces existen $x, y \in N$ tales que;

$$\begin{matrix} a + x = b \\ b + y = c \end{matrix} \implies (a + x) + y = c \iff a + (x + y) = c \therefore a < c$$

- **Irreflexividad:** Demostraremos por inducción sobre $a \in N$, $a \not< a$
  Base de Inducción: Por demostrar $i \not< i$, es decir, no existe ningún $c \in N$ tal que

$$i + c = i$$

  Supongamos que $i + c = i$ como $i + c = c + i = s(c) \therefore s(c) = i$ lo cual es una contradicción.
  Paso inductivo: Supongamos que $a \not< a$, por demostrar, $s(a) \not< s(a)$.
  Supongamos que $s(a) < s(a)$, esto implica que existe $c \in N$ tal que $s(a) + c = s(a)$. Como

$$s(a) + c = c + s(a) = s(c + a) = s(a + c)$$

  concluimos

$$s(a) = s(a + c)$$

  como s es inyectiva,

$$a + c = a$$

  por lo tanto $a < a$ contradiciendo la hipótesis de inducción que $a \not< a$.
  Por lo tanto $s(a) \not< s(a)$. Por lo que $<$ es irreflexiva.

- **$<$ es lineal:** Demostraremos que $\forall a, b \in N \ (a < b \ \vee \ b < a \ \vee \ a = b)$ por inducción sobre b.
  Base de Inducción: $b = i$. Por un teorema anterior (pagina 21), hay dos casos

$$\begin{cases} a = i & \text{En este caso } a = b. \\ a = s(c), \text{ para algún } c \in N. \end{cases}$$

  En este ultimo

$$a = s(c) = c + i = i + c$$

  Por definición esto implica que $i < a$, y hemos terminado.
  Paso inductivo: Supongamos que

$$\forall a, b \in N \ (a < b \ \vee \ b < a \ \vee \ a = b)$$

tratemos de demostrar para $s(b)$. Por hipótesis de inducción hay tres casos

$$\begin{cases} a = b & \text{Entonces } s(b) = b + i = a + i \therefore a < s(b) \\ a < b & \\ a < b & \end{cases}$$

Si $a < b$ Entonces hay un $c \in N$ tal que $b = a + c$, entonces $s(b) = s(a + c) = (a + c) + i = a + (c + i) = a + s(c) \therefore a < s(b)$.
Si $b < a$. Esto significa que existe $c \in N$ tal que $a = b + c$. Entonces tenemos dos subcasos

$$\begin{cases} c = i & \\ c = s(d) & \text{Para algún } d \in N \end{cases}$$

Si $c = i$ entonces $a = b + c = b + i = s(b)$
Si $c = s(d)$, entonces, $a = b+s(d) = b+(d+i) = b+(i+d) = (b+i)+d = s(b)+d$.
Por lo tanto $s(b) < a$.

Corolario

1. $i = \min(N)$
2. Si $a < b$, entonces,
$$s(b) \leq a.$$

Demostración:

1. Se sigue de la base inductiva de la proposición anterior.
2. Se sigue de la ultima parte de la proposición anterior.

Teorema

$<$ es un buen orden sobre N.

Demostración: Usaremos un resultado previo (pagina 20).
Sea $X \subseteq N$ y supongamos que

$$\forall a \in N \ (\text{seg}(a) \subseteq X \implies a \in X)$$

[Por demostrar $X = N$].
Sea

$$Y = \left\{ a \in N \middle| \ \text{seg}(a) \subseteq X \right\}$$

[Por demostrar $Y = N$] usando inducción.
Base Inductiva: Entonces, $\text{seg}(i) = \varnothing \subseteq X$

$$\therefore i \in Y$$

Paso Inductivo: Supongamos que $a \in Y$, i.e., $\text{seg}(Y)$ (note que esto implica que $a \in X$) [Por demostrar $s(a) \in Y$]

$$\text{seg}(s(a)) = \text{seg}(a) \cup \{a\} \subseteq X$$

$\therefore s(a) \in Y$ por el principio de inducción $Y = N$.
Entonces si $a \in N \implies$ como $s(a) \in Y$ entonces $a \in \text{seg}(s(a)) \subseteq X \therefore X = A \therefore$ Por el resultado previo $<$ es un buen orden.

Teorema

Sean (N, s, i) y (M, t, j) dos sistemas de Peano. Entonces "Son Isomorfos".

$$\begin{aligned}&\exists\, \varphi : N \to M \text{ biyectiva}\\ &\text{tal que } \varphi(i) = i\\ &\varphi(s(a)) = t(\varphi(a)) \quad \forall a \in N.\end{aligned}$$

Demostración:

- **Paso 1:** Encontrar φ, $\exists!\varphi$:

$$\begin{array}{ccc} i \in N & \xrightarrow{s} & N \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ j \in M & \xrightarrow{t} & M \end{array}$$

- **Paso 2:** Encontrar la "inversa" de φ, $\exists!\psi$

$$\begin{array}{ccc} j \in M & \xrightarrow{t} & M \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} \\ i \in N & \xrightarrow{s} & N \end{array}$$

$$\begin{aligned}&\psi(j) = i\\ &\psi(t(x)) = s(\psi(x))\end{aligned}$$

- **Paso 3:** Mostrar que ψ es la inversa de φ

$$\begin{array}{ccccc} i \in N & \xrightarrow{s} & N & & \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} & & \\ j \in M & \xrightarrow{t} & M & & \psi\circ\varphi \\ {\scriptstyle\psi}\downarrow & & \downarrow{\scriptstyle\psi} & & \\ i \in N & \xrightarrow{s} & N & & \end{array}$$

$$\begin{aligned}&\varphi\circ\psi(i) = i\\ &(\varphi\circ\psi)(s(a)) = s(\varphi\circ\psi(a))\\ &f(i) = i\\ &\underbrace{f(s(a)) = s(f(a))}_{\text{tanto } \psi\circ\phi \text{ como } Id_N \text{ satisfacen esto}} \qquad \forall a\\ &\therefore Id_n = f = \varphi\circ\psi\end{aligned}$$

$$\exists! g$$

$$\begin{array}{ccc} j \in M & \xrightarrow{t} & M \\ {\scriptstyle g}\downarrow & & \downarrow{\scriptstyle g} \\ j \in M & \xrightarrow{t} & M \end{array}$$

$$\exists! g \text{ con } \begin{cases} g(j) = j \\ g(t(x)) = t(g(x)) \end{cases}$$

Como $\varphi \circ \psi$ y Id_M también tienen esa propiedad, $\varphi \circ \psi = g = Id_M$

$\therefore \varphi$ es biyectiva $\implies$ φ es isomorfismo.

Axioma de Infinitud

$$(\exists x)(\varnothing \in x \ \wedge \ (\forall y)(y \in x \implies y \cup \{y\} \in x))$$

Informalmente: existe un conjunto infinito.

Otra forma de ver al axioma es:

Conjunto inductivo

$$x \text{ es un conjunto inductivo} = \exists \varnothing \in X \wedge \forall x \in X (x \cup \{x\} \in X)$$

$\mathbb{N}, \omega$

Sea X un conjunto inductivo, definimos

$$\omega = \left\{ x \in X \middle| \ (\forall y)(y \text{ es inductivo} \implies x \in y) \right\}$$

$$= \left\{ x \middle| \ x \text{ pertenece a todo conjunto inductivo.} \right\}$$

y

$$\mathbb{N} = \omega \backslash \{0\}.$$

Función sucesor en $\mathbb{N}$

Recordemos que $1 = \{\varnothing\}$ definimos la función sucesor

$$\begin{aligned} S : \mathbb{N} &\to \mathbb{N} \\ n &\mapsto n \cup \{n\} \end{aligned}$$

Teorema

La terna $(\mathbb{N}, S, 1)$ es un sistema de Peano.

Demostración:

1. $1 \in \mathbb{N}$
2. $S : \mathbb{N} \to \mathbb{N}$

Cumple los primeros dos requisitos para un sistema de Peano.
Para demostrar los requisitos restantes utilizaremos un lema.

Lema

Para todo $x \in \omega$.

$$\bigcup_{y \in x \cup \{x\}} y = x$$

Demostración:

$$A = \left\{ x \in \omega \middle| \bigcup_{y \in x \cup \{x\}} y = x \right\}$$

Note que

$$\bigcup_{y \in \varnothing \cup \{\varnothing\}} y = \bigcup_{y \in \{\varnothing\}} y = \varnothing$$

$\therefore \varnothing \in A$.
Supongamos ahora que $x \in A$, y

$$\bigcup_{y \in (x \cup \{x\}) \cup \{x \cup \{x\}\}} y = \left(\bigcup_{y \in x \cup \{x\}} y \right) \cup (x \cup \{x\}) = x \cup (x \cup \{x\}) = x \cup \{x\} . \therefore x \cup \{x\} \in A$$

$\therefore A$ es un conjunto inductivo $\implies \omega \subseteq A \therefore A = \omega$ de modo que $\forall x \in \omega,\ x \in A$ y $\therefore$

$$\bigcup_{y \in x \cup \{x\}} y = x$$

3. $1 \notin \text{ran}(S)$: De lo contrario existe $n \in \mathbb{N}$ tal que

$$\{\varnothing\} = 1 = S(n) = n \cup \{n\}$$

Por el axioma de extensionalidad

$$n \in n \cup \{n\} = \{\varnothing\}$$

$\therefore n = \varnothing$, i.e. $n = 0$, lo cual es una contradicción.

4. S es una función inyectiva: Supongamos que $x, y \in \mathbb{N}$ son tales que $x \cup \{x\} = S(x) = S(y) = y \cup \{y\}$

$$\therefore x = \bigcup_{\zeta \in x \cup \{x\}} \zeta = \bigcup_{\zeta \in y \cup \{y\}} \zeta = y,$$

Por el lema anterior.
Observación: Si y es cualquier conjunto inductivo, entonces,

$$\omega \subseteq y$$

5. Sea $A \subseteq \mathbb{N}$ tal que

   (a) $1 \in A$

   (b) $\forall a \in A\ (s(a) \in A)$

Note que $X = \{\varnothing\} \cup A \subseteq \omega$ es un conjunto inductivo:

$$\varnothing \in X \text{ Por definición.}$$

Si $x \in X$, entonces, dos casos

$$\begin{cases} x \in \varnothing \implies x \cup \{x\} = 1 \in A \subseteq X \\ x \in A \implies x \cup \{x\} = S(x) \in A \subseteq X \end{cases}$$

$\therefore \omega \subseteq X \implies X = \omega$

$$\therefore A = X \backslash \{\varnothing\} = \omega \backslash \{0\} = \mathbb{N}.$$

Construcción de $\mathbb{Z}$ Existen varias formas de definir $\mathbb{Z}$

$$\underbrace{\mathbb{N} \cup \{\varnothing\} \cup (\mathbb{N} \times \{0\})}$$

Se puede pero es muy complejo.

$\sim$ en $\mathbb{Z}$

En el conjunto $\mathbb{N} \times \mathbb{N}$ definimos la relación binaria $\sim$ estipulando que

$$(a, b) \sim (c, d) \iff a + d = b + c$$

Observación: Piense como $a - b = c - d \implies a + d = b + c$

Proposición

$\sim$ es una relación de equivalencia en $\mathbb{N} \times \mathbb{N}$.

Demostración:

- **Reflexiva:** $[(a, b) \sim (a, b)]$ Como

  $$a + b = b + a$$

  entonces $(a, b) \sim (a, b) \quad \forall (a, b) \in \mathbb{N} \times \mathbb{N}$.

- **Simetría:** Supongamos que $(a, b),\ (c, d) \in \mathbb{N} \times \mathbb{N}$ son tales que $(a, b) \sim (c, d)$. Entonces $a + d = b + c$. Entonces $c + b = d + a \therefore (c, d) \sim (a, b)$

- **Transitiva:** Supongamos que $(a, b) \sim (c, d)$ y $(c, d) \sim (e, f)$. Entonces $a + d = b + c$ y $c + f = d + e$ sumando estas condiciones

  $$a + d + c + f = b + c + d + e$$

  $$\implies (a + f) + (c + d) = (b + e) + (c + d)$$

  Por la cancelatividad de la suma,

  $$a + f = b + e \therefore (a, b) \sim (e, f)$$

$\mathbb{Z}$

Definimos $\mathbb{Z}$ como:

$$\mathbb{Z} = (\mathbb{N} \times \mathbb{N})/\sim$$

Intuitivamente:
$-5 = \{(1,6),(2,7),\dots,\}$
$-7 = \{(1,8),(2,9),\dots\}$

$$3 = \begin{cases} \mathbb{N} : \{\varnothing, \{\varnothing\}, \{\varnothing, \{\varnothing\}\}\} \\ \mathbb{Z} : \{(4,1),(5,2),\dots\} \end{cases}$$

Suma en $\mathbb{Z}$

Definimos $+ : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

$$[(a,b)]_\sim + [(c,d)]_\sim = [(a+c, b+d)]_\sim$$

Intuitivamente: $a - b + c - d = (a + c) - (b + d)$

Demostraremos que $+$ está bien definida [Por demostrar $(a + c, b + d) \sim (a' + c', b' + d')$]

Supongamos que $\begin{matrix}(a,b) \sim (a',b') \\ (c,d) \sim (c',d')\end{matrix}$ Entonces, sumando

$$a+b'+c+d' = b+d+a'+c' \iff (a+c, b+d) \sim (a'+c', b'+d') \implies [(a+c, b+d)]_\sim = [a'+c', b'+d']_\sim$$

Proposición

$+$ es conmutativa

Demostración:

$$[(a,b)]_\sim + [(c,d)]_\sim = [(a+c, b+d)]_\sim = [(c+a, d+b)]_\sim = [(c+d)]_\sim + [(a,b)]_\sim$$

Proposición (Tarea)

$+$ es asociativa

Demostración: Sean $[(a,b)]_\sim, [(c,d)]_\sim, [(e,f)]_\sim \in \mathbb{Z}$ entonces

$$\big([(a,b)]_\sim + [(c,d)]_\sim\big) + [(e,f)]_\sim = [(a+c, b+d)]_\sim + [(e,f)]_\sim$$

$$= \Big[\big((a+c)+e, (b+d)+f\big)\Big]_\sim = \Big[\big(a+(c+e), b+(d+f)\big)\Big]_\sim$$

$$[(a,b)]_\sim + \big([c,d]_\sim + [e,f]_\sim\big)$$

Intuitivamente: $(a - b)(c - d) = ac + bd - bc + ad$

Producto en $\mathbb{Z}$

$$\cdot : \mathbb{Z} \to \mathbb{Z}$$

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd, bc+ad)]_\sim$$

Proposición

1. $$[(1,1)]_\sim = \left\{ (a,a) \middle| \, a \in \mathbb{N} \right\}$$

2. $$[(a,b)]_\sim + [(1,1)]_\sim = [(a,b)]_\sim$$

Demostración:

- Sea $(a,b) \in [(1,1)]_\sim$, entonces $(a,b) \sim (1,1) \implies a+1 = b+1$. Entonces, $a = b \therefore (a,b) = (a,a)$. Recíprocamente, si $a \in \mathbb{N}$ entonces $(a,a) \sim (1,1)$ pues $a+1 = 1+a, \therefore (a,a) \in [(1,1)]_\sim$
- $[(a,b)]_\sim + [(1,1)] = [(a+1, b+1)]_\sim \implies a+b+1 = 1+b+a \implies a+b = a+b \implies [(a,b)]_\sim$

Proposición

Dado $[(a,b)]_\sim$

$$[(b,a)]_\sim + [(a,b)]_\sim = [(a,a)]_\sim$$

Demostración:

$$[(b,a)]_\sim + [(a,b)]_\sim = [(b+a, a+b)]_\sim$$

Por 2.

$$= [(1,1)]_\sim = [(a,a)]_\sim$$

Unicidad

La identidad aditiva es única.

Proposición

$\cdot$ Esta bien definido.

Proposición

Dado $[(a,b)]_\sim$, se tiene que:

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(c,d)]_\sim \cdot [(a,b)]_\sim$$

Demostración:

$$[(a,b)]_\sim \cdot [(c,d)]_\sim = [(ac+bd, ad+bc)]_\sim$$

Reordenando los términos, obtenemos:

$$= [(ca + db, cb + da)]_\sim$$

Por lo tanto, se cumple la propiedad conmutativa:

$$= [(c, d)]_\sim \cdot [(a, b)]_\sim$$

Proposición

Dado $[(a, b)]_\sim$, $[(c, d)]_\sim$ y $[(e, f)]_\sim$, se cumple que:

$$([(a, b)]_\sim \cdot [(c, d)]_\sim) \cdot [(e, f)]_\sim = [(a, b)]_\sim \cdot ([(c, d)]_\sim \cdot [(e, f)]_\sim)$$

Demostración:

$$[(a, b)]_\sim \cdot [(c, d)]_\sim = [(ac + bd, ad + bc)]_\sim$$

Luego:

$$[(ac + bd, ad + bc)]_\sim \cdot [(e, f)]_\sim = [(ac + bd)e + (ad + bc)f, (ac + bd)f + (ad + bc)e]_\sim$$

Expandiendo los términos:

$$= [(ace + bde + acf + bcf, acf + bcf + ade + bde)]_\sim$$

Agrupando términos:

$$= [(ace + adf + bcf + bde, acf + ade + bcf + bde)]_\sim$$

Por otro lado:

$$[(c, d)]_\sim \cdot [(e, f)]_\sim = [(ce + df, cf + de)]_\sim$$

Por lo tanto:

$$[(a, b)]_\sim \cdot [(c, d)]_\sim \cdot [(e, f)]_\sim = [(a, b)]_\sim \cdot [(ce, df), (cf, de)]_\sim$$

$$= [(ace + adf, acf + ade)]_\sim$$

Proposición

1. $$[(2, 1)]_\sim = \left\{ (a + 1, a) \,\middle|\, a \in \mathbb{N} \right\}$$

2. $$[(2, 1)]_\sim \cdot [(a, b)]_\sim = [(a, b)]_\sim$$

Demostración:

1. Sea $(a, b) \in [(2, 1)]_\sim \implies (a, b) \sim (2, 1)$.
   Si $(a, b) \sim (2, 1) \implies 2 \cdot b = 1 \cdot a \implies a = b + 1 \therefore (a, b) = (b + 1, b)$.
   Recíprocamente: Si $b \in \mathbb{N} \implies (b + 1, b) \sim (2, 1)$

$$b + 1 + 1 = b + 2 \iff b + 2 = b + 2 \therefore (b + 1, b) \in [(b + 1, b)]_\sim$$

2. $[(2,1)]_\sim \cdot [(a,b)] = [(2a+b, 2b+a)]$ Por 1. Sea $q \in \mathbb{N}$

$$(1,2) \sim (q+1, q) \implies 2+q = q+1+1$$

Multiplicando por (a,b) ambos lados

$$\ldots (2a+b, 2b+a) \sim (a,b) \implies [(a,b)]_\sim \cdot [(2,1)]_\sim = [(a,b)]_\sim$$

Proposición

Si $m, n \in \mathbb{Z}$ y $mn = 0$, entonces $m = 0$ o $n = 0$

Orden en $\mathbb{Z}$

Dados $[(a,b)]_\sim, [(c,d)]_\sim \in \mathbb{Z}$ definimos el orden parcial $\leq$ en $\mathbb{Z}$ como:

$$[(a,b)]_\sim \leq [(c,d)]_\sim \iff a+d \leq c+b$$

Proposición

$\leq$ está bien definida

Demostración: $\implies$)
$(a,b) \sim (a',b')$ y $(c,d) \sim (c',d')$

$$\implies \begin{matrix} a+b' = b+a' \\ c+d' = d+c' \end{matrix}$$

Si $a+d \leq c+b \implies$

$$(a,b') + (d,c') + a' + d' \leq (c+d') + (b+a') + b' + c'$$

$$\ldots a' + d' \leq c' + b'$$

Análogamente para $\impliedby$)

Proposición

1. $\leq$ es reflexiva
2. $\leq$ es antisimetrica
3. $\leq$ es transitiva
4. $\leq$ es lineal

Demostración:

1. Como:
$$a+b = b+a \implies [(a,b)]_\sim \leq [(a,b)]_\sim$$
2. Si $[(a,b)]_\sim \leq [(c,d)]_\sim$ y $[(c,d)]_\sim \leq [(a,b)]_\sim$

$$\implies \begin{matrix} a+d \leq b+c \\ c+b \leq d+a \end{matrix} \implies a+d = b+c \implies (a,b) \sim (c,d)$$

$\therefore [(a,b)]_\sim = [(c,d)]_\sim$

3. Si $[(a,b)]_\sim \leq [(c,d)]_\sim$ y $[(c,d)]_\sim \leq [(e,f)]_\sim$

$$\implies a+d \leq b+c \text{ y } c+f \leq e+f$$

$$\implies a+d+f \leq b+c+f \text{ y } b+c+f \leq e+d+b$$

$$\therefore a+d+f \leq e+d+b \implies a+f \leq e+b \implies [(a,b)]_\sim \leq [(e,f)]_\sim$$

4. Dados $a,b,c,d, \in \mathbb{N}$

$$\begin{cases} \text{o bien} & a+d \leq c+b \implies [(a,b)]_\sim \leq [(c,d)]_\sim \\ \text{o bien} & c+b \leq a+d \implies [(c,d)]_\sim \leq [(a,b)]_\sim \end{cases}$$

Proposición

$[(a,b)]_\sim \leq [(c,d)]_\sim$ implica

$$[(a,b)]_\sim + [(e,f)]_\sim \leq [(c,d)]_\sim + [(e,f)]_\sim$$

Demostración: Si $[(a,b)]_\sim \leq [(c,d)]_\sim$ entonces $a+d \leq b+c$ Sumando $e+f$

$$\implies a+e+d+f = b+f+c+e$$

$$\implies [(a+e,b+f)]_\sim \leq [(c+e,d+f)]_\sim$$

Por lo tanto

$$[(a,b)]_\sim + [(e,f)]_\sim \leq [(c,d)]_\sim + [(e,f)]_\sim$$

Proposición

Si $[(a,b)]_\sim \leq [(c,d)]_\sim$ y $0 \leq [(e,f)]_\sim$, entonces

$$[(a,b)]_\sim \cdot [(e,f)]_\sim \leq [(c,d)]_\sim \cdot [(e,f)]_\sim$$

Demostración: Si $[(a,b)]_\sim \leq [(c,d)]_\sim$ y $[(1,1)]_\sim < [(e,f)]_\sim$, $\implies \underbrace{a+d \leq b+c}_{*}$ y $1+f < e+1 \implies f < e$, entonces $\exists g$ tal que $e = f+g$. Multiplicando $*$ por g:

$$ag+dg \leq bg+cg\ ;$$

sumando $af+df+cf+df$ por ambos lados,

$$\implies a(g+f)+d(g+f)+bf+cf \leq af+df+b(g+f)+c(g+f)$$

$$\ldots [(ae+bf, af+be)]_\sim \leq [(ce+df, cf+de)]_\sim$$

$$\therefore [(a,b)]_\sim \cdot [(e,f)]_\sim \leq [(c,d)]_\sim \cdot [(e,f)]_\sim$$

Encaje de $\mathbb{N}$ en $\mathbb{Z}$

Un encaje:

$$E : \mathbb{N} \to \mathbb{Z}$$
$$a \longmapsto [(a+1,1)]_\sim$$

1. E es inyectiva
   Sean $a, b \in \mathbb{N}$ tales que $E(a) = E(b)$

$$[(a+1,1)]_\sim = [(b+1,1)]_\sim \implies a+1+1 = b+1+1 \implies a = b$$

2. Para todo $n \in \mathbb{Z}$, se cumple una de las siguientes tres:

$$n = E(a) \quad \text{para algún } a \in \mathbb{N}$$
$$n = 0$$
$$n = -E(a) \quad \text{para algún } a \in \mathbb{N}$$

Si $n = [(a,b)]_\sim$, entonces hay 3 casos:

- $b < a$ Dos subcasos:
  - $b = 1$, Entonces hay un $d \in \mathbb{N}$ tal que $a = d + 1$. Entonces $[(a,b)]_\sim = [(d+1,1)]_\sim = E(d)$
  - $b = c + 1$ para algún c, entonces hay un $d \in \mathbb{N}$ tal que $a = d + 1$; entonces $c + 1 < d + 1 \therefore \exists e \in \mathbb{N}$ tal que $d = c + e$. $\therefore [(a,b)]_\sim = [(d+1, c+1)]_\sim = [(e+1,1)]_\sim = E(e)$
- $a = b \implies n = 0$
- $a < b$. Entonces $[(b,a)]_\sim$ cae en el caso 1. $\therefore \exists c\ [(b,a)]_\sim = E(c) \implies [(a,b)]_\sim = -E(c)$

3. Si $a, b \in \mathbb{N}$, entonces

$$E(a) + E(b) = [(a+1,1)]_\sim + [(b+1,1)]_\sim$$
$$[(a+1+b+1, 1+1)]_\sim = [(a+b+1,1)]_\sim = E(a+b)$$

4. Si $a, b \in \mathbb{N}$, entonces

$$E(a)E(b) = [(a+1,1)]_\sim \cdot [(b+1,1)]_\sim$$
$$= [((a+1)(b+1)+1, a+1+b+1)]_\sim = [(ab+a+b+1+1, a+b+2)]_\sim$$
$$[(ab+1,1)]_\sim = E(ab)$$

5. Si $a, b \in \mathbb{N}$, entonces

$$a \le b \iff E(a) \le E(b)$$
$$E(a) \le E(b) \iff [(a+1,1)]_\sim \le [(b+1,1)]_\sim$$
$$\iff a+1+1 \le 1+b+1 \iff a \le b$$

Construcción de $\mathbb{Q}$

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

Intuición: Tomar parejas ordenadas en $\mathbb{Z}$ y dejar que (m, n) "representa" a $\frac{m}{n}$

$\mathbb{Q}$

En $\mathbb{Z} \times \mathbb{N}$, definimos la siguiente relación:

$$(k, l) \sim (m, n) \iff kn = lm$$

Intuitivamente $\frac{k}{l} = \frac{m}{n} \implies kn = lm$ Es decir:

$$\mathbb{Q} = (\mathbb{Z} \times \mathbb{N})/\sim$$

Proposición

$\sim$ es una relación de equivalencia en $\mathbb{Z} \times \mathbb{N}$

Demostración

- **Reflexiva:** $(m, n) \sim (m, n)$, ya que $mn = nm$
- **Simétrica:** Si $(k, l) \sim (m, n) \implies kn = lm \implies ml = nk$

$$(m, n) \sim (l, k)$$

- **Transitiva:** Si $(k, l) \sim (m, n)$ u $(m, n) \sim (i, j)$, entonces

$$\underset{\text{por } j}{kn = lm} \text{ y } \underset{\text{por } l}{mj = ni}$$

$$knj = lmj \text{ y } lmj = lni \implies knj = lni$$

$$\implies kj = li \therefore (k, l) \sim (i, j)$$

Suma en $\mathbb{Q}$

Definimos $+$ como:

$$[(m, n)]_\sim + [(k, l)]_\sim = [(ml + nk, nl)]_\sim$$

Proposición

$+$ está bien definida.

Demostración: $\begin{matrix}(m, n) \sim (m', n') \\ (k, l) \sim (k', l')\end{matrix}$ Entonces $\begin{matrix}mn' = m'n & (1) \\ kl' = k'l & (2)\end{matrix}$

Multiplicando (1) por ll', $mn'll' = m'nll'$ (3)

Multiplicando (2) por nn', $kl'nn' = k'lnn'$ (4)

Sumando (3) y (4), obtenemos

$$mln'l' + nkn'l' = nlm'l' + nln'k' \iff (ml + nk, nl) \sim (m'l' + n'k', n'k')$$

Proposición

$[(m,n)]_\sim + [(k,l)]_\sim = [(k,l)]_\sim + [(m,n)]_\sim$

Demostración: $[(m,n)]_\sim + [(k,l)]_\sim = [(ml+nk,nl)]_\sim = [(nk+ml,nl)]_\sim = [(kn+ml,nl)]_\sim = [(k,l)]_\sim + [(m,n)]_\sim$

Proposición

$[(m,n)]_\sim + \left([(k,l)]_\sim + [(i,j)]_\sim\right) = \left([(m,n)]_\sim + [(k,l)]_\sim\right) + [(i,j)]_\sim$

Demostración: $= [(m,n)]_\sim + [(kj+li,lj)]_\sim = [(mlj+nkj+nli,nlj)]_\sim = \ldots = \left([(m,n)]_\sim + [(k,l)]_\sim\right) + [(i,j)]_\sim$

Proposición

1. $[(0,1)]_\sim = \left\{(0,n) \middle| \, n \in \mathbb{N}\right\}$
2. $[(0,1)]_\sim + [(k,l)]_\sim = [(k,l)]_\sim$

Demostración:

1. Sea $(a,b) \in [(0,1)]_\sim$ entonces $(a,b) \sim (0,1) \implies a \cdot 1 = b \cdot 0 \implies a = 0$, $(a,b) = (0,b)$
   Ahora, sea $b \in \mathbb{N}$ entonces $(0,b) \sim (0,1)$, $0 \cdot 1 = b \cdot 0$
2. $[(0,1)]_\sim + [(k,l)]_\sim = [(0l+1k,1l)]_\sim = [(k,l)]_\sim$

Proposición

Dado $[(m,n)]_\sim \in \mathbb{Q}$

$$[(m,n)]_\sim + [(-m,n)]_\sim = [(0,1)]_\sim$$

Demostración: $[(m,n)]_\sim + [(-m,n)]_\sim = [(mn-mn,n^2)]_\sim = [(n(m-m),n^2)]_\sim = [(0,n^2)]_\sim$, $(0,n^2) \sim (0,1)$

$\cdot$ en $\mathbb{Q}$

En $\mathbb{Q}$ definimos $\cdot$ como:

$$[(m,n)]_\sim \cdot [(k,l)]_\sim = [(mk,nl)]_\sim$$

Proposición

$\cdot$ está bien definido.

$(m,n) \sim (m',n')$
$(k,l) \sim (k',l')$ Entonces $mn' = m'n$ (1), $kl' = k'l$ (2) Multiplicando (1) y (2), obtenemos:

$$mn'kl' = m'nk'l \implies mkn'l' = nlm'k'$$

$$(mk,nl) \sim (m'k',n'l')$$

Proposición

$[(m,n)]_\sim \cdot [(k,l)]_\sim = [(k,l)]_\sim \cdot [(m,n)]_\sim$

Demostración: $[(m,n)]_\sim \cdot [(k,l)]_\sim = [(mk,nl)]_\sim = [(km,ln)]_\sim = [(k,l)]_\sim \cdot [(m,n)]_\sim$

Proposición

$[(m,n)]_\sim \cdot \Big([(k,l)]_\sim \cdot [(i,j)]_\sim\Big) = \Big([(m,n)]_\sim \cdot [(k,l)]_\sim\Big) \cdot [(i,j)]_\sim$

Demostración: $= [(m,n)]_\sim \cdot [(ki,lj)]_\sim = [(m(ki),n(lj))]_\sim = [((mn)i,(nl)j)]_\sim = \Big([(m,n)]_\sim \cdot [(k,l)]_\sim\Big) \cdot [(i,j)]_\sim$

Proposición

1. $[(1,1)]_\sim = \left\{(m,m) \,\middle|\, m \in \mathbb{N}\right\}$
2. $[(1,1)]_\sim \cdot [(m,n)]_\sim = [(m,n)]_\sim$

Demostración:

1. Sea $(a,b) \in [(1,1)]_\sim$ entonces $(a,b) \sim (1,1) \implies 1 \cdot a = b \cdot 1 \implies a = b$ análogamente para $\Longleftarrow$)
2. $[(1,1)]_\sim \cdot [(m,n)]_\sim = [(1 \cdot m, 1 \cdot n)]_\sim = [(m,n)]_\sim$

Proposición

Dado $[(m,n)]_\sim \in \mathbb{Q}$, con $[(m,n)]_\sim \neq [(0,1)]_\sim$, entonces:

1. Si $m > 0$, entonces
$$[(m,n)]_\sim \cdot [(n,m)]_\sim = [(1,1)]_\sim$$
2. Si $m < 0$, entonces
$$[(m,n)]_\sim \cdot [(-n,-m)]_\sim = [(1,1)]_\sim$$

Demostración:

1. $[(m,n)]_\sim \cdot [(n,m)]_\sim = [(mn,nm)]_\sim = [(1,1)]_\sim$
2. $[(m,n)]_\sim \cdot [(-n,-m)]_\sim = [(-nm,(-m)n)]_\sim = [(1,1)]_\sim$

Proposición

$[(m,n)]_\sim \cdot \Big([(k,l)]_\sim + [(i,j)]_\sim\Big) = [(m,n)]_\sim \cdot [(k,l)]_\sim + [(m,n)]_\sim \cdot [(i,j)]_\sim$

Demostración: $[(m,n)]_\sim \cdot [(kj+li,lj)]_\sim = [(m(kj+li),nlj)]_\sim = [(mkj+mli,nlj)]_\sim = [(m,n)]_\sim \cdot [(k,l)]_\sim + [(m,n)]_\sim \cdot [(i,j)]_\sim$

Orden en $\mathbb{Q}$

$\leq$ en $\mathbb{Q}$

Dados dos $[(n,m)]_\sim,\ [(k,l)]_\sim \in \mathbb{Q}$ diremos que $[(n,m)]_\sim \leq [(k,l)]_\sim$ si y solo si

$$nl \leq mk$$

Proposición

$\leq$ es un orden lineal en $\mathbb{Q}$

Demostración:

- **Reflexividad:** Dado $[(n,m)]_\sim$,

  $$nm = mn,$$

  por lo tanto,

  $$[(n,m)]_\sim \leq [(n,m)]_\sim$$

- **Antisimetria:** Supongamos que $[(n,m)]_\sim \leq [(k,l)]_\sim$ y $[(k,l)]_\sim \leq [(n,m)]_\sim$. Entonces, $nl \leq mk$ y $km \leq ln$. Como el orden en $\mathbb{Z}$ es antisimetrico,

  $$nl = mk$$

  $$\therefore (n,m) \sim (k,l) \implies [(n,m)]_\sim = [(k,l)]_\sim$$

- **Transitividad:** Supongamos que: $[(n,m)]_\sim \leq [(k,l)]_\sim$ y $[(k,l)]_\sim \leq [(i,j)]_\sim$. Entonces $ml \leq nk \ldots (1)$ y $kj \leq li \ldots (2)$.
  Multiplicando (1) por j, $mlj \leq nkj$ y multiplicando (2) por n, $nkj \leq nli$.
  Por la transitividad del orden en $\mathbb{Z}$, $mlj \leq nli$, cancelando l por ambos lados $mj \leq ni$, por lo tanto

  $$[(m,n)]_\sim \leq [(i,j)]_\sim$$

- **Linealidad:** Dados $[(n,m)]_\sim, [(k,l)]_\sim \in \mathbb{Q}$ hay dos casos (por la linealidad del orden en $\mathbb{Z}$).

  1. $nl \leq mk$; esto implica que

     $$[(n,m)]_\sim \leq [(k,l)]_\sim$$

  2. $mk \leq nl$; esto implica que

     $$[(k,l)]_\sim \leq [(n,m)]_\sim$$

Proposición

Si $[(m,n)]_\sim \leq [(k,l)]_\sim$, entonces:

1. $[(m,n)]_\sim + [(i,j)]_\sim \leq [(k,l)]_\sim + [(i,j)]_\sim$ para todo $[(i,j)]_\sim \in \mathbb{Q}$
2. $[(m,n)]_\sim \cdot [(i,j)]_\sim \leq [(k,l)]_\sim \cdot [(i,j)]_\sim$ para todo $[(i,j)]_\sim \in \mathbb{Q}$ tal que $[(i,j)]_\sim \geq [(0,1)]_\sim$

Demostración:

1. Por hipótesis
$$ml \leq nk$$
Multiplicando por j^2, obtenemos:
$$mjlj \leq njkj$$
Ahora, sumando a ambos lados $nilj$, obtenemos
$$mjkj + nilj \leq njkj + njli$$
$$\implies (mj + ni)lj \leq nj(kj + li) \therefore [(mh + ni, nj)]_\sim \leq [(kj + li, lj)]_\sim$$
$$[(m, n)]_\sim + [(i, j)]_\sim \leq [(k, l)]_\sim + [(i, j)]_\sim$$

2. Por hipótesis
$$ml \leq nk \ldots (*) \text{ y } 0 \cdot j \leq 1 \cdot i, \text{ es decir, } 0 \leq i$$
Como $i, j \geq 0$ en $\mathbb{Z}$ multiplicamos ambos lados de $(*)$ por ij para obtener
$$mlij \leq njij$$
$$\implies milj \leq njki \therefore [(mi, nj)]_\sim \leq [(ki, lj)]_\sim$$
$$[(m, n)]_\sim \cdot [(i, j)]_\sim \leq [(k, l)]_\sim \cdot [(i, j)]_\sim$$

Encaje de $\mathbb{Z}$ a $\mathbb{Q}$

El encaje (inmersión):
$$E : \mathbb{Z} \to \mathbb{Q}$$
$$n \longmapsto [(n, 1)]_\sim$$

1. E es inyectiva: Sean $n, m \in \mathbb{Z}$ tales que $E(n) = E(m)$. Entonces
$$[(n, 1)]_\sim = [(m, 1)]_\sim$$
$$\therefore (n, 1) \sim (m, 1) \implies n \cdot 1 = 1 \cdot m$$
$$n = m$$

2. Dados $n, m \in \mathbb{Z}$,
$$E(n) + E(m) = [(n, 1)]_\sim + [(m, 1)]_\sim$$
$$= [(n + m, 1)]_\sim = E(m + n)$$

3. $E(n) \cdot E(m) = [(n, 1)]_\sim \cdot [(m, 1)]_\sim$
$$= [(nm, 1)]_\sim = E(nm)$$

4. Dados $n, m \in \mathbb{Z}$
$E(n) \leq E(m) \iff [(n, 1)]_\sim \leq [(m, 1)]_\sim$
$$\iff n \leq m$$

Divisibilidad en $\mathbb{Z}$

Si $a, b \in \mathbb{Z}$, diremos que a divide a b, denotado $a|b$ si $\exists c \in \mathbb{Z}$ ($\mathbb{b} = \mathbb{ca}$)

Proposición

Sean $a, b, c \in \mathbb{Z}$

1. $a|a$
2. Si $a|b$ y $b|a$, entonces $a = \pm b$
3. Si $a|b$ y $b|c$, entonces $a|c$
4. Si $a|b$ y $b|c$, entonces $a|b + c$
5. Si $a|b$ y $c \in \mathbb{Z}$, entonces $a|bc$

Demostración:

1. $a = 1 \cdot a$, $\therefore a|a$
2. Supongamos que $a|b$ y $b|a$ entonces $\exists c, d \in \mathbb{Z}$ tales que

$$b = ac \quad a = bd$$

   Entonces $a = (ac)d = a(cd)$

$$\implies cd = 1$$

   Por lo tanto o bien $c = d = 1$ o bien $c = d = -1 \implies a = b$ o $a = -b$

3. Supongamos que $a|b$ y $b|c$ entonces existen $d, e \in \mathbb{Z}$ tales que $b = ad$ y $c = be$

$$\implies c = (ad)e = a(de)$$

$$\therefore a|c.$$

4. Supongamos que $a|b$ y $a|c$ entonces $\exists d, e \in \mathbb{Z}$ tales que $b = ad$ y $c = ae$

$$\therefore b + c = ad + ae = a(d + e)$$

$$\therefore a|b + c$$

5. Supongamos que $a|b$ entonces $\exists d \in \mathbb{Z}$ tal que

$$b = ad \implies bc = (ad)c = a(dc)$$

$$\therefore a|bc$$

Proposición

Si $a, b, c \in \mathbb{Z}$ cumplen $a|b$ y $a|c$, entonces

$$a|xb + yc \quad \text{para todos } x, y \in \mathbb{Z}$$

Demostración Se sigue de 4. y 5.
Observación: Sea $a \in \mathbb{Z}$, entonces:

$$\begin{array}{cc} a|a & a = 1 \cdot a \\ -a|a & a = (-1)(-a) \\ 1|a & -1|a \end{array}$$

Número Primo

Un número $p \in \mathbb{Z}$ es primo si $p \neq 1,\ p \neq -1,\ p \neq 0$ y los únicos números enteros que dividen a p son $1, -1, p, -p$.

Teorema

Todo $n \in \mathbb{Z},\ n \neq 0$ se puede escribir como:

$$n = (-1)^{\epsilon} p_1^{\alpha_1}, \ldots, p_k^{\alpha_k}$$

en donde $\epsilon = \{0, 1\}$, $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ y $p_1, \ldots, p_k$ son primos positivos.

Demostración: Basta demostrar para $n \in \mathbb{N}$. La demostración será por inducción:
$n = 1$: Basta tomar $\epsilon = 0$

$$k = 0$$

Supongamos que el teorema es cierto para todo $a < n$.

$$\text{Dos casos: } \begin{cases} n \text{ es primo: } p_1 = n,\ \alpha_1 = 1\ n = n \\ n \text{ no es primo:} \end{cases}$$

Entonces existen $a, b \in \mathbb{Z}$ tales que $n = ab$ con $a \neq 1,\ a \neq n$ y $b \neq 1,\ b \neq n$ y, sin pérdida de generalidad,

$$a, b > 0.$$

Además, debe ser el caso que $a, b < n$. Entonces, por hipótesis inductiva existen $p_1, \ldots, p_k$ primos positivos y $\alpha_1 \ldots \alpha_k \in \mathbb{N}$ tales que

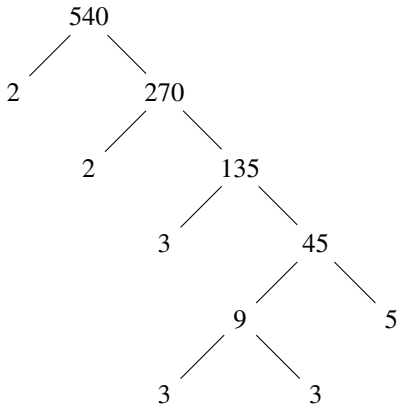
$$a = p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

y $q_1, \ldots, q_l$ primos positivos y $\beta_1 \ldots, \beta_l \in \mathbb{N}$ tales que

$$b = q_1^{\beta_1} \ldots q_l^{\beta_l}$$

$$\implies n = p_1^{\alpha_1} \ldots p_k^{\alpha_k} q_1^{\beta_1} \ldots q_l^{\beta_l}\ .$$

Ejemplo:



Teorema (Algoritmo de la división)

Dados $a, b \in \mathbb{Z}$, con $a > 0$, existen únicos $q, r \in \mathbb{Z}$ tales que

$$b = qa + r$$

con $0 \leq r < a$.

Demostración: Sea

$$A = \left\{ xa + b \,\middle|\, x \in \mathbb{Z} \right\}$$

Note que $A \cap \mathbb{N} \neq \emptyset$, pues $\underset{\text{para } x \text{ suficientemente grande}}{xa + b \in A \cap \mathbb{N}}$ Por el principio del buen orden en $\mathbb{N}$, existen $x \in \mathbb{Z}$ tales que $xa + b \in \min(A \cap \mathbb{N})$. Definimos

$r = xa + b$
$q = -x.$ además $0 \leq r$ por definición . Si tuviéramos $r \geq a$, entonces
$b = -xa + r = q + r$

$$r = xa + b$$

$$0 \leq r - a = x - a + b - a = (x - 1)a + b$$

y $r - a < r$, contradiciendo la minimalidad de $r \therefore r < a$.
Para la unicidad supongamos que $q', r' \in \mathbb{Z}$ tales que

$$b = q'a + r'$$
y $0 \leq r' < a$.

Entonces, sumando ambas condiciones sobre r y $r' \implies -a \leq r - r' < a$ Además $r = b - qa$ y $r' = b - q'a$ sumando ambas $r - r' = (q' - q)a$

$$\implies -a < (q' - q)a < a$$

y esto solo se cumple si $q - q' = 0 \implies q = q' \implies r = r'$.

Máximo común divisor

Sean $a, b \in \mathbb{Z}$, no ambos cero. Un máximo común divisor de a, b es un $d \in \mathbb{Z}$ tal que:

1. $d|a$ y $d|b$
2. Si $e \in \mathbb{Z}$ tal que $e|a$ y $e|b$, entonces

$$e|d$$

Observaciones:

1. Si existe un m.c.d. de a, b, entonces este es único hasta el signo: Si d, d' son m.c.d. de a, b entonces $d|a,\ d|b,\ d'|a,\ d|b' \implies d|d'$ y $d'|d \therefore d = \pm d'$
2. Dados $a, b \in \mathbb{Z}$ denotaremos por (a, b) al (único) m.c.d. positivo de a, ben caso de que exista.

Teorema

Para cualesquiera $a, b \in \mathbb{Z}$, no ambos cero, existe un m.c.d. de a, b.
Además, existen $x, y \in \mathbb{Z}$ tales que

$$(a, b) = xa + yb$$

Demostración: $A = \{xa + yb \mid x, y \in \mathbb{Z}\}$ Note que $A \cap \mathbb{N} \neq \emptyset$. Sean $x, y \in \mathbb{Z}$ tales que

$$d := xa + yb = \min(A \cap \mathbb{N})$$

Afirmamos que d es un m.c.d. de a, b. Por el algoritmo de la división, existen $q, r \in \mathbb{Z}$ tales que $a = qd + r, \quad 0 \leq r < d$. Si $r > 0$, entonces $r = qd - a = q(xa + yb) - a = (qx - 1)a + qyb$, contradiciendo que d es mínimo.

$$\therefore r = 0 \text{ y } a = qd \implies d|a$$

Análogamente, sean $q', r' \in \mathbb{Z}$ tales que

$$b = q'd + r', \quad 0 \leq r' < d$$

Si $r' > 0 \implies r' = b - q'd = b - q'(ax + by) = q'xa + (q'y - q)b$ lo cual es una contradicción

$$\therefore r' = 0 \implies b = q'd \implies d|b$$

Ahora, sea $e \in \mathbb{Z}$ tal que $e|a$ y $e|b \implies e|xa + yb = d$ $\therefore d$ es un m.c.d. de a, b.
Ejemplo: Calcular $(6, 8)$

$$(6, 8) = (6, 2) = (2, 0) = 2$$

Calcular $(69, 6999)$

$$(69, 6999) = (69, 30) = (9, 3) = (3, 0) = 3$$

Proposición

Sean $a, b \in \mathbb{Z}$,y sean q, r tales que $b = qa + r$. Entonces,

$$(a, b) = (a, r)$$

Demostración: Por definición, $(a, b)|a$ y además, $(a, b)|b$, por lo tanto

$$(a, b) \Big| b - qa = r$$

Por lo tanto, $(a, b) \Big| (a, r)$.

Recíprocamente, por definición $(a, r) \Big| a$ y $(a, r) \Big| r$. Por lo tanto $(a, r) \Big| qa + r \implies (a, r) \Big| (a, b)$. Así, $(a, b) \Big| (a, r)$.

Primos relativos o coprimos

Dos enteros $a, b \in \mathbb{Z}$ son primos relativos si

$$(a, b) = 1$$

Ejemplo: 9 y 8, 25 y 81, 35 y 141, etc.

Lema

Dados $a, b \in \mathbb{Z}$, (a, b) es:

1. El valor mas pequeño posible de $ax + by$ que es positivo con $x, y \in \mathbb{Z}$
2. El divisor común de a y b tal que otro divisor común es menor o igual

Demostración:

1. Se demostró en la existencia de (a, b)
2. Si $e|a$ y $e|b$ entonces $e|(a, b) \implies \exists c$ tal que $(a, b) = ec$ si $e < 0 \implies e \leq (a, b)$ en caso contrario, tanto e como c son > 0 y $\therefore e \leq (a, b)$ [De lo contrario, $(a, b) < e$, $1 < e \implies (a, b) < ec$ contradicción].

Observación:

1. Si $a \in \mathbb{Z}$ y $p \in \mathbb{Z}$ es primo, entonces

$$\begin{cases} (a, p) = 1 \\ (a, p) = p \implies p|a \end{cases}$$

Conclusión: O bien $p|a$, o bien a y p son primos relativos

2. Si $a, b \in \mathbb{Z}$, entonces:

$$a \text{ y } b \text{ son primos relativos} \iff \exists x, y \in \mathbb{Z} \text{ tales que } 1 = ax + by$$

Teorema

Sean $a, b, c \in \mathbb{Z}$. Si $a|bc$ y $(a, b) = 1$, entonces $a|c$

Demostración: Sea $d \in \mathbb{Z}$ tal que $bc = da$ además existen $x, y \in \mathbb{Z}$ tales que $1 = xa + yb$ Multiplicando por c, $c = xac + ybc = xac + ydа = (xc + yd)a \therefore a|c$

Corolario

Sean $a, c, p \in \mathbb{Z}$; $n \in \mathbb{N} \cup \{0\}$ tales que

$$a \Big| p^n c. \text{Si } p \nmid a \implies a|c$$

Teorema (Fundamental de la Aritmética)

Si $n \in \mathbb{Z}$ y $n \neq 0$, entonces existen primos positivos $p_1 < \ldots < p_k$ y $\alpha_1, \ldots, \alpha_k \in \mathbb{N}$ tales que

$$n = (-1)^{\epsilon} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

con $\varepsilon \in \{0, 1\}$. Además, esta expresión es única.

Demostración Solo resta demostrar la unicidad. Supongamos que $\epsilon, \delta \in \{0, 1\}$, y $p_1 < \ldots < p_k$ y $q_1 < \ldots < q_r$ y $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_r \in \mathbb{N}$ son tales que:

$$(-1)^{\epsilon} p_1^{\alpha_1} \ldots p_k^{\alpha_k} = (-1)^{\delta} q_1^{\beta_1} \ldots q_k^{\beta_r} = n$$

Si $n > 0 \implies \varepsilon = \delta = 0$ y si $n < 0 \implies \varepsilon = \delta = 1$

$$\therefore p_1^{\alpha_1} \ldots p_k^{\alpha_k} = q_1^{\beta_1} \ldots q_r^{\beta_r}$$

$$= q_1 \left(q_1^{\beta_1 - 1} q_2^{\beta_2} \ldots q_r^{\beta_r} \right) \implies q_1 \Big| p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

Si q_1 fuera distinto de todos los p_i, entonces: $q_1 \nmid p_1$

$$\implies q_1 \Big| p_2^{\alpha_2} \ldots p_k^{\alpha_k}$$

pero $q_1 \nmid p_2$

$$\implies q_1 \Big| p_3^{\alpha_3} \ldots p_k^{\alpha_k}$$

$$\vdots$$

$$q_1 | 1, \text{ contradicción}$$

$\implies$ existe i tal que $q_1 = p_i$

$$\therefore p_1^{\alpha_1} \ldots p_i^{\alpha_i} \ldots p_k^{\alpha_k} = p_i^{\beta_1} q_2^{\beta_2} \ldots q_r^{\beta_r}$$

Si $\alpha_i \neq \beta_1$ tendríamos que

$$p_1^{\alpha_1} \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_k^{\alpha_k} = p_i^{\beta_1 - \alpha_i} q_2^{\beta_2} \ldots q_r^{\beta_r}$$

$$\implies p_i \Big| p_1 \ldots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \ldots p_k^{\alpha_k}$$

Repitiendo el procedimiento anterior,

$$p_i \Big| 1 \text{ contradicción.}$$

$\therefore \alpha_i = \beta_1$

$$\implies p_1^{\alpha_1} \dots p_{i-1}^{\alpha_{i-1}} p_{i+1}^{\alpha_{i+1}} \dots p_k^{\alpha_k} = q_2^{\beta_2} \dots q_r^{\beta_r}$$
$$\vdots$$

Continuando con este proceso, eventualmente concluimos que $r = k$, y

$$\begin{array}{ll} q_1 = p_1 & \alpha_1 = \beta_1 \\ q_2 = p_2 & \alpha_2 = \beta_2 \\ \vdots & \vdots \\ p_k = q_k & \alpha_k = \beta_k \end{array}$$

Proposición

Sea $n = (-1)^{\epsilon} p_1^{\alpha_1} \dots p_k^{\alpha_k}$ y $m = (-1)^{\delta} p_1^{\beta_1} \dots p_k^{\beta_k}$ en donde, $\varepsilon, \delta \in \{0, 1\}$ $p_1 < \dots < p_k$ son primos positivos, y $\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_k \in \mathbb{N} \cup \{0\}$. Entonces,

$$n \Big| m \iff \alpha_1 \leq \beta_1, \alpha_2 \leq \beta_2, \dots, \alpha_k \leq \beta_k$$

Demostración:

$\Longleftarrow$)

$$m = (-1)^{\delta} p_1^{\beta_1} \dots p_k^{\beta_k} = (-1)^{\delta}(-1)^{\epsilon}(-1)^{\overbrace{\underbrace{\left(p^{\beta_1-\alpha_1} \dots p_k^{\beta_k-\alpha_k}\right)}_{n}}^{\in \mathbb{Z}}} \left(p_1^{\alpha_1} \dots p_k^{\alpha_k}\right)$$

$$= (-1)^{\delta}(-1)^{\epsilon} \left(p_1^{\beta_1-\alpha_1} \dots p_k^{\beta_k-\alpha_k}\right) n \implies n|m$$

$\Longrightarrow$)

Si $n|m$, entonces hay algún $l \in \mathbb{Z}$ tal que

$$m = nl. \quad \text{Si } l = (-1)^{\xi} p_1^{\gamma_1} \dots p_k^{\gamma_k},$$

con $\alpha_1, \dots, \alpha_k \in \mathbb{N} \cup \{0\}$

$$\implies (-1)^{\delta} p_1^{\beta_1} \dots p_k^{\beta_k} = m = nl = (-1)^{\epsilon} p_1^{\alpha_1} \dots p_k^{\alpha_k} (-1)^{\xi} p_1^{\gamma_1} \dots p_k^{\gamma_k}$$
$$= (-1)^{\epsilon+\xi} p^{\alpha_1+\gamma_1} \dots p^{\alpha_k+\gamma_k}$$

Por el teorema fundamental de la aritmética,

$$\begin{array}{l} \beta_1 = \alpha_1 + \gamma_1 \\ \beta_2 = \alpha_2 + \gamma_2 \\ \vdots \\ \beta_k = \alpha_k + \gamma_k \end{array}$$

Como $\gamma_1, \gamma_2, \dots, \gamma_k \geq 0$

$$\implies \begin{array}{l} \beta_1 \geq \alpha_1 \\ \vdots \\ \beta_k \geq \alpha_k \end{array}$$

Teorema

Sean $a, b \in \mathbb{Z}$ y $p_1 < \ldots < p_k$ son primos positivos tales que

$$a = (-1)^{\epsilon} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$
$$b = (-1)^{\delta} p_1^{\beta_1} \ldots p_k^{\beta_k}$$

con $\varepsilon, \delta \in \{0, 1\}$ y $\alpha_1, \ldots, \alpha_k, \beta_1 \ldots, \beta_k \in \mathbb{N} \cup \{0\}$. Entonces

$$(a, b) = p_1^{\min\{\alpha_1, \beta_1\}} p_2^{\min\{\alpha_2, \beta_2\}} \ldots p_k^{\min\{\alpha_k, \beta_k\}}$$

Demostración: Sea $(a, b) = p_1^{\gamma_1} \ldots p_k^{\gamma_k}$

Como $\begin{array}{l} (a,b) \Big| a \implies \gamma_1 \leq \alpha_1, \ldots, \gamma_k \leq \alpha_k \\ (a,b) | b \implies \gamma_1 \leq \beta_1, \ldots, \gamma_k \leq \beta_k \end{array}$

$\therefore \gamma_1 \leq \min\{\alpha_1, \beta_1\}, \ldots, \gamma_k \leq \min\{\alpha_k, \beta_k\}$ Además

$$p_1^{\min\{\alpha_1, \beta_1\}} \ldots p_k^{\min\{\alpha_k, \beta_k\}} \Big| a$$

y

$$p_1^{\min\{\alpha_1, \beta_1\}} \ldots p_k^{\min\{\alpha_k, \beta_k\}} \Big| b$$

$$\implies p_1^{\min\{\alpha_1, \beta_1\}} \ldots p_k^{\min\{\alpha_k, \beta_k\}} \Big| (a, b)$$

$\therefore \min\{\alpha_1, \beta_1\} \leq \gamma_1, \ldots, \min\{\alpha_k, \beta_k\} \leq \gamma_k$

$$\therefore \gamma_i = \min\{\alpha_i, \beta_i\}.$$

Mínimo común múltiplo

Si $a, b \in \mathbb{Z}$ no ambos cero, m es un mínimo común múltiplo de a, b si:

1. $a|m$ y $b|m$;
2. Si $n \in \mathbb{Z}$ es tal que $a|n$ y $b|n$, entonces $m|n$

$[a, b]$ es el único m.c.m. positivo de a, b cuando existe.

Proposición

Sean $a, b \in \mathbb{Z}$ no cero

1. Si m es un mínimo común múltiplo de a, b entonces m es único hasta el signo
2. Si $a = (-1)^{\epsilon} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$ y $b = (-1)^{\delta} p_1^{\beta_1} \ldots p_k^{\beta_k}$
   los p_i primos positivos, $\varepsilon, \delta \in \{0, 1\}$ y $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_k \in \mathbb{N} \cup \{0\}$, entonces
   $$[a, b] = p_1^{\max\{\alpha_1, \beta_1\}} \ldots p_k^{\max\{\alpha_k, \beta_k\}}$$
3. $(a, b)[a, b] = ab$

Demostración:

1. Si m, m' son m.c.m's de a, b entonces $a|m$ y $b|m \implies m'|m$
   y $a|m'$, $b|m' \implies m|m' \implies m = \pm m'$

2. Sea $[a,b] = p_1^{\gamma_1}, \ldots, p_k^{\gamma_k}$

   Como $\begin{array}{l} a \Big| [a,b] \implies \alpha_1 \leq \gamma_1, \ldots, \alpha_k \leq \gamma_k \\ b \Big| [a,b] \implies \beta_1 \leq \gamma_1 \ldots, \beta_k \leq \gamma_k \end{array}$

   $\therefore \gamma_1 \geq \max\{\alpha_1, \beta_1\}, \ldots, \gamma_k \geq \max\{\alpha_k, \beta_k\}$ además

   $$a \Big| p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_k^{\max\{\alpha_k,\beta_k\}}$$

   y

   $$b \Big| p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_k^{\max\{\alpha_k,\beta_k\}}$$

   $$\implies [a,b] \Big| p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_k^{\max\{\alpha_k,\beta_k\}}$$

   $\therefore \max\{\alpha_1, \beta_1\} \geq \gamma_1, \ldots, \max\{\alpha_k, \beta_k\} \geq \gamma_k$

   $$\therefore \gamma_i = \max\{\alpha_i, \beta_i\}$$

3. $(a,b)[a,b] = p_1^{\min\{\alpha_1,\beta_1\}} \ldots p_k^{\min\{\alpha_k,\beta_k\}} p_1^{\max\{\alpha_1,\beta_1\}} \ldots p_k^{\max\{\alpha_k,\beta_k\}}$

   $$= p_1^{\alpha_1} \ldots p_k^{\alpha_k} p_1^{\beta_1} \ldots p_k^{\beta_k} = ab$$

Teorema (Euclides)

Hay una infinidad de números primos.

Demostración: Supongamos que no, y que $p_1 < p_2 < \ldots < p_n$ es una lista de todos los números primos positivos. Entonces sea

$$n = 1 + p_1 p_2, \ldots, p_n$$

Nótese que n no es divisible por p_1 ni por $p_2 \ldots p_n$. Por lo tanto, cualquier divisor de p de n es un primo distinto de $p_1, \ldots, p_n$. Así podemos ver que para cualquier n, el número de primos no es exactamente n. Por lo que el número de primos es infinito.

Trabajando en $\mathbb{N}$

Teorema

Sea $n \in \mathbb{N}$, descompongamos;

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, \quad p_i \text{ primos } \alpha_i \in \mathbb{N}$$

Entonces

1. n tiene $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ divisores.
2. $$\sum_{d \mid n} d = \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\right) \dots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

Ejemplo: $6 = 2^1 3^1$ (1,2,3,6 son sus divisores), $12 = 6+3+2+1 = \left(\frac{2^{1+1}-1}{2-1}\right)\left(\frac{3^{1+1}-1}{3-1}\right)$

Demostración:

1. Si $d \mid n$, entonces $\alpha = p_1^{\beta_1} \dots p_k^{\beta_k}$ con $0 \le \beta_i \le \alpha_i$ posibles valores para $(\beta_1, \dots, \beta_k)$ hay $(\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$ posibilidades.
2. $$\sum_{d \mid n} d = \sum_{\substack{0 \le \beta_1 \le \alpha_1 \\ \vdots \\ 0 \le \beta_k \le \alpha_k}} p_1^{\beta_1} \dots p_k^{\beta_k} = \left(\sum_{\beta_1=0}^{\alpha_1} p_1^{\beta_1}\right)\left(\sum_{\beta_2=0}^{\alpha_2} p_2^{\beta_2}\right) \dots \left(\sum_{\beta_k=0}^{\alpha_k} p_k^{\beta_k}\right)$$
$$= \left(\frac{p_1^{\alpha_1+1} - 1}{p_1 - 1}\right)\left(\frac{p_2^{\alpha_2+1} - 1}{p_2 - 1}\right) \dots \left(\frac{p_k^{\alpha_k+1} - 1}{p_k - 1}\right)$$

$$\prod_{p \text{ primo}} \left(\sum_{k=0}^{\infty} \frac{1}{p^k}\right) = \sum_{n=1}^{\infty} \frac{1}{n}$$

Número perfecto

Un número $n \in \mathbb{N}$ es perfecto si

$$\sum_{d \mid n} d = 2n$$

Ejemplos: 6 y 28 son números perfectos

Observación: Supongamos que $\overbrace{2^{m+1} - 1}^{\text{Primos de Mersenne}}$ es un número primo. Entonces, $2^m(2^{m+1} - 1)$ es perfecto.

Demostración: Sea $n = 2^m(2^{m+1}-1)$

$$\sum_{d\mid n} d = (2^{m+1}-1)\left(\frac{(2^{m+1}-1)^2-1}{2^{m+1}-1-1}\right) = (2^{m+1}-1)\left(\frac{(2^{m+1}-1+1)(2^{m+1}-1-1)}{2^{m+1}-1-1}\right)$$

$$\implies (2^{m+1}-1)2^{m+1} = 2^{m+1}(2^{m+1}-1)$$
$$= 2(2^m(2^{m+1}-1)) = 2n$$

Existe un teorema de Euler que dice: Si n es perfecto y par, entonces $n = 2^m(2^{m+1}-1)$ para alguna m tal que $2^{m+1}-1$ es primo.

Número multiplicativamente perfecto

Un número $n \in \mathbb{N}$ es multiplicativamente perfecto si

$$\prod_{d\mid n} d = n^2$$

Observación: Si n es multiplicativamente perfecto, entonces n no es primo ni el cuadrado de un primo.
Demostración: Sea p primo

$$\prod_{d\mid p} d = 1\cdot p = p \neq p^2 \qquad \Big| \qquad \prod_{d\mid p^2} d = 1\cdot p\cdot p^2 = p^3 \neq p^2$$

Observación: Supongamos que n es multiplicativamente perfecto, y sea d un divisor propio de n. Sea e tal que $n = de$. Entonces,

$$n^2 = \prod_{d\mid n} d = 1n\cdot d\cdot e \text{ (producto de los demás divisores)}$$

$$= n^2 \text{ (producto de los demás divisores)}$$

En conclusión, ya no hay más divisores.
En conclusión, si n es multiplicativamente perfecto, n debe tener máximo dos primos que lo dividen.
Exactamente dos primos p, q

$$n = p^\alpha q^\beta$$

y $(\alpha+1)(\beta+1) = 4$

$$\therefore \begin{array}{l} \alpha = 0,\ \beta = 3 \\ \alpha = 1,\ \beta = 1 \\ \alpha = 3,\ \beta = 0 \end{array}$$

Solo hay dos opciones:

$$n = pq \quad \text{con } p, q \text{ primos distintos}$$
$$\prod_{d\mid n} d = 1\cdot p\cdot q\cdot n = n^2$$

$$n = p^3 \quad \text{con } p \text{ número primo}$$
$$\prod_{d\mid n} n = 1\cdot p\cdot p^2\cdot p^3 = n\cdot n = n^2$$

Libre de cuadrados

Un número $n \in \mathbb{N}$ es libre de cuadrados si

$$\forall a \neq 1, \quad a^2 \nmid n$$

Equivalentemente, si p es primo

$$\implies p^2 \nmid n.$$

Equivalentemente, si:

$$n = p^{\alpha_1} \dots p_k^{\alpha_k}$$

entonces $\alpha_i \leq 1$, es decir,

$$n = p_1 \dots, p_k \quad \text{para } p_1, \dots, p_k \text{ primos.}$$

Observación: Sea $n \in \mathbb{N}$

$$\begin{aligned} n &= p_1^{\alpha_1} \dots p_k^{\alpha_k} \\ &= p_1^{2\beta_1 + r_1} p_2^{2\beta_2 + r_2} \dots p_k^{2\beta_k + r_k}; \; r_i \in \{0, 1\} \\ &= \left(p_1^{2\beta_1} p_2^{2\beta_2} \dots p_k^{2\beta_k}\right) \left(p_1^{r_1} \dots p_k^{r_k}\right) \\ &= \underbrace{\left(p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k}\right)^2}_{\text{Cuadrado}} \underbrace{\left(p_1^{r_1} \dots p_k^{r_k}\right)}_{\text{libre de cuadrados}} \end{aligned}$$

En conclusión: para todo $n \in \mathbb{N}$, $\exists a, b \in \mathbb{N}$ tales que

$$n = a^2 b$$

con b libre de cuadrados.
Ejemplo: $24 = 2^3 3 = 2^2(2 \cdot 3) = 4 \cdot 6$

Función μ de Möbius

La función μ de Möbius se define como sigue:

$$\mu(n) \begin{cases} 0 & \text{si } n \text{ no es libre de cuadrados} \\ (-1)^l & \text{si } n = p_1 \dots p_l \text{ con } p_1, \dots, p_l \text{ primos} \end{cases}$$

Ejemplos:

$$\begin{aligned} &\mu(24) = 0 \\ &\mu(6) = 1 \\ &\mu(70) = -1 \\ &\mu(1) = 1 \\ &\mu(p) = -1 \text{ si } p \text{ es primo.} \end{aligned}$$

Proposición

Si $n > 1$, entonces

$$\sum_{d|n} \mu(n) = 0$$

Demostración: Sea $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ con $p_1, \dots, p_k$ primos distintos y $\alpha_1, \dots, \alpha_k \in \mathbb{N}$

$$\sum_{d|n} \mu(d) = \sum_{0 \le \beta_i \le \alpha_i} \mu\left(p_1^{\beta_1} \dots p_k^{\beta_k}\right)$$

Si cualquier $\beta_1 \ge 2$

$$= \sum_{0 \le \beta_i \le 1} \mu\left(p_1^{\beta_1} \dots p_k^{\beta_k}\right)$$

$$= \mu(1) + \sum \mu(p_i) + \sum \mu(p_i p_j) + \sum \mu(p_i p_j p_k) + \dots \mu(p_1 \dots p_k)$$

$$= 1 - k + \binom{k}{2} - \binom{k}{3} + \binom{k}{4}$$

$$(-1)^{k-1}\binom{k}{k-1} + (-1)^k$$

$$= (1-1)^k = 0$$

Función ϕ de Euler

La función ϕ de Euler $\phi : \mathbb{N} \to \mathbb{N}$, se define como

$$\phi(n) = \left|\left\{a \in \mathbb{N} \mid a \le n \text{ y } (a, n) = 1\right\}\right|$$

Ejemplos:

$\phi(1) = 1$ $\phi(10) = 4$ $\phi(21) = 12$
$\phi(2) = 1$ $\phi(24) = 8$
$\phi(3) = 2$
$\phi(4) = 2$

Teorema

Si $n \in \mathbb{N}$, entonces

$$\sum_{d|n} \phi(d) = n$$

Ejemplo: 24 divisores=1, 2, 3, 4, 6, 8, 12,24

$\phi(1) = 1$
$\phi(2) = 1$
$\phi(3) = 2$
$\phi(4) = 2$
$\phi(6) = 2$
$\phi(8) = 4$
$\phi(12) = 4$
$\phi(24) = 8$

Demostración: Considere las fracciones

$$\frac{1}{n}, \frac{2}{n}, \frac{3}{n}, \frac{4}{n}, \frac{5}{n}, \dots \frac{n-1}{n}, \frac{n}{n} \quad \dots (*)$$

Simplificando las fracciones obtenemos todas las posibles fracciones de la forma $\frac{a}{d}$ con $d|n$ y $(a,d) = 1$ y $a \leq d$, recíprocamente, para cualquier fracción de la forma $\frac{a}{d}$ con $d|n, (a,d) = 1$ y $a \leq d$ en función es igual a $\frac{ae}{n}$ con $ae \leq n$ donde $n = de$ y por lo tanto, una fracción aparece en la lista $(*)$, por lo tanto

$$\left\{ \frac{1}{n}, \frac{2}{n}, \dots \frac{n}{n} \right\} = \dot{\bigcup_{d|n}} \left\{ \frac{a}{d} \;\middle|\; a \in \mathbb{N}, a \leq d, (a,d) = 1 \right\}$$

$\therefore$

$$n = \left| \left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n} \right\} \right| = \sum_{d|n} \left| \left\{ \frac{a}{d} \;\middle|\; a \in \mathbb{N}, a \leq d, (a,d) = 1 \right\} \right| = \sum_{d|n} \left| \left\{ a \in \mathbb{N} \;\middle|\; a \leq d, (a,d) = 1 \right\} \right| = \sum_{d|n} \phi(d).$$

Para $n = 10$:

$$\frac{1}{10}, \frac{2}{10}, \frac{3}{10}, \frac{4}{10}, \frac{5}{10}, \frac{6}{10}, \frac{7}{10}, \frac{8}{10}, \frac{9}{10}, \frac{10}{10}$$

$$\frac{1}{10}, \frac{1}{5}, \frac{3}{10}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{7}{10}, \frac{4}{5}, \frac{9}{10}, \frac{1}{1}$$

$$\phi(1) = 1$$
$$\phi(2) = 1$$
$$\phi(5) = 4$$
$$\phi(10) = 4$$

Observación: Sea p número primo

1. $\phi(p) = p - 1$
2. $\phi(p^n) = p^n \cdot p^{n-1} = (p-1)p^{n-1}$

Si $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$

$$\phi(n) = \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2}) \dots \phi(p_k^{\alpha_k})$$

Congruencias

Existen soluciones enteras de la ecuación

$$x^2 - 31x = 43$$

Si hubiera soluciones $x \in \mathbb{Z}$, entonces:

+	Par	Impar
Par	Par	Impar
Impar	Impar	Par

Si x es par: $\underbrace{x^2}_{\text{par}} - \underbrace{31x}_{\text{par}} = \underset{\text{impar}}{43}$

$\cdot$	Par	Impar
Par	Par	Impar
Impar	Impar	Par

Congruencia módulo m

Sea $m > 1$. Decimos que $a, b \in \mathbb{Z}$ son congruentes módulo m, simbolizado

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

Si

$$m \Big| b - a$$

Proposición

La relación "Ser congruencia módulo m" es de equivalencia

Demostración:

Reflexividad: Como $0 = m \cdot 0$

$$m \Big| 0 = a - a \implies a \equiv a \bmod m$$

Simetría: Si $a \equiv b \bmod m$, entonces $m \Big| b - a$

$$\implies m \Big| -(b-a) = a - b \therefore b \equiv a \bmod m$$

Transitiva: Si $a \equiv b \bmod m$ y $b \equiv c \bmod m$, entonces

$$m \Big| b - a \ \wedge \ m | c - b$$

$$\therefore m \Big| (b-a) + (c-b) = c - a \implies a \equiv c \bmod m$$

Normalmente, el conjunto $\mathbb{Z}/\equiv (\mathrm{mod} m)$ se le denota como

$$\mathbb{Z}/m\mathbb{Z} = \left\{ [a]_{\equiv_m} \Big| \ a \in \mathbb{Z} \right\}.$$

Observación: Dados $a, b \in \mathbb{Z}$ y $m \geq 2$, sean q_1, q_2, r_2, r_1 tales que

$$\begin{aligned} a &= q_1 m + r_1 \quad 0 \leq r_1 < m \\ b &= q_2 m + r_2 \quad 0 \leq r_2 < m. \end{aligned}$$

Entonces

$$a \equiv b \bmod m \iff r_1 = r_2$$

Demostración:

$\Longleftarrow$) $r = r_1 = r_2$

$b - a = (q_2 - q_1)m \implies m \Big| b - a$

$$\therefore a \equiv b \bmod m$$

$\Longrightarrow$) Supongamos que $a \equiv b \bmod m$, es decir $m \Big| b - a = q_2 m + r_2 - (q_1 m + r_1)$

$$= (q_2 - q_1)m + (r_2 - r_1)$$

Así $\exists \alpha \in \mathbb{Z}$ tal que

$$(q_2 - q_1)m + (r_2 - r_1) = m\alpha$$

$$\Longrightarrow \; r_2 - r_1 = m\alpha - (q_2 - q_1)m \; \therefore m \Big| r_2 - r_1$$

Además, $0 \leq r_1 < m \; 0 \leq r_2 < m \Longrightarrow \; -m < -r_1 \leq 0 \; \Longrightarrow \; -m < r_2 - r_1 < m$ la única posibilidad es que

$$r_1 - r_2 = 0$$

es decir $r_1 = r_2$

$$\mathbb{Z}/m\mathbb{Z} = \left\{ [0]_{\equiv_m}, [1]_{\equiv_m}, \ldots, [m-1]_{\equiv_m} \right\}$$

Ejemplos:

$$\mathbb{Z}/2\mathbb{Z} = \{[0]_{\equiv_2}, [1]_{\equiv_2}\} = \{\text{Pares, Impares}\}$$

$$\mathbb{Z}/3\mathbb{Z} = \{[0]_{\equiv_3}, [1]_{\equiv_3}, [2]_{\equiv_3}\}$$

$\left|\mathbb{Z}/m\mathbb{Z}\right| = m$

Teorema

Sean $m \geq 2$ y $a, b, c \in \mathbb{Z}$, entonces, si $a \equiv (b \bmod m)$,

1. $a + c \equiv b + c (\text{mod} m)$
2. $ac \equiv bc (\text{mod} m)$

Demostración: Por hipótesis $a \equiv b (\text{mod} m)$ es decir $m \Big| b - a$

1. $m \Big| b - a + c - c = (b + c) - (a + c)$

$$\therefore a + c \equiv b + c (\text{mod} m)$$

2. $m \Big| (b - a)c = bc - ac$

$$\therefore ac \equiv bc (\text{mod} m)$$

Ejemplos:
Las ecuaciones:

1. $3x^2 + 2 = y^2$
2. $7x^3 + 2 = y^3$

Carecen de soluciones enteras.
Demostración:

1. Si hubieran $x, y \in \mathbb{Z}$ tales que $3x^2 + 2 = y^2$, entonces

$$3x^2 + 2 \equiv y^2 (\text{mod} 3)$$
$$2 \equiv y^2 (\text{mod} 3)$$

$y \equiv 0, 1, 2 (\text{mod} 3) \; \Longrightarrow \; y^2 \equiv 0, 1, 1 (\text{mod} 3)$ contradicción.

2. Supongamos que $x, y \in \mathbb{Z}$ tales que $7x^3 + 2 = y^3$,entonces

$$7x^3 + 2 \equiv y^3 (\text{mod} 7)$$
$$2 \equiv y^3 (\text{mod} 7)$$

$y \equiv 0, 1, 2, 3, 4, 5, 6 (\text{mod} 7) \implies y^3 \equiv 0, 1, 1, 6, 1, 6 (\text{mod} 7)$ Lo cual es una contradicción

---

Congruencias Lineales

$5x + 48 \equiv 2x + 5 (\text{mod} 7)$
$3x \equiv -43 (\text{mod} 7)$
$5 \cdot 3x \equiv (5)(-43) (\text{mod} 7) \implies x \equiv (5)(-1) (\text{mod} 7) \implies x \equiv 2 (\text{mod} 7)$
$5x - 48 \equiv 2x + 47 (\text{mod} 6)$
$3x \equiv 1 (\text{mod} 6)$
$x \equiv 0, 1, 2, 3, 4, 5, 6 (\text{mod} 6)$
$3x \equiv 0, 3, 0, 3, 0, 3 (\text{mod} 6)$

No hay solución

Teorema

Sean $m \geq 2$, $a, b \in \mathbb{Z}$. Si $(a, m) = 1$, entonces la congruencia $ax \equiv b (\text{mod} m)$ tiene solución, y esta es única hasta congruencia módulo m.

Demostración: Por hipótesis, $(a, m) = 1$, entonces, existen $s, t \in \mathbb{Z}$, tales que, $as + tm = 1$, por lo tanto

$$as + tm \equiv 1 (\text{mod} m)$$
$$as \equiv 1 (\text{mod} m)$$

por lo tanto,

$$ax \equiv b (\text{mod} m)$$
$$\iff sax \equiv sb (\text{mod} m)$$
$$\iff x \equiv sb (\text{mod} m)$$

Esta demostración nos da una forma de encontrar el "inverso multiplicativo" para despejar x, pero aún necesitamos una técnica para escribir $(a, m) = sa + tm$.
$(5, 27)$ del algoritmo de la división

$$\begin{array}{c|c|c} 27 = 5 \cdot 5 + 2 & 5 = 2 \cdot 2 + 1 & 2 = 1 \cdot 2 + 0 \\ \implies 2 = 27 - 5 \cdot 5 & 1 = 5 + (-2) \cdot 2 & \end{array}$$

$$1 = 5 + (-2) \cdot 2 \implies 1 = 5 + (-2)(27 - 5 \cdot 5) = (11)(5) + (-2)(27)$$

Ejemplo: Resolver la congruencia $4x \equiv 5 (\text{mod} 9)$
Notemos que $(4, 9) = 1$ además

$$1 = 5 - 4(1) \quad 5 = 9 - (4)(1) \implies 1 = 9 + (4)(-2)$$

por lo que el inverso multiplicativo será -2 multiplicando ambos lados de la congruencia:

$$4(-2)x \equiv (-2)(5) (\text{mod} 9)$$
$$x \equiv -10 (\text{mod} 9)$$
$$\boxed{x \equiv 8 (\text{mod} 9)}$$

Ejercicios: Resolver las congruencias

1. $2x \equiv 7(\text{mod}17)$
2. $7x \equiv 10(\text{mod}26)$
3. $13x \equiv -4(\text{mod}2436)$
4. $19x \equiv 130(\text{mod}141)$
5. $6x \equiv 9(\text{mod}25)$

Solución:

1. Nótese que $(2, 17) = 1$

$$1 = 17 + (2)(-8)$$

por lo que el inverso multiplicativo será -8, multiplicando a la congruencia

$$\begin{aligned}(-8)2x &\equiv (-8)(7)(\text{mod}17)\\ x &\equiv -56(\text{mod}17)\\ \boxed{x &\equiv 12(\text{mod}17)}\end{aligned}$$

2. Notemos que $(7, 26) = 1$ haciendo un procedimiento similar obtenemos

$$1 = 26(3) + 7(-11)$$

por lo que el inverso multiplicativo sera -11,

$$\begin{aligned}(-11)7x &\equiv (-11)10(\text{mod}26)\\ x &\equiv -110(\text{mod}26)\\ \boxed{x &\equiv 20(\text{mod}26)}\end{aligned}$$

3. $(13, 2436) = 1$ además

$$1 = 13(937) + (-5)(2436)$$

multiplicando a la congruencia por 937,

$$\begin{aligned}13(937)x &\equiv -4(937)(\text{mod}2436)\\ x &\equiv -3748(\text{mod}2436)\\ \boxed{x &\equiv 1124(\text{mod}2436)}\end{aligned}$$

4. $(19, 141) = 1$ además

$$1 = 52(19) - 7(141)$$

multiplicando por 52

$$\begin{aligned}(52)19x &\equiv 52(130)(\text{mod}141)\\ x &\equiv 6760(\text{mod}141)\\ \boxed{x &\equiv 133(\text{mod}141)}\end{aligned}$$

5. $(25, 6)$ además

$$1 = 25 + (6)(-4)$$

multiplicamos por -4 la congruencia

$$\begin{aligned}(-4)6x &\equiv (-4)9(\text{mod}25)\\ x &\equiv -36(\text{mod}25)\\ \boxed{x &\equiv 14(\text{mod}25)}\end{aligned}$$

Este método es efectivo para saber que la solución es única tan solo sabiendo si $(a, m) = 1$ pero ahora consideremos

- $12x \equiv 8(\text{mod}20)$, si

  $$x \equiv 4(\text{mod}20), \text{ entonces } x \text{ es solución igual que;}$$
  $$x \equiv 9(\text{mod}20)$$
  $$x \equiv 14(\text{mod}20)$$
  $$x \equiv 19(\text{mod}20)$$

  es decir múltiples soluciones.
  Otro caso sera la siguiente congruencia

- $12x \equiv 5(\text{mod}20)$, podemos realizar este análisis

x	12x
0	12
1	12
2	4
3	16

  y podemos seguir pero notaremos que para que se cumpla la congruencia debemos de tener que el numero termine en 5 lo cual nunca pasara, por lo que la congruencia no tiene solución.

Teorema

Sean $a, b \in \mathbb{Z}$ y $m \geq 2$. Entonces, la congruencia $ax \equiv b(\text{mod}m)$ tiene solución $\iff (a, m) \Big| b$. En el caso donde sí tiene solución, habrá (a, m) soluciones distintas hasta congruencia módulo m.

Demostración: $\implies$)
Supongamos que $x \in \mathbb{Z}$ es tal que $ax \equiv b(\text{mod}m)$.

$$\implies m \Big| b - a. \text{ Como } (a, b) \Big| m, \text{ entonces } (a, m) \Big| b - a$$

Además, $(a, m) \Big| a$

$$\therefore (a, m) \Big| (b - a) + a = b$$

$\impliedby$) Por hipótesis, existe $k \in \mathbb{Z}$ tal que $b = (a, m)k$ además existen $s, t \in \mathbb{Z}$ tales que $(a, m) = sa + tm$ por lo tanto $(a, m) \equiv sa(\text{mod}m)$ multiplicando por k

$$(a, m)k \equiv sak(\text{mod}m)$$
$$b \equiv a(sk)(\text{mod}m)$$

$\therefore$ el entero sk es una solución de la congruencia.
Ahora, en el caso donde x_0 es solución, es decir $ax_0 \equiv b(\text{mod}m)$.
Sea $d \in \mathbb{Z}$ tal que $m = (a, m)d$ y sea $e \in \mathbb{Z}$ tal que $a = (a, m)e$, entonces $da = d(a, m)e = me$. Entonces, para cualquier $l \in \mathbb{Z}$, afirmamos que $x_0 + ld$ también es solución:

$$a(x_0 + ld) \equiv ax_0 + ald$$
$$\equiv b + ald(\text{mod}m)$$
$$\equiv b + mel(\text{mod}m)$$

Recíprocamente, sea x_1 cualquier otra solución de la congruencia. Entonces

$$\begin{aligned}
&ax_0 \equiv b(\mathrm{mod}m)\\
&ax_1 \equiv b(\mathrm{mod}m)\\
&a(x_0 - x_1) \equiv 0(\mathrm{mod}m)\\
&m\Big|a(x_0 - x_1)\\
&\implies (a,m)d\Big|(a,m)e(x_0 - x_1)\\
&\therefore d\Big|e(x_0 - x_1)
\end{aligned}$$

Note además, que $(e,d) = 1 \therefore d\Big|x_0 - x_1$, es decir

$$x_0 - x_1 = ld \text{ para algún } l$$

$$\implies x_1 = x_0 - ld$$

Por lo tanto, las soluciones a la congruencia son;

$$x_0, x_0 + d, x_0 + 2d, x_0 + 3d, \ldots, x_0 + ((a,m) - 1)d, \quad \underbrace{x_0 + (a,m)d}_{\text{es la misma que} x_0(\ \mathrm{mod}\ m)}$$

$\therefore$ hay (a,m) soluciones distintas.
Ejercicios: Resuelva las siguientes congruencias

1. $10x \equiv 7(\mathrm{mod}15)$
2. $10x \equiv 5(\mathrm{mod}15)$
3. $6x \equiv 8(\mathrm{mod}30)$
4. $6x \equiv 24(\mathrm{mod}30)$

Solución:

1. Por el teorema anterior $(10,15) = 5$ y $5 \nmid 7$ por lo que no tiene solución.
2. Sabemos que $(15,10) = 5\Big|5$ por lo que tiene solución, en total 5 soluciones distintas, haremos un paso similar a los problemas anteriores

   $$5 = 15 + (-1)(10) \implies 5 \equiv (-1)(10)(\mathrm{mod}m)$$

   Multiplicando a ambos lados por $\frac{1}{(10,15)}$, obtenemos

   $$x_0 \equiv -1(\mathrm{mod}15)$$

   o

   $$x_0 \equiv 14(\mathrm{mod}15)$$

   ahora para encontrar las otras soluciones tenemos que sumar del lado derecho de la congruencia $\frac{m}{(a,m)} = 3$ así las soluciones son

   $$x_{1,2,3,4,5} = 14, 2, 5, 8, 11(\mathrm{mod}15)$$

3. Nótese que $(30,6) = 6 \nmid 8 \therefore$ no hay solución

4. Notemos que $(30, 6) = 6 \big| 24$ por lo que la congruencia tiene solución, en total 6 soluciones, expresemos al m.c.d. como combinación lineal de 30 y 6;

$$6 = 30(\ ) + 6(\ )$$

es claro que los números faltantes serán $1, -4$ es decir

$$6 = 30(1) + 6(-4)$$

ahora de esta ecuación la expresaremos módulo 30 podemos escribir la congruencia de la siguiente forma

$$6(-4) \equiv 6(\text{mod}30)$$

nótese que el 30(1) desapareció; esto es por que cuando estamos trabajando en módulo 30 el residuo sera 0 por lo que prescindimos de el, ahora necesitamos que de alguna forma aparezca el 24 de lado derecho (pues la congruencia original lo pide), esto se lograra si multiplicamos por 4 ambos lados de la congruencia

$$\begin{aligned} &6(-4)(4) \equiv 6(4)(\text{mod}30) \\ \iff\ &6(-16) \equiv 24(\text{mod}30) \end{aligned}$$

por lo que -16 sera la primera solución, esta solución módulo 30 es $x_0 = 14$. Finalmente tenemos que encontrar el termino a sumar x_0 este es $\frac{30}{(6,30)} = 5$por lo que

$$x_{1,2,3,4,5,6} = 14, 19, 24, 29, 4, 9(\text{mod}30)$$

Ejercicios: Resuelva las siguientes congruencias

1. $8x \equiv 6(\text{mod}14)$
2. $72x \equiv 47(\text{mod}200)$
3. $4183x \equiv 5781(\text{mod}15087)$
4. $66x \equiv 100(\text{mod}121)$
5. $21x \equiv 14(\text{mod}91)$

Solución:

1. Nótese que $(8, 14) = 2 \big| 6$ por lo tanto, tiene solución (2 soluciones). Ahora la combinación lineal:

$$2 = 8(\ ) + 14(\ ) \implies 8(2) + 14(-1)$$

aplicamos módulo 14

$$8(2) \equiv 2(\text{mod}14) \implies 8(2)(3) \equiv 6(\text{mod}14) \implies 8(6) \equiv 6(\text{mod}14)$$

por lo que, 6 es solución de la congruencia, ahora $\frac{14}{(14,8)} = 7$ i.e.

$$x_{1,2} \equiv 6, 13(\text{mod}14)$$

2. Calculamos $(72, 200) = 8 \nmid 47$ por lo que no hay solución. Otra forma de ver que no existe solución es mediante su descomposición en potencia de primos $72 = 2^3 \cdot 3^2$ y $200 = 2^3 \cdot 5^2$

3. $(15087, 41) = 47 \mid 5781$ $(5781 = 47(123))$ hay solución en particular 47 soluciones. Solo exhibiremos una, pues las demás se obtendrán sumando $\frac{m}{(a,m)} = 321$ a la solución; Después de aplicar el algoritmo de Euclides múltiples veces obtenemos

$$47 = 15087(-28) + 4183(101)$$

aplicando módulo 15087

$$4183(101) \equiv 47 (\mathrm{mod} 15087) \implies 4183(101)(123) \equiv 5081 (\mathrm{mod} 15087)$$

Por lo que $(101)(123) = 12423 = x_0$ es nuestra solución y las demás se obtendrán sumando 321

4. $(121, 66) = 11 \nmid 100$ por lo que no tiene solución.

5. $(21, 91) = 7 \mid 14$por lo que tiene 7 soluciones

$$7 = 91(1) + 21(-4) \implies 21(-4) \equiv 7 (\mathrm{mod} 91)$$

multiplicando por 2

$$21(-8) \equiv 14 (\mathrm{mod} 91)$$

Por lo que $x_0 = -8 \underset{(\mathrm{mod}\ 91)}{\longrightarrow} 83$ sumamos $\frac{91}{(21,91)} = 13$ y obtenemos

$$x_{1,2,3,4,5,6,7} \equiv 83, 5, 18, 31, 44, 57, 70 (\mathrm{mod} 91)$$

Lema

Sean $a, b \in \mathbb{Z}$ y $m \geq 2$. Si $a \equiv b (\mathrm{mod} m)$, entonces

$$(a, m) = (b, m).$$

Demostración: Por hipótesis, existen $q_1, q_2, r \in \mathbb{Z}$ tales que

$$\begin{matrix} a = mq_1 + r \\ b = mq_2 + r \end{matrix} \quad \text{con } 0 \leq r < m.$$

Por un teorema anterior (página 49)

$$(a, m) = (a, r) = (b, m).$$

Lema

Sean $a, b, m \in \mathbb{Z}$ tales que $(a, m) = (b, m) = 1$. Entonces

$$(ab, m) = 1$$

Demostración: Supongamos que no, es decir, $(a,m)=(b,m)=1$ pero $(ab,m)\neq 1$. Sea p un número primo tal que $p\Big|(ab,m)$. Entonces $p\Big|m$ y $p\Big|ab$. Dos casos

$$\begin{cases} p\Big|a \implies p\Big|(a,m) \implies (a,m)\neq 1 \text{ contradicción} \\ p\nmid a \implies (a,p)=1 \therefore \text{como } p\Big|ab \implies p\Big|b \therefore p\Big|(b,m) \implies (b,m)\neq 1, \text{ contradicción} \end{cases}$$

Observación: Si p es primo y $p\Big|ab \implies (p\Big|a \vee p\Big|b)$

Teorema de Euler

Sean $a,m\in\mathbb{Z}$ con $m\geq 2$. Si $(a,m)=1$, entonces:

$$a^{\phi(m)}\equiv 1(\mathrm{mod}m)$$

Demostración: Sean $1\leq k_1<\ldots<k_{\phi(m)}\leq m$ tales que $(k_i,m)=1$. Considere los números $ak_1,ak_2,\ldots,ak_{\phi(m)}$
Note que $(ak_i,m)=1$ por el segundo lema, además: Si $ak_i\equiv ak_j(\mathrm{mod}m)$ entonces

$$m\Big|ak_i-ak_j \implies m\Big|a(k_i-k_j) \therefore m\Big|k_i-k_j$$

$$\begin{array}{l} 1\leq k_i\leq m \\ -m\leq -k_j\leq -1 \\ \hline -m+1\leq k_i-k_j\leq m-1 \\ -m\leq k_i-k_j<m \end{array}$$

$$\therefore k_i-k_j=0 \implies k_i=k_j$$

En conclusión, la lista $ak_1,\ldots,ak_{\phi(m)}$ contiene los mismos términos, módulo m, que la lista

$$k_1,k_2,\ldots,k_{\phi(m)}$$

$$\left[\begin{array}{c} m=10 \qquad \phi(m)=4 \\ 1,3,7,9 \\ a=3 \\ 3,9,21,27 \\ 3,9,1,7 \\ \mathrm{mod}\ m \end{array}\right]$$

Entonces

$$k_1,k_2,\ldots,k_{\phi(m)}\equiv(ak_1)(ak_2)\ldots(ak_{\phi(m)})(\mathrm{mod}m)$$

$$k_1,k_2,\ldots,k_{\phi(m)}\equiv a^{\phi(m)}(k_1k_2\ldots k_{\phi(m)})(\mathrm{mod}m)$$

Por el segundo lema

$$(k_1k_2\ldots k_{\phi(m)},m)=1$$

$$\implies m\Big|(k_1k_2\ldots k_{\phi(m)})(a^{\phi(m)}-1)$$

$$\therefore m\Big|a^{\phi(m)}-1$$

$$\therefore a^{\phi(m)}\equiv 1(\mathrm{mod}m).$$

Corolario (Pequeño teorema de Fermat)

Si $a, p \in \mathbb{Z}$, p es primo, y $p \nmid a$, entonces

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

Corolario (Pequeño teorema de Fermat versión 2)

Si $a \in \mathbb{Z}$, p es primo, entonces

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

Demostración:

1. $p \nmid a$: Entonces $a^{p-1} \equiv 1 (\mathrm{mod}\, p) \implies a^{p} \equiv a (\mathrm{mod}\, p)$
2. $p|a$: Entonces $p \Big| a^{p} \implies p \Big| a^{p} - a \implies a^{p} \equiv a (\mathrm{mod}\, p)$

El método RSA

El método RSA es una manera de encriptar un mensaje a partir de la teoría de números creado por Ronald Rivest, Adi Shamir y Leonard Adleman en el MIT.
El método consiste en lo siguiente:

El sistema de encriptamiento RSA

Un **Receptor** crea una clave privada, la cual se mantiene en secreto, y una clave pública, que es habilitada al público. Cualquier persona con la clave pública puede ser el **Remitente** el cual puede mandar mensajes secretos al **Receptor** aunque nunca se hayan comunicado o intercambiado cualquier información además de la clave pública. Así es como lo hacen:
Antes que nada el **Receptor** crea una clave pública y privada como sigue.

1. Genere dos primos grandes distintos, p y q. Estos serán usados para generar la clave privada, y por tanto deberán permanecer ocultos. (En la practica actual p y q son escogidos de tal forma que tengan una longitud de cien dígitos.)

2. Fije $n = pq$

3. Seleccione un entero $e \in [0, n)$ tal que $= (e, \phi(n)) = 1$.
   La clave publica es el par (e, n). Este sera distribuido ampliamente.

4. Sea la clave privada $d \in [0, n)$ el inverso de e módulo $\phi(n)$, es decir

   $$e \cdot d \equiv 1\big(\bmod \phi(n)\big)$$

   esta clave privada puede ser encontrada utilizando el algoritmo de Euclides y expresando como combinación lineal. La clave privada d debe permanecer oculta.

Codificación Para transmitir un mensaje $m \in [0, n)$ hacia el **Receptor**, un **Remitente** usa la clave publica para encriptar m en un mensaje numérico

$$\hat{m} = m^e (\mathrm{mod} n).$$

El **Remitente** puede entonces transmitir el mensaje $\hat{m}$ al **Receptor**
Decodificación El **Receptor** desencripta el mensaje $\hat{m}$ de vuelta a m usando la clave privada:

$$m = \hat{m}^d (\mathrm{mod} n)$$

Sistemas de congruencias lineales

La motivación de este tema sera encontrar la solución a congruencias simultaneas; en otras palabras. Al resolver un sistema de congruencias lineales, encontramos un número x que cumple todas las congruencias simultáneamente, es decir, un número que:

- Al dividirse entre cada módulo m_i, deja exactamente el residuo a_i especificado

Lema

Sean $a_1, \dots, a_n, m \in \mathbb{Z}$ tales que $(a_i, a_j) = 1$ para $i \neq j$ y $a_i \Big| m$ para todo i. Entonces

$$a_1 \dots a_n \Big| m$$

Demostración: Por inducción, para $n = 2$:

$$a_1 \Big| m \text{ y } a_2 \Big| m \text{ y } (a_1, a_2) = 1$$

$\exists x, y, z, w \in \mathbb{Z}$ tales que:

$$m = xa_1, \ m = ya_2$$

$$1 = za_1 + wa_2$$

Multiplicando por m

$$m = mza_1 + mwa_2$$

$$= ya_2za_1 + xa_1wa_2$$

$$= a_1, a_2(yz + xw)$$

$$\therefore a_1a_2 \Big| m$$

Supongamos que el enunciado se cumple para n, y $a_, a_2 \dots, a_n, a_{n+1}$ todos ellos dividen a m y son primos relativos a pares.
Entonces, por hipótesis inductiva

$$a_1 \dots a_n \Big| m$$

además $a_{n+1} \Big| m$ y $(a_1 \dots a_n, a_{n+1}) = 1$. Por el caso $n = 2$,

$$(a_1 \dots a_n)a_{n+1} \Big| m.$$

Teorema chino del residuo

Sean $m_1, \dots, m_t, b_1, \dots, b_t \in \mathbb{Z}$ tales que $(m_i, m_j) = 1$ para $i \neq j$. Entonces, el sistema de congruencias

$$x \equiv b_1 (\text{mod} m_1)$$
$$\vdots$$
$$x \equiv b_t (\text{mod} m_t)$$

tiene solución. además esta solución es única hasta congruencia módulo $m_1, \dots, m_t$.

Demostración: Sea, para cada i

$$n_i = m_1 \dots m_{i-1}m_{i+1} \dots m_t$$

[Note que $(n_i, m_i) = 1$.]
Sean $a_i, b_i \in \mathbb{Z}$ tales que

$$1 = a_in_i + b_im_i$$

Sea

$$x = b_1 a_1 n_1 + a_2 b_2 n_2 + \ldots + b_t a_t n_t$$

x es una solución al sistema de congruencias, ya que, para cada i,

$$\begin{aligned} a_i n_i &\equiv 1 (\mathrm{mod} m_i) \\ a_i n_i &\equiv 0 (\mathrm{mod} m_j) \text{ para } i \neq j \end{aligned}$$

$$\therefore \begin{aligned} x &\equiv b_1 0 + b_2 0 + \ldots + b_{i-1} 0 + b_i 1 + b_{i+1} 0 + \ldots + b_t 0 \\ &\equiv b_i (\mathrm{mod} m_i) \end{aligned}$$

Ahora, supongamos que x' es otra solución al sistema de congruencias. Entonces,

$$x' \equiv b_i (\mathrm{mod} m_i)$$

Restando para cada i.

$$\begin{aligned} x - x' &\equiv 0 (\mathrm{mod} m_i) \\ \Longrightarrow \; & m_i \Big| (x - x') \end{aligned}$$

Por el Lema anterior

$$\begin{aligned} & m_1 \ldots m_t \Big| (x - x') \\ \Longrightarrow \; & x \equiv x' (\mathrm{mod} m_1 \ldots m_t). \end{aligned}$$

Ejemplo:

$$\begin{aligned} x &\equiv 2 (\mathrm{mod} 3) \\ x &\equiv 1 (\mathrm{mod} 5) \\ x &\equiv 6 (\mathrm{mod} 7) \end{aligned}$$

$$\begin{aligned} \text{para } 3: \quad & 1 = 12(3) + (-1)(35) \\ \text{para } 5: \quad & 1 = (-4)(5) + (1)(21) \\ \text{para } 7: \quad & 1 = (-2)(7) + (1)(15) \end{aligned}$$

la solución sera

$$\begin{aligned} x &\equiv (-35)(2) + (21)(1) + (15)(6) (\mathrm{mod} 105) \\ \Longleftrightarrow \; & x \equiv 41 (\mathrm{mod} 105) \end{aligned}$$

Ejercicios: Resolver los siguientes sistemas de congruencias

1. $\begin{aligned} x &\equiv 2 (\mathrm{mod} 5) \\ x &\equiv 3 (\mathrm{mod} 7) \\ x &\equiv 10 (\mathrm{mod} 11) \end{aligned}$

2. $\begin{aligned} x &\equiv 3 (\mathrm{mod} 7) \\ x &\equiv 3 (\mathrm{mod} 5) \\ x &\equiv 4 (\mathrm{mod} 12) \end{aligned}$

3. $\begin{aligned} x &\equiv 1 (\mathrm{mod} 3) \\ x &\equiv 2 (\mathrm{mod} 5) \\ x &\equiv 3 (\mathrm{mod} 7) \end{aligned}$

4. $\begin{aligned} x &\equiv 4 (\mathrm{mod} 5) \\ x &\equiv 7 (\mathrm{mod} 8) \\ x &\equiv 3 (\mathrm{mod} 9) \end{aligned}$

$x \equiv 5(\text{mod}6)$

5. $x \equiv 4(\text{mod}11)$
   $x \equiv 3(\text{mod}17)$

   $x \equiv 5(\text{mod}11)$

6. $x \equiv 14(\text{mod}29)$
   $x \equiv 15(\text{mod}31)$

Solución:

1. Empezaremos por encontrar las combinaciones de cada módulo con el producto de los módulos restantes;

$$\begin{aligned} 1 &= 5(31) + 77(-2) \\ 1 &= 7(8) + 55(-1) \\ 1 &= 11(16) + 35(5) \end{aligned}$$

   ahora solo tomamos los valores de los productos y los multiplicamos por el coeficiente que acompaña a cada módulo individual de la congruencia

$$\begin{aligned} x &\equiv (-154)(2) + (-55)(3) + (-175)(10) \\ &\equiv -2275 \\ &\equiv 37(\text{mod}385) \end{aligned}$$

   el módulo 385 es el producto de todos los módulos.

2. Haremos un procedimiento similar

$$\begin{aligned} 1 &= 7(-17) + 60(2) \\ 1 &= 5(11) + 84(-1) \\ 1 &= 12(3) + 35(-1) \end{aligned}$$

$$\begin{aligned} x &\equiv 120(3) + (-84)(3) + (-35)(4) \\ &\equiv -32(\text{mod}420) \\ &\equiv 388(\text{mod}420) \end{aligned}$$

3.

$$\begin{aligned} 1 &= 3(12) + (-1)(35) \\ 1 &= 5(-4) + (1)(21) \\ 1 &= 7(2) + (1)(15) \end{aligned}$$

   la congruencia:

$$\begin{aligned} x &\equiv (-35) + 42 + 45 \\ &\equiv 52(\text{mod}105) \end{aligned}$$

4.

$$\begin{aligned} 1 &= 5(29) + (-2)72 \\ 1 &= 8(17) + (-3)45 \\ 1 &= 9(9) + (-2)40 \end{aligned}$$

   la congruencia:

$$\begin{aligned} x &\equiv 4(-144) + 7(-135) + 3(-80) \\ &\equiv -1761(\text{mod}360) \\ &\equiv 39(\text{mod}360) \end{aligned}$$

5.

$$1 = 6(-31) + 187(1)$$
$$1 = 11(-37) + 102(4)$$
$$1 = 17(-31) + 66(8)$$

la congruencia:

$$\begin{aligned} x &\equiv 187(5) + 102(16) + 66(24) \\ &\equiv 4151 (\mathrm{mod} 1122) \\ &\equiv 785 (\mathrm{mod} 1122) \end{aligned}$$

6.

$$1 = 11(27) + 899(-4)$$
$$1 = 29(-47) + 341(4)$$
$$1 = 31(-72) + 319(7)$$

la congruencia:

$$\begin{aligned} x &\equiv 899(-20) + 341(56) + 319(105) \\ &\equiv 34611 (\mathrm{mod} 9889) \\ &\equiv 4944 (\mathrm{mod} 9889) \end{aligned}$$

Teorema

Si $a, b \in \mathbb{Z}$ y $(a, b) = 1$, entonces

$$\phi(ab) = \phi(a)\phi(b)$$

Antes de anunciar la demostración del teorema, veamos un bosquejo de la idea general de la demostración.
Consideremos el número 12, sabemos que se puede descomponer en $4 \cdot 3$, ahora considere el arreglo de 4 columnas y 3 filas conformado por los números previos a este

$$\begin{array}{cccc} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{array}$$

seleccionaremos los números que son primos entre sí con 12 y descartaremos los demás

$$\begin{array}{cccc} \boxed{1} & \cancel{2} & \cancel{3} & \cancel{4} \\ \boxed{5} & \cancel{6} & \boxed{7} & \cancel{8} \\ \cancel{9} & \cancel{10} & \boxed{11} & \cancel{12} \end{array}$$

Observe que hay exactamente $2 = \phi(4)$ columnas que contienen números que son primos relativos a 4, esto ocurre porque cada número en la misma columna tiene el mismo residuo módulo 4. Note además que en cada columna hay $2 = \phi(3)$ números que son primos relativos con 3.
Demostración: Considere el arreglo rectangular de tamaño ab

$$\begin{array}{ccccccc} 1 & 2 & \dots & i & \dots & a & [1 \le i \le a] \\ a+1 & a+2 & \dots & a+i & \dots & 2a & \\ 2a+1 & 2a+2 & \dots & 2a+i & \dots & 3a & \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \\ (j-1)a+1 & (j-1)a+2 & \dots & (j-1)a+i & \dots & ja & [1 \le j \le b] \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \\ (b-1)a+1 & (b-1)a+2 & \dots & (b-1)a+i & \dots & ba & \end{array}$$

Usamos el arreglo para contar cuántos de estos números son primos relativos con a.
Observación 1: Si $1 \leq i \leq a$ es tal que $(i, a) \neq 1$ entonces $\forall j$

$$(ja + i, a) \neq 1$$

[Pues $i \equiv ja + i (\text{mod} a)$ y $\therefore (i, a) = (ja + i, a)$]
$\therefore$ Solo las columnas tales que $(i, a) = 1$ pueden contribuir a la cuenta: $\phi(a)$ de estas columnas.
Observación 2: Para cada $1 \leq j \neq j' \leq b$ entonces

$$ja + i \not\equiv j'a + i (\text{mod} b)$$

$\Big[$ De lo contrario, si $ja + i \equiv j'a + i (\text{mod} b) \implies b \Big| a(j - j')$ como $(a, b) = 1 \implies b \Big| j - j'$ con

$$-b < j - j' < b \implies j - j' = 0 \therefore j = j' \Big]$$

además. Si $ja + i \equiv k (\text{mod} b)$

$$\implies (ja + i, b) = (k, b)$$

Por lo tanto: En cada columna podemos reducir módulo b y eliminar aquellos para los cuales $(k, b) \neq 1$.
$\therefore$ Cada columna contribuye $\phi(b)$ números.
Observación 3: $(ab, k) = 1 \iff (a, k) = 1 = (b, k)$ (Pagina 66)
Por lo tanto, al contar los k tales que $(ab, k) = 1$ es lo mismo que contar los k tales que $(a, k) = 1 = (b, k)$

$$\therefore \phi(ab) = \phi(a)\phi(b).$$

Corolario 1

Si $a_1, \ldots, a_k \in \mathbb{Z}$ son tales que $(a_i, a_j) = 1$ si $i \neq j$ entonces

$$\phi(a_1 \ldots a_k) = \phi(a_1) \ldots \phi(a_k)$$

Demostración: Empleando un argumento inductivo sobre el teorema anterior se obtiene el resultado deseado

$$\begin{aligned} \phi(a_1 \ldots a_k) &= \phi(a_1 \ldots a_{k-1})\phi(a_k) \\ &= \phi(a_1 \ldots a_{k-2})\phi(a_{k-1})\phi(a_k) \\ &\vdots \\ &= \phi(a_1) \ldots \phi(a_k) \end{aligned}$$

Corolario 2

Sea $n \in \mathbb{N}$, y sean $p_1, \dots, p_k$, primos distintos y $\alpha_1, \dots, \alpha_k \in \mathbb{N}$ tales que $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$. Entonces

$$\begin{aligned}\phi(n) &= \phi\left(p_1^{\alpha_1}\right) \dots \phi\left(p_k^{\alpha_k}\right) \\ \phi(n) &= \left(p_1^{\alpha_1} - p_1^{\alpha_1 - 1}\right) \dots \left(p_k^{\alpha_k} - p_k^{\alpha_k - 1}\right) \\ &= p_1^{\alpha_1}\left(1 - \frac{1}{p_1}\right) \dots p_k^{\alpha_k}\left(1 - \frac{1}{p_k}\right)\end{aligned}$$

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

La motivación de la siguiente sección sera representar un numero $n \in \mathbb{N} \cup \{0\}$ en una base distinta $b \in \mathbb{N} \backslash \{1\}$.

Lema

Sea $b \in \mathbb{N}$ con $b \geq 2$. Para todo $n \in \mathbb{N}$ existe un único k tal que

$$b^k \leq n < b^{k+1}$$

Demostración: Por inducción sobre n
$n = 1$ basta tomar $k = 0$
Supongamos que se cumple para n, y $b^k \leq n < b^{k+1}$, entonces tenemos dos casos

$$\begin{cases} n + 1 < b^{k+1} \implies b^k \leq n + 1 < b^{k+1} \\ n + 1 = b^{k+1} \implies b^{k+1} \leq n + 1 < b^{k+2} \end{cases}$$

Lema

Para cualquier $k \in \mathbb{N} \cup \{0\}$, y para cualesquiera $a_0, \dots, a_{k-1}$, tales que $0 \leq a_i < b$, se cumple que

$$b^k > a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \dots + a_1 b + a_0.$$

Demostración: Basta probar que $b^k > (b-1)(b^{k-1} + \dots + b + 1)$

$$= b^k + \cancel{\dots} + \cancel{b^2} + \cancel{b} - \cancel{b^{k-1}} - \dots - \cancel{b} - 1$$

Serie telescópica

$$= b^k - 1$$

Teorema

Todo numero $n \in \mathbb{N} \cup \{0\}$ se puede escribir, de manera única, como

$$n = a_k b^k + a_{k-1}b^{k-1} + \dots + a_1 b + a_0$$

en donde cada $0 \leq a_i < b$.

Demostración: Por inducción sobre el único entero k tal que

$$b^k \leq n < b^{k+1}$$

Base: $k = 0$

$$1 \leq n < b^1$$

$$1 \leq n < b$$

Paso inductivo: Si $b^k \leq n < b^{k+1}$
Sean $q, r \in \mathbb{N} \cup \{0\}$ tales que:

$$n = q \cdot b^k + r \quad 0 \leq r < b^k$$

Observación: $1 \leq q < b$; de lo contrario, si

$$b \leq q \implies n = q \cdot b^k + r \geq b \cdot b^k + r \geq b^{k+1}$$

Lo cual es una contradicción. Pues asumimos que $n < b^{k+1}$.
Ahora, como $r < b^k$, entonces si $b^l \leq r < b^{l+1}$

$$\implies l \leq k - 1$$

$\therefore$ se puede aplicar la hipótesis de inducción,

$$r = a_l b^l + a_{l-1} b^{l-1} + \cdots + a_1 b + a_0 \quad 0 \leq a_i < b$$

$$\implies n = q b^k + a_l b^l + a_{l+1} b^{l+1} + \cdots + a_1 b + a_0$$

Para ver la unicidad de la representación supongamos que

$$a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 = c_l b^l + c_{l-1} b^{l-1} + \cdots + c_1 b + c_0$$

con $0 \leq a_i,\ c_i < b$. Sin perdida de generalidad, $a_k, c_k \neq 0$. Calculando potencias mas altas de b, podemos suponer que $k \neq l$, Supongamos sin perder generalidad que $k > l$. Entonces por el segundo lema, $a_k b^k + \cdots + a_0 \geq b^k > c_l b^l + \cdots + c_1 b + c_0$ lo cual es una contradicción. Pues supusimos que $a_k b^k + \cdots + a_0 = c_l b^l + \cdots + c_1 b + c_0$.
Ejemplo: Escribir 1592 en base 16.
Nótese que

$$\begin{aligned} n &= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 \\ &= (a_k b^{k-1} + \cdots + a_1) b + a_0 \end{aligned}$$

Es decir, podemos aplicar el algoritmo de la división múltiples veces y quedarnos con los residuos para formar el numero en la base propuesta;

$$\begin{aligned} 1592 &= 99 \cdot 16 + 8 \\ 99 &= 6 \cdot 16 + 3 \\ 6 &= 0 \cdot 16 + 6 \end{aligned}$$

Por lo que el 1592 en base 16 es

$$(1592)_{16} = 638$$

Criterios de Divisibilidad

Puesto que ahora sabemos que podemos representar un numero en una base de manera única, podemos analizar su divisibilidad en base 10.
Sea $n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0$ con $0 \leq a_i \leq 9$.

Numero	Que pasa?	Criterio
2	$n \equiv a_0 (\mathrm{mod} 2)$	n es par $\iff$ a_0 lo es
5	$n \equiv a_0 (\mathrm{mod} 5)$	$5\|n \iff 5\|a_0 \iff a_0 \in \{0,5\}$
3	$n \equiv a_0 + a_1 + \cdots + a_k (\mathrm{mod} 3)$	$3\|n \iff 3\|a_0 + \cdots + a_k$
9	$n \equiv a_0 + a_1 + \cdots + a_k (\mathrm{mod} 9)$	$9\|n \iff 9\|a_0 + \cdots + a_k$
4	$n \equiv 10a_1 + a_0 (\mathrm{mod} 4)$	$4\|n \iff 4\|10a_1 + a_0$
11	$n \equiv a_0 + a_2 + \cdots - a_1 - a_3 - \ldots (\mathrm{mod} 11)$	$11\|n \iff 11\|a_0 + a_2 + \cdots - a_1 - a_3 - \ldots$

Por ejemplo, para el criterio de 3 consideramos $10 \equiv 1 (\mathrm{mod} 3) \implies 10^l \equiv 1 (\mathrm{mod} 3)$ y así se deducen los siguientes.

Lema

Sea p un numero primo y $a \in \mathbb{Z}$. Entonces,

$$a^2 \equiv 1 (\mathrm{mod} p) \iff \begin{array}{c} a \equiv 1 (\mathrm{mod} p) \\ \text{o} \\ a \equiv -1 (\mathrm{mod} p) \end{array}$$

Demostración: Si $a \equiv 1 (\mathrm{mod} p)$

$$\iff p \Big| a^2 - 1$$

$$\iff p \Big| (a+1)(a-1)$$

$$\underset{p \text{ es primo}}{\iff} \begin{array}{c} p \Big| a+1 \\ \text{o} \\ p \Big| a-1 \end{array}$$

$$\iff \begin{array}{c} a \equiv -1 (\mathrm{mod} p) \\ \text{o} \\ a \equiv 1 (\mathrm{mod} p) \end{array}$$

Teorema (Teorema de Wilson)

Si $p \in \mathbb{N}$, entonces

$$p \text{ es primo} \iff (p-1)! \equiv -1 (\mathrm{mod} p).$$

Demostración: $\Longleftarrow$) Usaremos un argumento contrapositivo. Si p no es primo, entonces $\exists a, b < p$ tales que $p = a \cdot b$. Dos casos:

1. $a \neq b$:

$$(p-1)! = 1 \cdot 2 \ldots a \ldots b \ldots (p-1)$$

$$1 \cdot 2 \ldots (a-1)(a+1) \ldots (b-1)(b+1) \ldots (p-1)ab$$

$$= 1 \cdot 2 \ldots (a-1)(a+1) \ldots (b-1)(b+1) \ldots (p-1)p \equiv 0 (\mathrm{mod} p)$$

2. Solo se puede factorizar como $p = a^2 \to p = q^2$ con q primo y $q \geq 3$

$$(p-1)! = 1 \cdot 2 \ldots (q-1)q(q+1) \ldots (2q-1)2q(q+1) \ldots (p-1)$$

$$= 1 \cdot 2 \ldots (q-1)(q+1) \ldots (2q-1)2(q+1) \ldots (p-1)\underset{p}{q^2} \equiv 0 (\mathrm{mod} p)$$

Ultimo caso $p = 4$:

$$(p-1)! = 6 \equiv 2 \not\equiv -1 (\mathrm{mod} 4)$$

$\Longrightarrow$) Supongamos que p es primo. Dos casos

1. $p = 2$:

$$(p-1)! = 1! = 1 \equiv -1 (\mathrm{mod} 2)$$

2. p es impar. Entonces:
Para cada $i < p$, se tiene que $(i, p) = 1$ pues p es primo $\therefore$ existe $j < p$ tal que $i \cdot j \equiv 1 (\mathrm{mod} p)$. además, si $\begin{matrix} i \not\equiv 1 (\mathrm{mod} p) \\ i \not\equiv -1 (\mathrm{mod} p) \end{matrix} \implies j \neq i$ por el Lema (pagina 77).
Por lo tanto, los números $2, 3, \ldots, p-2$ se particionan en parejas i, j tales que $ij \equiv 1 (\mathrm{mod} p)$.

$$\therefore (p-1)! = 1 \cdot 2 \ldots (p-2)(p-1) \equiv 1 \cdot \underbrace{1 \cdots 1}_{\frac{p-3}{2} \text{ veces}} (p-1) (\mathrm{mod} p) \equiv -1 (\mathrm{mod} p)$$

Conversión de Números (Ejercicios)

1. **Decimal a binario**
   (a) $231 = (1110, 0111)_2$
   (b) $4532 = (1, 0001, 1011, 0100)_2$
   (c) $97644 = (1, 0111, 1101, 0110, 1100)_2$
2. **Binario a decimal**
   (a) $(1, 1111)_2 = 31$
   (b) $(1, 0101, 0101)_2 = 341$
   (c) $(110, 1001, 0001, 0000)_2 = 26896$
3. **Hexadecimal a decimal**
   (a) $(80E)_{16} = 2062$
   (b) $(135AB)_{16} = 79275$

(c) $(ABBA)_{16} = 43963$

(d) $(DEFACED)_{16} = 233811181$

4. **Hexadecimal a binario**

(a) $(BADFACED)_{16} = (1011, 1010, 1101, 1111, 1010, 1100, 1110, 1101)_2$

(b) $(ABCDEF)_{16} = (1010, 1011, 1100, 1101, 1110, 1111)_2$

5. **Binario a hexadecimal**

(a) $(1111, 0111)_2 = (F7)_{16}$

(b) $(1010, 1010, 1010)_2 = (AAA)_{16}$

(c) $(111, 0111, 0111, 0111)_2 = (7777)_{16}$

(d) $(1011, 0111, 1011)_2 = (B7B)_{16}$

(e) $(1, 1000, 0110, 0011)_2 = (1863)_{16}$

Reciprocidad Cuadrática

La motivación del siguiente tema será determinar si $x^2 \equiv a(\text{mod}p)$ p es un número primo tiene solución.

Residuo cuadrático

Sea p un numero primo y $a \in \mathbb{Z}$. Decimos que a es un residuo cuadrático módulo p si existe $x \in \mathbb{Z}$ tal que

$$x^2 \equiv a(\text{mod}p)$$

Ejemplo

x	x^2 mod 11
0	0
1	1
2	4
3	9
4	5
5	3
6	3
7	5
8	9
9	4
10	1

Nótese que aparecen dos veces los valores bajo módulo 11, los números que estén en ambas columnas serán residuos cuadráticos en este caso $0, 1, 4, 9, 5, 3$.

x	x^2 mod 7
0	0
1	1
2	4
3	2
4	2
5	4
6	1

En este caso $0, 1, 4, 2$ son los residuos cuadráticos.

Teorema

Sea p un numero primo impar y $a \in \mathbb{Z}$. Entonces:

1. Si $p|a$ la ecuación $x^2 \equiv a(\text{mod}p)$ tiene una única solución, [0 es residuo cuadrático] $[x^2 \equiv 0(\text{mod}p)]$
2. Si $p \nmid a$ entonces la ecuación $x^2 \equiv a(\text{mod}p)$ tiene o bien 0, o bien 2 soluciones.
3. Entre los números $1, \dots, p-1$ hay $\frac{p-1}{2}$ que son residuos cuadráticos y $\frac{p-1}{2}$ que no lo son.

Demostración:

1. Si $p \Big| a \implies a \equiv 0(\text{mod}p)$ y $0^2 \equiv a(\text{mod}p)$
   Ahora, si $x \in \mathbb{Z}$ tal que $x^2 \equiv 0(\text{mod}p)$ entonces
   $$p \Big| x \cdot x \implies p \Big| x \therefore x \equiv 0(\text{mod}p)$$

2. Supongamos que el numero de soluciones a la congruencia $x^2 \equiv a(\text{mod}p)$ no es cero, y sea x_0 una solución:
   $$x_0^2 \equiv a(\text{mod}p)$$
   Entonces $(-x_0)^2 = x_0^2 \equiv a(\text{mod}p)$
   además, $x_0 \not\equiv -x_0(\text{mod}p)$ pues de lo contrario, tendríamos que $p \Big| x_0 - (-x_0) = 2x_0$
   $$\implies \text{o bien } p|2, \text{ o bien } p|x_0$$
   Si $p|2 \implies p = 2$ lo cual es una contradicción pues por hipótesis p es un primo impar.
   Si $p|x_0$:
   $$\begin{aligned} & x_0 \equiv 0(\text{mod}p) \\ & x_0^2 \equiv 0(\text{mod}p) \\ \implies & a \equiv 0(\text{mod}p) \\ \implies & p|a \end{aligned}$$
   Lo cual es una contradicción pues suponemos inicialmente que $p \nmid a$.

3. Inmediata.

Símbolo de Legendre

Dado un número primo p y $a \in \mathbb{Z}$, definimos el símbolo de Legendre como

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } p \mid a \\ 1 & \text{si } p \nmid a \text{ y } a \text{ es residuo cuadrático módulo } p \\ -1 & \text{en caso contrario.} \end{cases}$$

En otras palabras

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{si } x^2 \equiv a (\mathrm{mod} p) \text{ tiene una solución} \\ 1 & \text{si } x^2 \equiv a (\mathrm{mod} p) \text{ tiene dos soluciones} \\ -1 & \text{si } x^2 \equiv a (\mathrm{mod} p) \text{ no tiene soluciones} \end{cases}$$

Ejemplos:

$$\left(\frac{4}{7}\right) = 1 \qquad \left(\frac{3}{7}\right) = -1 \qquad \left(\frac{14}{7}\right) = 0$$
$$\left(\frac{10}{7}\right) = \left(\frac{3}{7}\right) = -1 \qquad \left(\frac{7}{11}\right) = -1 \qquad \left(\frac{9}{11}\right) = 1$$

Teorema (Criterio de Euler)

Sean $a \in \mathbb{Z}$ y p un primo impar. Entonces

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) (\mathrm{mod} p)$$

Demostración: Hay tres casos:

1. $p|a$. Entonces, $a \equiv 0 (\mathrm{mod} p)$ y

$$\therefore a^{\frac{p-1}{2}} \equiv \underset{\left(\frac{a}{p}\right)}{0} (\mathrm{mod} p)$$

2. Si $p \nmid a$ y a no es un residuo cuadrático módulo p. Entonces existe un $b \in \mathbb{Z}$ y $p \nmid b$ (pues seria congruente con cero) tal que $b^2 \equiv a (\mathrm{mod} p)$. Entonces

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv (b^2)^{\frac{p-1}{2}} (\mathrm{mod} p) \\ &\equiv b^{p-1} (\mathrm{mod} p) \\ &\equiv \underset{\left(\frac{a}{p}\right)}{1} (\mathrm{mod} p) \end{aligned}$$

3. Si $p \nmid a$ y a no es un residuo cuadrático módulo p. Entonces, considere los números

$$1, 2, \ldots, p-2, p-1.$$

Para cada $i \in \{1, \ldots, p-1\}$ existe j tal que

$$\underbrace{ij \equiv a (\mathrm{mod} p)}_{\text{La congruencia } 1x \equiv a (\mathrm{mod}\ p) \text{ siempre tiene solución}}$$

además $j \not\equiv i(\bmod p)$ (ya que no es residuo cuadrático módulo p). Estos números se pueden acomodar en $\frac{p-1}{2}$ parejas cuyo producto es $\equiv a(\mathrm{mod}\, p)$ Entonces,

$$(p-1)! = 1 \cdot 2 \cdots (p-2)(p-1) = \overbrace{a \cdot a \cdots a}^{\frac{p-1}{2} \text{ veces}} = a^{\frac{p-1}{2}} \underset{\left(\frac{a}{p}\right)}{\equiv} -1 \,(\mathrm{mod} p) \quad \text{Teorema de Wilson}$$

Utilizando este último teorema podemos inferir ciertas propiedades del símbolo de Legendre, por ejemplo:

$$\left(\frac{ab}{p}\right) \equiv (ab)(\mathrm{mod} p)$$
$$\equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} (\mathrm{mod} p)$$
$$= \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Propiedades del símbolo de Legendre

1. Si $a \equiv b(\mathrm{mod} p)$, entonces
$$\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$$
2. $$\left(\frac{a^2}{p}\right) = 1$$
3. $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$$

Ejemplos:

$\left(\frac{642}{37}\right) = \left(\frac{13}{37}\right) \qquad \left(\frac{642}{31}\right) = \left(\frac{22}{31}\right) = \left(\frac{2\cdot 11}{31}\right) = \left(\frac{2}{31}\right)\left(\frac{11}{31}\right)$
$\left(\frac{41}{29}\right) = \left(\frac{12}{29}\right) = \left(\frac{2^2\cdot 3}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{2}{29}\right)\left(\frac{3}{29}\right) = \left(\frac{2}{29}\right)^2\left(\frac{3}{29}\right) = \left(\frac{3}{29}\right)$
En general, si $a \in \mathbb{Z}$

$$a = (-1)^{\epsilon} p_1^{\alpha_1} \ldots p_k^{\alpha_k}$$

donde los p_i son primos distintos, cada $\alpha_i = 2\beta_i + \gamma_i; \quad \gamma_i \in \{0, 1\}$. Entonces

$$\left(\frac{a}{p}\right) = \left(\frac{(-1)^{\epsilon} p_1^{\alpha_1} \ldots p_k^{\alpha_k}}{p}\right) = \left(\frac{(-1)^{\epsilon}}{p}\right)\left(\frac{p_1^{\alpha_1}}{p}\right) \ldots \left(\frac{p_k^{\alpha_k}}{p}\right)$$
$$= \left(\frac{(-1)^{\epsilon}}{p}\right)\left(\frac{p_1^{2\beta_1+\gamma_1}}{p}\right) \ldots \left(\frac{p_k^{\beta_k+\gamma_k}}{p}\right)$$
$$= \left(\frac{(-1)^{\epsilon}}{p}\right)\left(\frac{\left(p_1^{\beta_1}\right)^2}{p}\right)\left(\frac{p_1^{\gamma_1}}{p}\right) \ldots \left(\frac{\left(p_k^{\beta_k}\right)^2}{p}\right)\left(\frac{p_k^{\gamma_k}}{p}\right)$$

$$= \left(\frac{(-1)^{\epsilon}}{p}\right)\left(\frac{p_1^{\gamma_1}}{p}\right)\cdots\left(\frac{p_k^{\gamma_k}}{p}\right)$$
$$= \left(\frac{\operatorname{sgn}(a)}{p}\right)\prod_{\alpha_i \text{ impares}}\left(\frac{p_i}{p}\right)$$

Por lo tanto, para calcular cualquier símbolo de Legendre, basta conocer:

- $\left(\frac{1}{p}\right)$
- $\left(\frac{-1}{p}\right)$
- $\left(\frac{2}{p}\right)$
- $\left(\frac{q}{p}\right)$ si q es primo impar.

Es fácil notar que $\left(\frac{1}{p}\right) = 1$, ahora calculemos los demás casos.

Proposición

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 (\text{mod} 4) \\ -1 & \text{si } p \equiv 3 (\text{mod} 4) \end{cases}$$

Demostración: Dos casos:

1. $p = 4b + 1$ para algún $b \in \mathbb{Z}$, entonces,
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4b}{2}} = (-1)^{2b} = 1$$
2. $p = 4b + 3$ para algún $b \in \mathbb{Z}$, entonces,
$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{\frac{4b+2}{2}} = (-1)^{2b+1} = -1$$

Lema (de Gauß)

Sea p primo impar y $a \in \mathbb{Z}$ con $p \nmid a$.
Sea
$$n = \left|\left\{ i \;\middle|\; \frac{p}{2} < i \text{ y } i \equiv ja (\text{mod} p) \quad \text{para } 1 \leq j \leq \frac{p-1}{2} \right\}\right|$$
Entonces,
$$\left(\frac{a}{p}\right) = (-1)^n$$

Antes de demostrar el Lema, para calcular n consideramos $1 \cdot a, 2 \cdot a, \cdots, \left(\frac{p-1}{2}\right) a$ residuos módulo p y después contamos cuántos son mayores que $\frac{p}{2}$.

Ejemplo: $\left(\frac{5}{7}\right)$ notemos que $\frac{p-1}{2} = \frac{6}{2} = 3$ entonces consideramos los residuos 1,2 y 3, como $a = 5$ entonces multiplicando por 5 estos residuos obtenemos

$$5, 10, 15$$

reducimos módulo 7

$$5, 3, 1$$

y contamos cuántos son mayores que $\left\lfloor \frac{p}{2} \right\rfloor$ en este caso solo 5 lo es, por lo que $n = 1$.

Demostración: Al reducir $a, 2a, \ldots, \left(\frac{p-1}{2}\right) a \quad (*)$ módulo p obtenemos

$$s_1, \ldots, s_m < \frac{p}{2} < r_1, \ldots, r_n \qquad \left[m + n = \frac{p-1}{2}\right]$$

$[(*)\ ia \equiv ja (\mathrm{mod} p) \implies p|a(i-j) \implies p|(i-j)]$
además,

$$p - r_i < \frac{p}{2}$$

Note que $p - r_i \neq s_j$ para todo j [De lo contrario, $p - ia \equiv ja (\mathrm{mod} p) \implies p|p - (i + j)a \implies p| - (p - (i + j)a) + p \implies p|(i + j)a \implies p|i + j$ con $i \leq i + j < p$, contradicción]
Por lo tanto

$$s_1, \ldots, s_m, p - r_1, \ldots, p - r_n \leq \frac{p-1}{2}$$

Los s_m son distintos entre si. $\therefore$ son la misma lista que $1, \ldots, \frac{p-1}{2}$ pero con el orden cambiado. Por lo tanto, multiplicando todos:

$$\left(\frac{p-1}{2}\right)! = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) = s_1 \cdots s_m (p - r_1) \ldots (p - r_n)$$

$$\equiv s_1 \cdots s_m (-r_1) \cdots (-r_n) (\mathrm{mod} p)$$

$$\equiv (-1)^n s_1 \cdots s_m \cdot r_1 \cdots r_n (\mathrm{mod} p)$$

$$\equiv (-1)^n a(2a)(3a) \cdots \left(\frac{p-1}{2}\right) a \equiv (-1)^n a^{\frac{p-1}{2}} \left(1 \cdot 2 \cdots \left(\frac{p-1}{2}\right)\right)$$

$$\equiv (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! (\mathrm{mod} p)$$

además $\left(\left(\frac{p-1}{2}\right)!\ ,\ p\right) = 1 \quad \therefore \left(\frac{p-1}{2}\right)!$ tiene inverso multiplicativo mod p

$$\implies 1 \equiv (-1)^n a^{\frac{p-1}{2}} (\mathrm{mod} p)$$

$$\equiv (-1)^n \left(\frac{a}{p}\right) (\mathrm{mod} p)$$

como tanto $(-1)^n$ como $\left(\frac{a}{p}\right)$ son 1 o -1 la conclusión es que

$$(-1)^n = \left(\frac{a}{p}\right)$$

Teorema

Si p es primo impar, entonces

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{si } p \equiv 1 \text{ o } 7 (\text{mod} 8) \\ -1 & \text{si } p \equiv 3 \text{ o } 5 (\text{mod} 8) \end{cases}$$

Demostración: Considere

$$1, 2, \ldots, \frac{p-1}{2} \text{ Multiplicados por } 2 :$$

$$2, 4, \ldots, p-1 \text{ No hay falta de reducir módulo } p$$

Note que:

$$2j < \frac{p}{2} \iff j < \frac{p}{4} \iff j \leq \left\lfloor \frac{p}{4} \right\rfloor$$

$\therefore$ El "n" del lema de Gauß es:

$$n = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor$$

Ahora si, calculamos $\left(\frac{2}{p}\right)$, 4 casos

1. $p = 8b + 1$ entonces

$$n = \frac{8b}{2} - \left\lfloor 2b + \frac{1}{4} \right\rfloor = 4b - 2b = 2b$$

2. $p = 8b + 3$ entonces

$$n = \frac{8b+2}{2} - \left\lfloor \frac{8b+3}{4} \right\rfloor = 4b + 1 + 2b = 2(2b+1) + 1$$

$$\therefore \left(\frac{2}{p}\right) = (-1)^n = -1$$

3. $p = 8b + 5$

$$n = \frac{8b+4}{2} + \left\lfloor \frac{8b+5}{4} \right\rfloor = 4b + 2 + 2b + 1 = 2(2b+1+b) + 1$$

$$\implies \left(\frac{2}{p}\right) = (-1)^n = -1$$

4. $p = 8b + 7$

$$n = \frac{8b+6}{2} + \left\lfloor \frac{8b+7}{4} \right\rfloor = 4b + 3 + 2b + 1 = 6b + 4 = 2(3b+2)$$

$$\therefore \left(\frac{2}{p}\right) = (-1)^n = 1$$

Lema

Sea p primo impar y $a \in \mathbb{Z}$ también impar y con $p \nmid a$. Entonces

$$\left(\frac{a}{p}\right) = (-1)^N$$

en donde

$$N = \sum_{i=1}^{\frac{(p-1)}{2}} \left\lfloor \frac{ia}{p} \right\rfloor$$

Demostración: Consideramos $a, 2a, \ldots, \left(\frac{p-1}{2}\right) a$ y al reducirlos módulo p obtenemos:

$$s_1, \ldots, s_m < \frac{p}{2} < r_1, \ldots, r_n \quad [n \text{ es la misma del lema de Gauß}]$$

Al igual que en la demostración del Lema de Gauß, los números $s_1, \ldots, s_m, p-r_1, \ldots, p-r_n < \frac{p}{2}$ y son distintos entre si, y $\therefore$ son los números $1, \ldots, \frac{p-1}{2}$ pero posiblemente listados en un orden distinto.
Por lo tanto

$$\sum_{i=1}^{\frac{p-1}{2}} i = \sum_{i=1}^{m} s_i + \sum_{i=1}^{n} (p - r_i)$$
$$= np + \sum_{i=1}^{m} s_i - \sum_{i=1}^{n} r_i \qquad (*)$$

además, para cada $i = 1, \ldots, \frac{p-1}{2}$ tenemos que $ia = \underbrace{(\text{cociente})}_{\left\lfloor \frac{ia}{p} \right\rfloor} p + \underbrace{\text{residuo}}_{\text{los } s_j, r_j}$ entonces

$$\begin{aligned} a &= \left\lfloor \frac{a}{p} \right\rfloor p + res_1 \\ 2a &= \left\lfloor \frac{2a}{p} \right\rfloor p + res_2 \\ &\vdots \\ \left(\frac{p-1}{2}\right) a &= \left\lfloor \frac{\left(\frac{p-1}{2}\right) a}{p} \right\rfloor p + res_{\frac{p-1}{2}} \end{aligned}$$

$$\sum_{i=1}^{\frac{p-1}{2}} ia = p \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor + \sum_{j=1}^{m} s_j + \sum_{j=1}^{n} r_j \qquad (**)$$

Restando $(*)$ y $(**)$ obtenemos:

$$a \sum_{i=1}^{\frac{p-1}{2}} i - \sum_{i=1}^{\frac{p-1}{2}} = p \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor - np + 2 \sum_{i=1}^{n} r_i$$

$$\underbrace{\boxed{(a-1) \sum_{i=1}^{\frac{p-1}{2}} i}}_{\text{par}} = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor - np + \underbrace{\boxed{2 \sum_{i=1}^{n} r_i}}_{\text{impar}}$$

Por lo tanto, los números $p\sum_{i=1}^{\frac{p-1}{2}}$ y np son o ambos pares, o ambos impares. Como p es impar, entonces

$$N = \sum_{i=1}^{\frac{p-1}{2}} \left\lfloor \frac{ia}{p} \right\rfloor \text{ y } n \text{ son ambos pares o impares,}$$

$$\implies (-1)^N = (-1)^n = \left(\frac{a}{p}\right)$$

Lema de Gauß

Teorema (Ley de Reciprocidad Cuadrática de Gauß)

Sean p, q dos primos impares distintos. Entonces,

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)} = \begin{cases} 1 & \text{si } \left(\frac{p-1}{2}\right) \text{ o } \left(\frac{q-1}{2}\right) \text{ es par} \\ -1 & si \left(\frac{p-1}{2}\right) \text{ y } \left(\frac{q-1}{2}\right) \text{ son impares} \end{cases}$$

En otras palabras: p es residuo cuadrático módulo $p \iff q$ es residuo cuadrático módulo p en todos los casos excepto cuando $\begin{matrix} p \equiv 3(\mathrm{mod}4) \\ q \equiv 3(\mathrm{mod}4) \end{matrix}$ además en el caso cuando $p, q \equiv 3(\mathrm{mod}\,4)$ entonces p es residuo cuadrático módulo $q \iff q$ no es residuo cuadrático módulo p.

Demostración (Eisenstein): Sea

$$\mathcal{S} = \left\{ (x, y) \in \mathbb{Z} \times \mathbb{Z} \middle| \, 1 \leq x \leq \frac{p-1}{2} \text{ y } 1 \leq y \leq \frac{q-1}{2} \right\}$$

Note que

$$|\mathcal{S}| = \left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)$$

Por otro lado,

$$\mathcal{S} = \mathcal{S}_1 \dot{\bigcup} \mathcal{S}_2$$

en donde

$$\mathcal{S}_1 = \left\{ (x, y) \in \mathcal{S} \middle| \, qx > py \right\}$$

$$\mathcal{S}_2 = \left\{ (x, y) \in \mathcal{S} \middle| \, qx < py \right\}$$

Note que es imposible tener $qx = qy$ pues de lo contrario $\implies q|py \implies q|p \vee q|y$ contradicción.
Note que:

$$\mathcal{S}_1 = \left\{ (x, y) \in \mathcal{S} \middle| \, qx > py \right\} = \left\{ (x, y) \in \mathcal{S} \middle| \begin{matrix} 1 \leq x \leq \frac{p-1}{2} \\ \wedge\, 1 \leq y \leq \frac{qx}{p} \end{matrix} \right\}$$

$$\therefore |\mathcal{S}_1| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor = N_p \quad \text{Del Lema anterior}$$

$$S_2 = \left\{ (x,y) \in S \,\middle|\, qx < py \right\} = \left\{ (x,y) \in S \,\middle|\, \begin{array}{c} 1 \le y \le \frac{q-1}{2} \\ \wedge\, 1 \le y \le \frac{qy}{q} \end{array} \right\}$$

$$\implies |S_2| = \sum_{x=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor = N_q$$

Por lo tanto

$$\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right) = N_p + N_q$$

$$\implies \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{N_q}(-1)^{N_p}$$

$$= (-1)^{N_p+N_q} \quad \text{(Lema Anterior)}$$

$$= (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$$

Ejemplos:

1. $\left(\frac{7}{53}\right)$ Note que $53 \equiv 1 (\mathrm{mod} 4)$ por lo que $\left(\frac{7}{53}\right) = \left(\frac{53}{7}\right) = \left(\frac{4}{7}\right) = \left(\frac{2^2}{7}\right) = 1$
2. $\left(\frac{-158}{101}\right) = \left(\frac{-1}{101}\right)\left(\frac{2}{101}\right)\left(\frac{79}{101}\right) \implies (1)(-1)(1) = -1$

Teorema

$$\sum_{p \text{ primo}} \frac{1}{p} \text{ diverge}$$

Demostración: Dado n, sean $p_1, \ldots, p_l$ los primos menores que n y definimos:

$$\lambda(n) = \prod_{i=1}^{l} \frac{1}{1 - \frac{1}{p_i}}$$

Recordando que

$$\frac{1}{1-\frac{1}{p_i}} = \sum_{j=0}^{\infty} \frac{1}{(p_i)^j} \implies \prod_{i=1}^{l}\left(\sum_{j=0}^{\infty} \frac{1}{(p_i)^j}\right)$$

$$= \sum_{j_1,\ldots,j_l} \left(\frac{1}{p_1^{j_1}} \cdots \frac{1}{p_l^{j_l}}\right)$$

$$= \sum_{j_1,\ldots,j_l} \frac{1}{p_1^{j_1} \cdots p_l^{j_l}} > 1 + \frac{1}{2} + \cdots + \frac{1}{n}$$

Haciendo tender n a infinito, obtenemos que

$$\lim_{n\to\infty} \lambda(n) \text{ diverge}$$

Tomando logaritmos

$$\log(\lambda(n)) = \sum_{i=1}^{l} \log\left(\frac{1}{1-\frac{1}{p_i}}\right)$$

Usando la serie de Taylor de $\log\left(\frac{1}{1-x}\right)$:

$$= \sum_{i=1}^{l}\left(\sum_{n=1}^{\infty}\frac{\left(\frac{1}{p_i}\right)^n}{n}\right) = \sum_{i=1}^{l}\left(\sum_{n=1}^{\infty}\frac{1}{np_i{}^n}\right)$$

$$= \frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_l} + \sum_{i=1}^{l}\left(\sum_{n=2}^{\infty}\frac{1}{np_i{}^n}\right) \qquad (*)$$

Notemos que

$$\sum_{n=2}^{\infty}\frac{1}{np_i{}^n} < \sum_{n=2}^{\infty}\frac{1}{p_i^n} = \frac{1}{p_i^2}\sum_{n=0}^{\infty}\frac{1}{p_i^n}$$

$$= \frac{1}{p^2}\left(\frac{1}{1-\frac{1}{p_i}}\right) = \frac{1}{p_i^2 - p_i} < \infty$$

Por un lado sabemos que $\lambda(n)$ diverge por lo que $\log(\lambda(n))$ diverge a $+\infty$ conforme $n \to \infty$ y de $(*)$ sabemos que la suma anidada también converge, por lo que para que la ecuación tenga sentido $\frac{1}{p_1} + \frac{1}{p_2} + \cdots + \frac{1}{p_l}$ debe diverger conforme $n \to \infty$

Teorema

$$\pi(x) > \log(\log(x))$$

para x lo suficientemente grande
Donde $\pi(x)$ es una función que cuenta los números primos menores que x.

Demostración: Sea $p_1, p_2, \ldots, p_n, \ldots$ la sucesión de primos en orden creciente.
Observación: $p_{n+1} \leq p_1 p_2 \ldots p_n + 1$
Afirmación: para toda n,

$$p_n \leq 2^{2^n}$$

Dem.(Af.) Por inducción $n = 1 \implies p_1 = 2 \implies 2^{2^1} = 4$ se cumple; Si el resultado es cierto para toda $k \leq n$, entonces

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \leq 2^{2^1} 2^{2^2} \ldots 2^{2^n} + 1$$

$$= 2^{2^1 + \ldots 2^n} + 1 < 2^{2^{n+1}} + 1 \implies p_{n+1} \leq 2^{2^{n+1}}$$

Como consecuencia de la afirmación:,

$$n \leq \pi(2^{2^n})$$

Supongamos que $x > e^{e^3}$, elija n tal que

$$e^{e^{n+1}} < x \leq e^{e^n}$$

debe tenerse $n \geq 4$ Note que $e^{n-1} > 2^n$ Por lo tanto

$$\pi(x) \geq \pi(e^{e^{n-1}}) \geq \pi(e^{2^n}) \geq \pi(2^{2^n}) \geq n \geq \log(\log(x))$$

Definiendo a $\mathbb{R}$

Por medio de cortes de Dedekind.

Cortes de Dedekind

Un corte de Dedekind es un $X \subseteq \mathbb{Q}$ tal que:

1. $X \neq \emptyset$
2. X es un segmento inicial de $\mathbb{Q}$
   [Si $q, r \in \mathbb{Q}$ con $q \leq r$ y $r \in X \implies q \in X$]
3. X no tiene máximo
4. $X \neq \mathbb{Q}$

Ejemplos

- $\left\{ q \in \mathbb{Q} \;\middle|\; q^2 < 2 \right\} \cup \left\{ q \in \mathbb{Q} \;\middle|\; q \leq 0 \right\}$
- $\left\{ q \in \mathbb{Q} \;\middle|\; q < 0 \right\}$
- $\left\{ q \in \mathbb{Q} \;\middle|\; (2q-1)^2 < 5 \right\} \cup \left\{ q \in \mathbb{Q} \;\middle|\; 2q - 1 \leq 0 \right\}$

$\mathbb{R}$

Definimos a $\mathbb{R}$ como

$$\mathbb{R} := \left\{ X \subseteq \mathbb{Q} \;\middle|\; X \text{ es corte de Dedekind} \right\}$$

Al igual que con $\mathbb{Z}$ o $\mathbb{Q}$ tenemos que definir ciertos objetos para $\mathbb{R}$

Encaje de $\mathbb{Q}$ en $\mathbb{R}$

Un encaje

$$\begin{aligned} E : \mathbb{Q} &\longrightarrow \mathbb{R} \\ q &\longmapsto \left\{ r \in \mathbb{Q} \;\middle|\; r < q \right\} \end{aligned}$$

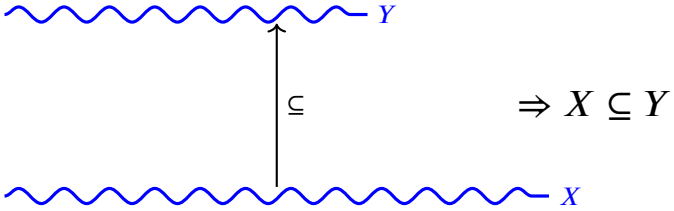
1. E es inyectiva: Si $q, q' \in \mathbb{Q}$ y $q < q'$. Tomamos $r \in \mathbb{Q}$ con $q < r < q'$ y $r \in E(q') \backslash E(q) \implies E(q') \neq E(q)$

Orden en $\mathbb{R}$

Dados $X, Y \in \mathbb{R}$ definimos:

$$X \leq Y \iff X \subseteq Y$$

Una ilustración de esta definición es la siguiente:



Proposición

$\leq$ es una relación de orden lineal

Demostración: Sean $X, Y \in \mathbb{R}$ y supongamos que $X \not\leq Y$ [Por demostrar $Y \leq X$ i.e. $Y \subseteq X$ i.e. $X \not\subseteq Y$];
Sea $q \in X \backslash Y$ y sea $r \in Y$ [P.D. $r \in X$]
Comparando $r, q \in \mathbb{Q}$, tenemos tres casos

$r < q$: Como $q \in X \implies r \in X$
$r = q$: Como $r \in Y \implies q \in Y_{\#c}$
$q < r$: Como $r \in Y$ y Y es corte de Dedekind $\implies q \in Y_{\#c}$

Proposición

Si $q, r \in \mathbb{Q}$ y $q \leq r$ entonces

$$E(q) \leq E(r)$$

Demostración: Si $q, r \in \mathbb{Q}$ [P.D. $E(q) \leq E(r)$ i.e. $E(q) \subseteq E(r)$]; Sea $s \in E(q)$ [P.D. $s \in E(r)$ i.e. $s < r$]; i.e. $s < q$. Por transitividad del orden en $\mathbb{Q}$, concluimos que $s < r$ y $s \in E(r)$. $\implies E(q) \subseteq E(r) \therefore E(q) \leq E(r)$

Axioma del Supremo

Todo subconjunto de $\mathbb{R}$ no vacío y acotado superiormente posee un supremo.

Proposición

$\mathbb{R}$ equipado con $\leq$, satisface el axioma del supremo.

Demostración: Sea $(\mathscr{X} \subseteq \mathbb{R}) \neq \varnothing$ tal que tiene una cota superior. Sea

$$Z = \bigcup_{X \in \mathscr{X}} X$$

de Z se desprenden los siguientes hechos:

- Para todo $x \in \mathscr{X}$, $X \subseteq Z \implies X \leq Z$, i.e. Z es cota superior de $\mathscr{X}$
- Siempre que Y sea un conjunto que satisface: $\forall X \in \mathscr{X},\ X \subseteq Y$ entonces $Z \subseteq Y$

Basta demostrar que Z es un corte de Dedekind. (una vez hecho esto, es inmediato que Z sería la mínima cota superior de $\mathscr{X}$).

1. $Z \neq \varnothing$: Como $\mathscr{X} \neq \varnothing$, Sea $x \in \mathscr{X}$. Entonces, al ser X un corte de Dedekind, $X \neq \varnothing$. Sea $x \in X \implies x \in Z \implies Z \neq \varnothing$.

2. Sean $q \in Z$ y $r < q$. [P.D. $r \in Z$] Como

   $$q \in Z = \bigcup_{X \in \mathscr{X}} X,$$

   existe $X \in \mathscr{X}$ tal que $q \in X$; como además $r < q$ y X es corte de Dedekind $\implies r \in X \therefore r \in \bigcup_{x \in \mathscr{X}} X = Z$

3. Supongamos que Z tiene máximo, es decir, existe $q \in Z$ tal que $\forall r \in Z,\ r \leq q$. Como $q \in Z = \bigcup_{X \in \mathscr{X}} X \implies$ hay algún $X \in \mathscr{X}$ tal que $q \in X$
   Sea $r \in X$ arbitrario, entonces $r \in Z \therefore r \leq q \implies q = \max(X)$, lo que contradice que X es corte de Dedekind.

4. Demostremos que $Z \neq \mathbb{Q}$. Como $\mathscr{X}$ es acotado superiormente, sea $y \in \mathbb{R}$ cota superior para $\mathscr{X}$. Al ser y corte de Dedekind, sea $q \in \mathbb{Q}$ con $q \notin y$. [P.D. $q \notin Z$],
   Note que $\forall r \in y,\ r < q$ [De lo contrario, tendiéramos $\begin{cases} q = r_{\#c} \\ q < r \implies q \in y_{\#c} \end{cases}$]
   Supongamos que

   $$q \in Z = \bigcup_{X \in \mathscr{X}} X$$

   $\implies$ existe un $X \in \mathscr{X}$ tal que $q \in X$. Esto implicaría que al ser X un corte de Dedekind $\forall r \in y \quad r \in X \implies y \subseteq X$. Como además $q \in X \backslash y \implies y \subsetneq X \implies y < X$, lo que contradice que y es cota superior de $\mathscr{X} \therefore q \notin Z \implies Z \neq \mathbb{Q}$.

+ en $\mathbb{R}$

Definimos $+ : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ mediante

$$X + Y = \left\{ q + r \,\middle|\, q \in X \text{ y } r \in Y \right\}$$

Proposición

Si $X, Y \in \mathbb{R}$ entonces $X + Y \in \mathbb{R}$

Demostración: Basta demostrar que $X + Y$ es corte de Dedekind

1. Como $X, Y \neq \emptyset$ tomemos $q \in X$ y $r \in Y \implies q + r \in X + Y \neq \emptyset$

2. Sea $a \in X + Y$ y $b < a$ [P.D. $b \in X + Y$]
   Existen $q \in X,\ r \in Y$ tales que $a = q + r$ tenemos $b < q + r \implies b - r < q$. Al ser X corte de Dedekind, $b - r \in X \therefore b = \underbrace{(b - r)}_{\in X} + \underbrace{r}_{\in Y} \in X + Y$

3. Supongamos que $q \in X$, $r \in Y$ son tales que $q + r$ es un máximo para $X + Y$ [P.D. q es el máximo para X]
   Sea $a \in X$. Entonces, $a + r \in X + Y$. Como $q + r = \max(X + Y)$ debe tenerse que $a + r \leq q + r \implies a \leq q \therefore q = \max(X)$, lo que contradice que X es un corte de Dedekind . $\therefore X + Y$ no tiene máximo.

4. Como X, Y son cortes de Dedekind existen $a \notin \mathbb{Q}\backslash X,\ b \notin \mathbb{Q}\backslash Y$ [P.D. $a + b \notin X + Y$]
   Sea $q + r \in X + Y$ ($q \in X,\ r \in Y$) note que $a \not\leq q \implies q < a$ y $b \not\leq r \implies r < b \implies q + r < a + b$ e n particular $q + r \neq a + b$. Como $q + r \in X + Y$ fue arbitrario, $\implies a + b \notin X + Y$ y $\therefore X + Y \neq \mathbb{Q}$.

Proposición

Si $X, Y \in \mathbb{R}$,entonces

$$X + Y = Y + X$$

Demostración: $X+Y = \left\{ q + r \,\middle|\, q \in X,\ r \in Y \right\} = \left\{ r + q \,\middle|\, q \in X,\ r \in Y \right\} = Y+X$

Proposición

Dados $X, Y, Z \in \mathbb{R}$ entonces

$$(X + Y) + Z = X + (Y + Z)$$

Demostración:

$$\begin{aligned}
(X + Y) + Z &= \left\{ a + s \,\middle|\, a \in X + Y \text{ y } s \in Z \right\} \\
&= \left\{ (q + r) + s \,\middle|\, q \in X,\ r \in Y,\ s \in Z \right\} \\
&= \left\{ q + (r + s) \,\middle|\, q \in X,\ r \in Y,\ s \in Z \right\} \\
&= \left\{ q + b \,\middle|\, q \in X,\ b \in Y + Z \right\} = X + (Y + Z).
\end{aligned}$$

Proposición

$$E(q + r) = E(q) + E(r)$$

Demostración: Sea $a + b \in E(q) + E(r)$ ($a \in E(q),\ b \in E(r)$) $\implies a < q$ y $b < r \implies a + b < q + r \therefore a + b \in E(q + r) \implies E(q + r) \subseteq E(q) + E(r)$
Recíprocamente, sea $a \in E(q+r)$, entonces $a < q+r \implies a-r < q$. Como $a-r, q \in \mathbb{Q}$ y $\mathbb{Q}$ es denso, entonces existe $c \in \mathbb{Q}$ tal que $a-r < c < q$. Sea $b = a-c < r \therefore b \in E(r)$ además;

$$a - b = a - (a - c) = c < q \implies a - b \in E(q)$$

$\therefore a = (a-b)+b \in E(q)+E(r)$ i.e. $E(q+r) \subseteq E(q)+E(r) \implies E(q)+E(r) = E(q+r)$

Proposición

$$E(0) = \left\{ r \in \mathbb{Q} \;\middle|\; r < 0 \right\}$$

es un neutro aditivo en $\mathbb{R}$.

Demostración: Sea $X \in \mathbb{R}$ arbitrario [P.D. $X + E(0) = X$]
Sea $q+r \in X+E(0)$ $(q \in X,\ r \in E(0)) \implies r < 0 \implies q+r < q+0 \implies q+r < q$.
Al ser X un corte de Dedekind, tenemos que $q + r \in X$. $\therefore X + E(0) \subseteq X$
Por otro lado, sea $q \in X$. Como X no tiene máximo, sea $a \in X$ tal que $q < a$. Entonces, si $r = q - a < 0 \implies r \in E(0)$ y $q - r = q - (q - a) = a \in X$ $\therefore q = (q - r) + r = a + r \in X + E(0)$.

Proposición

Si $X, Y, Z \in \mathbb{R}$ y $X \leq Y$, entonces $X + Z \leq Y + Z$.

Demostración: Sea $q + s \in X + Z$ $(q \in X,\ s \in Z)$ entonces, como $X \subseteq Y \implies q \in Y$
$\therefore q + s \in Y + Z \implies X + Z \subseteq Y + Z$ $\therefore X + Z \leq Y + Z$.

Proposición

Para todo $X \in \mathbb{R}$, existe $Y \in \mathbb{R}$ tal que

$$X + Y = 0 = \left\{ r \in \mathbb{Q} \;\middle|\; r < 0 \right\}$$

Demostración: Dado $X \in \mathbb{R}$, sea

$$Y = \left\{ r \in \mathbb{Q} \;\middle|\; \exists q \notin X \ (r < -q) \right\}.$$

Veamos primero que $Y \in \mathbb{R}$.

1. Como $X \in \mathbb{R}$ $\exists q \in \mathbb{Q} \backslash X$. Sea $r < -q \implies r \in Y \neq \varnothing$
2. Sea $r \in Y$ y $s \in \mathbb{Q}$ tal que $s < r$ [P.D. $s \in Y$].
   Entonces, existe $q \notin X$ tal que
   $$r < -q$$
   $\implies s < -q \implies s \in Y$.
3. Sea $r \in Y$. Entonces hay un $q \notin X$ tal que $r < -q$. Por la densidad de $\mathbb{Q}$, existe $s \in \mathbb{Q}$ tal que $r < s < -q$
   $$\therefore s \in Y \text{ y } r < s.$$
   $\therefore r$ no es un máximo para Y, así que Y no tiene máximo.
4. Sea $a \in X$ arbitrario. Sea $r \in \mathbb{Q}$ tal que $-r \leq a$.[Si $a \geq 0 \implies -a \leq a$ y $r = a$; Si $a < 0$ sea $-a < r$]. Demostremos que $r \notin Y$: Sea $q \in \mathbb{Q} \backslash X$ arbitrario. Entonces
   $$a \leq q \implies -r \leq q \implies r \geq -q,$$
   es decir $\neg(r < -q)$ $\therefore r \notin Y$ y $Y = \mathbb{Q}$.

Resta demostrar que $X+Y=\underbrace{\left\{r\in\mathbb{Q}\;\middle|\;r<0\right\}}_{E(0)}$.

Sea $q+r\in X+Y$ $(q\in X,\ r\in Y)$ entonces, existe $s\notin X$ tal que $r<-s$, además $q<s \implies q+r<s-s\therefore q+r<0 \implies q+r\in E(0)\therefore X+Y\subseteq E(0)$.
Recíprocamente, sea $r\in E(0)$, i.e. $r<0$. Entonces $0<-\frac{r}{2}$, note que debe existir un $q\in X$ tal que $q-\frac{r}{2}\notin X$[De lo contrario tendríamos $X=\mathbb{Q}$]. Como $r<\frac{r}{2}$, entonces

$$r-q<\frac{r}{2}-q=-\left(q-\frac{r}{2}\right)$$

por lo tanto, $r-q\in Y$, entonces,

$$r=q+(r-q)\in X+Y$$

$$\therefore E(0)\subseteq X+Y \implies X+Y=E(0)=\left\{r\in\mathbb{Q}\;\middle|\;r<0\right\}=0$$

Valor absoluto y · en $\mathbb{R}$

Dado $X\in\mathbb{R}$,

1. $|X|=\max\{X,-X\}$
2. Dados $X,Y\in\mathbb{R}$, definimos:

$$X\cdot Y=\begin{cases}\left\{q\in\mathbb{Q}\,\middle|\,q\leq 0\right\}\cup\left\{q\cdot r\;\middle|\;q\in X,\ r\in Y \text{ y } q,r>0\right\} & \text{si } X,Y>0\\ |X|\cdot|Y| & \text{si } X,Y<0\\ -(|X|\cdot|Y|) & \text{si exactamente uno de } X,Y \text{ es } <0\\ 0 & \text{si } X \text{ o } Y=0.\end{cases}$$

Demostremos las propiedades para $X,Y\in\mathbb{R}$ con $X,Y>0$.

Proposición

$$X\cdot Y\in\mathbb{R}$$

Demostración:

1. $\exists q\in X$ con $q>0$ $\exists r\in Y$ con $r>0$

$$\therefore qr>0 \text{ y } qr\in X\cdot Y$$

2. Sea $a\in X\cdot Y$ y $b<a$. Dos casos
   (a) $b\leq 0 \implies b\in X\cdot Y$ por definición
   (b) $0<b$, entonces $0<a$ y $\therefore\exists q\in X,\ r\in Y$ con $q,r>0$ tales que $a=qr$. Como $b<a=qr \implies \frac{b}{r}<q$, lo que implica $\frac{b}{r}\in X \implies b=\left(\frac{b}{r}\right)r\in X\cdot Y$
3. Sea $a\in X\cdot Y$ dos casos

(a) $a \leq 0 \implies$ por 1. tenemos algún $b \in X \cdot Y$ tal que $a < b$.

(b) $a > 0$. Entonces, existen $q \in X,\ r \in Y,\ q, r > 0$ tales que $a = qr$. Como ni X ni Y tienen máximo, existen $q' \in X,\ r' \in Y$ tales que

$$q < q' \text{ y } r < r'$$

$$\implies a = q \cdot r < q' \cdot r' \in X \cdot Y \therefore X \cdot Y \text{ no tiene máximo.}$$

4. Tomamos $q \in \mathbb{Q} \backslash X,\ r \in \mathbb{Q} \backslash Y$ tales que $q, r > 0$. Note que $\begin{matrix} \text{Si } a \in X \implies a < q \\ \text{Si } b \in Y \implies b < r \end{matrix} \therefore a \cdot b < q \cdot r$ para todo $a \cdot b \in X \cdot Y$ también si $c \leq 0 \implies c < q \cdot r \implies q \cdot r$ es cota superior para $X \cdot Y$ por lo tanto, $q \cdot r \notin X \cdot Y$

Proposición

$$X \cdot Y = Y \cdot X$$

Demostración:

$$\begin{aligned} X \cdot Y &= \left\{ q \in \mathbb{Q} \,\middle|\, q \leq 0 \right\} \cup \{ q \cdot r \,|\, q \in X,\ r \in Y \text{ y } q, r > 0 \} \\ &= \left\{ q \in \mathbb{Q} \,\middle|\, q \leq 0 \right\} \cup \{ r \cdot q \,|\, q \in X,\ r \in Y \text{ y } q, r > 0 \} \\ &= Y \cdot X \end{aligned}$$

Proposición (Ejercicio)

$$(X \cdot Y) \cdot Z = X \cdot (Y \cdot Z)$$

Demostración:

$$\begin{aligned} (X \cdot Y) \cdot Z &= \left\{ s \in \mathbb{Q} \,\middle|\, s \leq 0 \right\} \cup \left\{ s \times z \,\middle|\, s \in X \cdot Y,\ z \in Z \text{ y } s, z > 0 \right\} \\ &= \left\{ x \cdot y \in \mathbb{Q} \,\middle|\, x \cdot y \leq 0 \right\} \cup \left\{ (x \cdot y) \cdot z \,\middle|\, x \in X,\ y \in Y,\ z \in Z \text{ y } x, y, z > 0 \right\} \\ &= \left\{ x \cdot y \in \mathbb{Q} \,\middle|\, x \cdot y \leq 0 \right\} \cup \left\{ x \cdot (y \cdot z) \,\middle|\, x \in X,\ y \in Y,\ z \in Z \text{ y } x, y, z > 0 \right\} \\ &= \left\{ x \in \mathbb{Q} \,\middle|\, x \leq 0 \right\} \cup \left\{ x \cdot t \,\middle|\, x \in X,\ t \in Y \cdot Z \text{ y } x, t > 0 \right\} = X \cdot (Y \cdot Z) \end{aligned}$$

Proposición

$$E(1) = \left\{ q \in \mathbb{Q} \,\middle|\, q < 1 \right\}$$

satisface:

$$X \cdot E(1) = X \quad \forall X \in \mathbb{R}$$

Demostración: (Nos concentramos en el caso $X > 0$) Sea $a \in X \cdot E(1)$. Dos casos

1. $a \leq 0 \implies a \in X$

2. $a > 0$, entonces existen $q \in X,\ r \in E(1)$ con $q, r > 0$ tales que

$$a = q \cdot r$$

Como $r < 1 \implies q \cdot r < q \therefore q \cdot r \in X \implies X \cdot E(1) \subseteq X$.

Recíprocamente, sea $a \in X$. Dos casos

1. $a \leq 0 \implies a \in X \cdot E(1)$
2. $a > 0$: Como X no tiene máximo, Sea $b \in X$ tal que $a < b$. Entonces $0 < \frac{a}{b} < 1 \implies \frac{a}{b} \in E(1)$

$$\therefore a = b\left(\frac{a}{b}\right) \in X \cdot E(1) \therefore X \subseteq X \cdot E(1) \implies X = X \cdot E(1)$$

Proposición

Si $X > 0$, existe $Y > 0$ tal que

$$X \cdot Y = 1_{\mathbb{R}} = \left\{ q \in \mathbb{Q} \;\middle|\; q < 1 \right\}$$

Demostración: Sea $Y = \left\{ q \in \mathbb{Q} \;\middle|\; \exists r \notin X \; \left(q < \frac{1}{r} \right) \right\}$ Demostramos que $Y \in \mathbb{R}$

1. Sea $r \notin X$ con $r \neq 0$ y sea $q < \frac{1}{r} \implies q \in Y \therefore Y \neq \varnothing$
2. Sea $q \in Y$ y $a < q$. Entonces $\exists r \notin X$ tal que $q < \frac{1}{r} \implies a < \frac{1}{r} \implies a \in Y$.
3. Sea $q \in Y$. Entonces hay $r \notin X$ tal que $q < \frac{1}{r}$. Sea $a \in \mathbb{Q}$ con $q < a < \frac{1}{r} \implies a \in Y$ Y $q < a$. Como $q \in Y$ fue arbitrario, Y no tiene máximo.
4. Como $X > 0$, existe $q \in X$ con $q > 0$. Afirmamos que $\frac{1}{q} \notin Y$: Si $r \notin X$ $(r>0)$ arbitrario, entonces

$$q < r \implies \frac{1}{r} < \frac{1}{q};$$

en particular $\frac{1}{q} \not< \frac{1}{r} \therefore \frac{1}{q} \notin Y$.

Ahora sea $a \in X \cdot Y$. Dos casos

1. $a \leq 0 \implies a \in 1_{\mathbb{R}}$
2. $a > 0$. Entonces $\exists q \in X$, $r \in Y$ con $q, r > 0$ tales que $a = q \cdot r$. Sea $s \notin X$ tal que $r < \frac{1}{s}$ note que $q < s \implies \frac{1}{q} > \frac{1}{s} > r \therefore a = q \cdot r < 1 \implies a \in 1_{\mathbb{R}} \therefore X \cdot Y \leq 1_{\mathbb{R}}$

Recíprocamente, sea $a \in 1_{\mathbb{R}}$. Dos casos

1. $a \leq 0 \implies a \in X \cdot Y$
2. $a > 0$. Entonces $0 < a < 1$. Sea $t \in \mathbb{Q}$ tal que $a < t < 1$, y sea $q \in X$ tal que $\frac{q}{t} \notin X$. Entonces

$$\frac{1}{q} < \frac{t}{q} = \frac{1}{\frac{q}{t}} \therefore \frac{a}{q} \in Y$$

$$\implies a = q\left(\frac{a}{q}\right) \in X \cdot Y \therefore 1_{\mathbb{R}} \subseteq X \cdot Y \implies X \cdot Y = 1_{\mathbb{R}}$$

Proposición

Si $q, r \in \mathbb{Q}$ entonces,

$$E(qr) = E(q) \cdot E(r)$$

Demostración: [Nos enfocamos en el caso $q, r > 0$] Sea $a \in E(q) \cdot E(r)$. Dos casos

1. $a \leq 0 \implies a \underset{a \leq 0 < qr}{\in} E(qr)$
2. $a > 0 \implies a = b \cdot c$ para $\begin{matrix} b \in E(q) \\ c \in E(r) \end{matrix}$ $b, c > 0$.
   $\implies b < q$ y $c < r \implies a = bc < qr \implies a \in E(qr) \therefore E(q) \cdot E(r) \subseteq E(qr)$.

Recíprocamente, sea $a \in E(qr) \implies a < qr$. Dos casos

1. $a \leq 0 \implies E(q) \cdot E(r)$
2. $0 < a < qr$. Entonces
   $$\frac{a}{r} < q,$$
   al ser $\mathbb{Q}$ denso podemos tomar b tal que
   $$\frac{a}{r} < b < q.$$
   Entonces $b \in E(q)$ además $\frac{a}{r} < b \implies \frac{a}{b} < r \therefore \frac{a}{b} \in E(r) \implies a = b\left(\frac{a}{b}\right) \in E(q)E(r) \therefore E(qr) \subseteq E(q)E(r) \implies E(q)E(r) = E(qr)$.

Proposición:

Si $X, Y \in \mathbb{R}$ y $Z > 0$, entonces

$$X \leq Y \implies X \cdot Z \leq Y \cdot Z$$

Demostración: (Suponemos que $X, Y > 0$) Por hipótesis $X \subseteq Y$. [P.D. $X \cdot Z \subseteq Y \cdot Z$] Sea $a \in X \cdot Z$. Dos casos

1. $a \leq 0 \implies a \in Y \cdot Z$
2. $a > 0$. Entonces hay $q \in X$, $r \in Y$, $q, r > 0$ tales que $a = q \cdot r$. Como $X \subseteq Y \implies q \in Y \therefore a = q \cdot r \in Y \cdot Z \implies X \cdot Z \subseteq Y \cdot Z \therefore X \cdot Z \leq Y \cdot Z$.

Axioma de Elección

Axioma de Elección AE_1

$$\forall \mathscr{X}\Big(\forall X \in \mathscr{X}\ (X \neq \varnothing) \wedge \forall X, Y \in \mathscr{X}\ (X \neq Y \Rightarrow X \cap Y = \varnothing) \Rightarrow \exists S(\forall x \in \mathscr{X}\ \exists! a\ a \in X \cap S)\Big)$$

Informalmente: Para toda familia $\mathscr{X}$ de conjuntos no vacíos, disjuntos a pares, existe un conjunto 'selector' S que contiene exactamente a un elemento de cada X.

Axioma de Elección AE_2

$$\forall \mathscr{X}\Big(\forall X \in \mathscr{X}\ (X \neq \varnothing) \Rightarrow \exists f\ (f \text{ es función } \wedge\ \mathrm{dom}(f) = \mathscr{X}\ \wedge\ (\forall X \in \mathscr{X})\ f(X) \in X\Big)$$

Informalmente: Para toda familia de conjuntos $\mathscr{X}$ no vacíos, existe una 'función de elección' f con dominio en $\mathscr{X}$ tal que para todo conjunto x en la familia $f(X) \in X$

Usamos el axioma de elección en demostraciones de teoremas en distintas ramas de las matemáticas.

Teorema

$$ZF \vdash AE_1 \iff AE_2$$

i.e. Dentro del sistema axiomático de Zermelo-Fraenkel, **se puede demostrar** que AE_1 es equivalente a AE_2.

Demostración: $\Longleftarrow$) Sea $\mathscr{X}$ una familia disjunta de conjuntos no vacíos. [P.D. $\exists S$ selector].

Sea f una función de elección para $\mathscr{X}$. ($\mathrm{dom}(f)=\mathscr{X}$ y $\forall X \in \mathscr{X}\ X \in f(X)$) Afirmamos que $\mathrm{ran}(f) = \left\{ f(X) \,\middle|\, X \in \mathscr{X} \right\}$ es un selector para $\mathscr{X}$.

Para demostrar esto, sea $X \in \mathscr{X}$. Note que $f(X) \in X \cap \mathrm{ran}(f)$. Sea $y \in X \cap \mathrm{ran}(f)$ como $y \in \mathrm{ran}(f)$, existe $Y \in \mathscr{X}$ tal que $y = f(Y)$ entonces $f(Y) \in X \cap Y$ como $\mathscr{X}$ es una familia de conjuntos disjunta $\Longrightarrow$ $X = Y$ y $y = f(Y) = f(X)$ $\therefore f(X)$ es el único elemento de $X \cap \mathrm{ran}(f)$, $\therefore$ $\mathrm{ran}(f)$ es un selector.

$\Longrightarrow$) Sea $\mathscr{X}$ una familia de conjuntos no vacíos. Consideremos

$$\mathscr{Y} = \left\{ X \times \{X\} \,\middle|\, X \in \mathscr{X} \right\}$$

Note que todo elemento de $\mathscr{Y}$ cumple

$$X \times \{X\} = \left\{ (a, b) \,\middle|\, a \in X\ b \in \{X\} \right\} = \left\{ (a, X) \,\middle|\, a \in X \right\}$$

Note que

1. Todo $X \times \{X\} \in \mathcal{Y}$ es no vació

$$X \neq \varnothing \therefore \text{sea } x \in X \implies (x, X) \in X \times \{X\}$$

2. Si $X \times \{X\},\ Y \times \{Y\} \in \mathcal{Y}$ son distintos, entonces son disjuntos.
   Si $(a, b) \in X \times \{X\} \cap Y \times \{Y\} \implies \begin{matrix} b = X \\ b = Y \end{matrix} \implies X = Y$

Por hipótesis AE_1, existe S tal que $\forall X \times \{X\} \in \mathcal{Y}\ \exists!(a, b) \in (X \times \{X\}) \cap S$.
Definimos la función f con dominio $\mathcal{X}$ tal que

$$f(X) = \text{1ra entrada (único elemento } (X \times \{X\}) \cap S))$$

$$f = \left\{ (X, a) \in \mathcal{X} \times \bigcup_{y \in \mathcal{X}} y \;\middle|\; X \in \mathcal{X} \ \wedge\ (a, X) \in S \right\}.$$

Es fácil ver que f es una función de elección.

Lema de Zorn

Lema de Zorn

Sea $\mathbb{P}$ un conjunto y $\leq \subseteq \mathbb{P} \times \mathbb{P}$ una relación de orden parcial en $\mathbb{P}$.
Si toda cadena $\mathcal{C} \subseteq \mathbb{P}$ ($\leq$ es un orden total/lineal en $\mathcal{C}$) tiene una cota superior en $\mathbb{P}$, entonces $\mathbb{P}$ tiene por lo menos un elemento maximal.

Para demostrar teoremas usando el **Lema de Zorn** podemos seguir este esquema

1. Identificar el conjunto $\mathbb{P}$
2. Definir el orden parcial $\leq \subseteq \mathbb{P} \times \mathbb{P}$
3. Verificar la existencia de maximales
4. Mostrar que la cadena $\mathcal{C} \subseteq \mathbb{P}$

Ejemplos de uso del Lema de Zorn

Teorema

Todo espacio vectorial sobre $\mathbb{R}$ tiene una base.

Demostración: Sea V espacio vectorial sobre $\mathbb{R}$, sea

$$\mathbb{P} = \left\{ X \subseteq V \;\middle|\; X \text{ es linealmente independiente.} \right\}$$

Definimos, para $X, Y \in \mathbb{P}$

$$X \leq Y \iff X \subseteq Y.$$

Note que, si $X \in \mathbb{P}$ es maximal $\implies X$ es una base para V. De lo contrario, si X no es base para V, entonces $\text{span}(X) \neq V$ y $\therefore$ existe $v \in V$ tal que $v \notin \text{span}(X)$ $\therefore X \cup \{v\}$ es l.i. $\implies X \cup \{v\} \in \mathbb{P}$ y $X < X \cup \{v\}$ $\therefore X$ no es maximal en $\mathbb{P}$.

Sea $\mathscr{C} \subseteq \mathbb{P}$ una cadena. Sea

$$Z = \bigcup_{X \in \mathscr{C}} X,$$

afirmamos que $z \in \mathbb{P}$. Para ello, sean $v_1, \dots, v_n \in Z$ y $\alpha_1, \dots, a_n \in Z$ tales que $\alpha_1 v_1 + \cdots + \alpha_n v_n = 0$. Para cada i, hay un $X_i \in \mathscr{C}$ tal que $v_i \in X_i$. Al ser $\mathscr{C}$ linealmente ordenado, hay un j tal que $X_i \leq X_j$ para todo i i.e. $X_i \subseteq X_j \therefore v_1, \dots, v_n \in X_j$ como X_j es l.i., concluimos que $\alpha_1 = \alpha_2 = \cdots = \alpha_n = 0 \therefore Z$ es l.i. $\implies Z \in \mathbb{P}$ Como $X \subseteq Z \quad \forall X \in \mathscr{C}$ entonces Z es cota superior para $\mathscr{C}$. $\therefore$ por el Lema de Zorn, existe un elemento maximal $X \in \mathbb{P}$, i.e., X es una base para V.

Teorema

Toda gráfica conexa tiene un árbol generador.

Demostración: Sea G una gráfica con conjunto de aristas E.Sea

$$\mathbb{P} = \left\{ X \subseteq E \;\middle|\; X \text{ induce un árbol.} \right\}$$

Dados $X, Y \in \mathbb{P}$, definimos

$$X \leq Y \iff X \subseteq Y$$

Note que, si $X \in \mathbb{P}$ es maximal, entonces es un árbol generador. De lo contrario, existe un vértice v que no es extremo de ningún elemento de X.

Sea u algún elemento de la gráfica inducida por X, al ser G conexa, sea T una trayectoria de v a u. Sea u' el mínimo elemento de $G[X]$ que aparece en T, y sea T' la subtrayectoria de T que une a v y a u'. Sea $Y = X \cup T'$, entonces Y también es árbol pues no tiene ciclos. $\therefore Y \in \mathbb{P} \therefore X < Y \implies X$ no es maximal.

Sea $\mathscr{C} \subseteq \mathbb{P}$ una cadena, sea

$$Z = \bigcup_{X \in \mathscr{C}} X.$$

Afirmamos que $Z \in \mathbb{P}$, es decir, Z induce un árbol:

Z es conexo: Sean $u, v \in Z$, entonces existen $X, Y \in \mathscr{C}$ tales que $u \in G[X] \quad v \in G[Y]$. Al ser X, Y comparables o bien $X \subseteq Y$ o bien $Y \subseteq X$. Supongamos sin pérdida de generalidad que $X \subseteq Y \implies u, v \in G[Y] \therefore$ hay una trayectoria $T \subseteq Y$ que une a u con v entonces $T \subseteq Z$.

Z es acíclico: Supongamos que $e_1, e_2, e_3, \dots, e_k$ con un extremo de e_1 igual al otro extremo e_k es un ciclo en Z. Para cada i hay un $X_i \in \mathscr{C}$ con $e_i \in X_i$ al ser $\mathscr{C}$ una cadena, hay X_j; tal que $X_i \subseteq X_j \quad \forall i \therefore e_1, e_2 \dots, e_k \in X_j \implies X_j$ tiene un ciclo, contradicción.

Por el Lema de Zorn, hay un $X \in \mathbb{P}$ maximal, es decir, X es un árbol generador.

Teorema

En ZF, el Lema de Zorn implica el axioma de elección.

Demostración: Sea $\mathscr{X}$ una familia de conjuntos no vacíos. Sea

$$\mathbb{P} = \left\{ f \subseteq \mathscr{X} \times \bigcup_{X \in \mathscr{X}} X \;\middle|\; \begin{array}{c} f \text{ es función} \\ \text{y} \\ \forall X \in \operatorname{dom}(f)\ f(X) \in X \end{array} \right\}$$

Note que, si $f \in \mathbb{P}$ maximal, entonces f es una función de elección para $\mathscr{X}$. Pues si f no fuera una función de elección, existiría $X \in \mathscr{X}$ con $X \notin \text{dom}(f)$. Al ser $X \neq \varnothing$, existe $x \in X$. Entonces

$$g = f \cup \{(X, x)\} \in \mathbb{P}$$

y $f < g$, f no es maximal.

Sea $\mathscr{C} \in \mathbb{P}$ una cadena, sea

$$h = \bigcup_{f \in \mathscr{C}} f$$

, y sean (X, x) $(X, y) \in h$. Entonces existen $f, g \in \mathscr{C}$ con $(X, x) \in f$ y $(X, y) \in g$.

Al ser $\mathscr{C}$ una cadena, o bien $f \subseteq g$ o bien $g \subseteq f$. Supongamos sin pérdida de generalidad $f \subseteq g$, entonces (X, x), $(X, y) \in g$. Al ser g una función, concluimos que $x = y$.

Por el Lema de Zorn existe $f \in \mathbb{P}$ maximal, i.e. f es una función de elección para $\mathscr{X}$.

Segmento Inicial y Adecuado

Sea $X \subseteq \mathbb{P}$.

1. $S \subseteq X$ es un segmento inicial si:

$$\forall x \in S \; \forall y \in X \quad y < x \implies y \in S$$

2. X es adecuado si:

   (a) X esta bien ordenado por $\leq$

   (b) Para todo $S \subseteq X$ segmento inicial, si $X \setminus S \neq \varnothing$ entonces

$$\min_{\leq}(X \setminus S) = f\left(\left\{ p \in \mathbb{P} \;\middle|\; \begin{array}{l} p \text{ es cota} \\ \text{superior estricta} \\ \text{para } S \end{array} \right\}\right)$$

Teorema

En ZF, los siguientes son equivalentes

1. AE
2. LZ (Lema de Zorn)
3. WO (Principio del Buen Orden)

Demostración: 3. $\implies$ 1.:
Sea $\mathscr{X}$ una familia de conjuntos no vacíos. Sea

$$Z = \bigcup_{X \in \mathscr{X}} X,$$

y sea $\leq \subseteq Z \times Z$ una relación de buen orden en Z.

Sea

$$f : \mathscr{X} \longrightarrow \bigcup_{X \in \mathscr{X}} X$$

dada por

$$f(X) = \min_{\leq}(X) \in X$$

para todo $X \in \mathscr{X}$

$$\left[f = \left\{ (X, y) \in \mathscr{X} \times \bigcup_{X \in \mathscr{X}} X \;\middle|\; y = \min_{\leq}(X) \right\} \right]$$

, entonces f es una función de elección para $\mathscr{X}$.

1. $\implies$ 2.
Sea $\leq$ una relación de orden parcial en $\mathbb{P} \neq \varnothing$ y supongamos que toda cadena en $\mathbb{P}$ tiene una cota superior en $\mathbb{P}$.

Sea f una función de elección para $\wp(\mathbb{P})\backslash\{\varnothing\}$

$$\forall X \subseteq \mathbb{P},\ X \neq \varnothing\ f(X) \in X$$

Afirmación: Si C, D son conjuntos adecuados, entonces o bien $C \subseteq D$ o bien $D \subseteq C$
Demostración Af.: Supongamos que $C \nsubseteq D$, [P.D. $D \subseteq C$]
entonces $C \backslash D \neq \varnothing$ al ser C bien ordenado, sea $c_0 = \min_{\leq}(C \backslash D)$. Sea $D_0 = \left\{ x \in C \;\middle|\; x < c_0 \right\}$; note que $D_0 \subseteq D$ pues si $x \in D \implies x \in C$;; si $x \notin D \implies c_0 \leq x_{\#_c}$. Afirmamos que D_0 es un segmento inicial de D; en caso de que no, existiría algún $d \in D_0$ y existe $d' \in D$, $d' < d$ tal que $d' \notin D_0$. En particular, $d' < c_0$, $\therefore d' \notin C \implies D' = \left\{ d' \in D \;\middle|\; d' < c_0 \text{ y } d' \notin C \right\} \neq \varnothing$.

Sea $d_0 = \min(D')$ note que: $\left\{ y \in D \;\middle|\; y < d_0 \right\}$ es un segmento inicial de D pero también es un segmento inicial de C: Si $y \in D$ es tal que $y < d_0$, por la minimalidad de $d_0 \implies y \in C$. Además, si $y \in D$ es tal que $y < d_0$ y $x \in C$ con $x < y \implies x < d < d_0 < c_0$, entonces: $x < c_0 \therefore x \in D_0 \subseteq D$ como además $x < d_0$ hemos terminado.

Entonces, al ser C, D adecuados,

$$\min(D \backslash \{ y \in D \mid y < d_0 \}) = d_0$$

$$= f\left(\left\{ p \in \mathbb{P} \;\middle|\; \begin{array}{l} p \text{ es cota} \\ \text{superior para} \\ \{ y \in D \mid y < d_0 \} \end{array} \right\} \right)$$

por otro lado $\min(C \backslash \{ y \in D \mid y < d_0 \})$

$$= f\left(\left\{ p \in \mathbb{P} \;\middle|\; \begin{array}{l} p \text{ es cota superior} \\ \text{para } \{ y \in D \mid y < d_0 \} \end{array} \right\} \right) = d_0 \implies d_0 \in C,$$

contradicción.

$\therefore D_0$ es segmento inicial de D, y también de C. $\therefore$ Como D, C son adecuados, entonces

$$\min(C \backslash D_0) = c_0 = f\left(\left\{ p \in P \;\middle|\; \begin{array}{l} p \text{ es cota superior} \\ \text{de } D_0 \end{array} \right\} \right)$$

además, si $D \backslash D_0 \neq \emptyset$, entonces

$$\min(D \backslash D_0) = f\left(\left\{ p \in \mathbb{P} \;\middle|\; \begin{array}{l} p \text{ es cota superior} \\ \text{de } D_0 \end{array} \right\}\right) = c_0$$

En particular $c_0 \in D$, una contradicción. Esta condición muestra que $D_0 = D$, en particular $D \subseteq C$. De esta forma definiendo $X = \bigcup_{\substack{C \subseteq \mathbb{P} \\ \text{adecuado}}} C$. Tendremos que X es adecuado:

(a) Sea $Y \subseteq X$, $Y \neq \emptyset$, entonces existe $C \in \mathbb{P}$ adecuado tal que $C \cap \mathbb{P} \neq \emptyset$. Sea $x = \min(C \cap Y)$. Afirmamos que $x = \min(Y)$L Si hubiera $y \in Y$, $y < x \implies y \in C'$ para algún $C' \subseteq \mathbb{P}$ adecuado, pero por minimalidad de x, $y \notin C \implies C \nsubseteq C'$ $\therefore C' \subseteq C$ y C' es segmento inicial de C, $\therefore y \in C$, contradicción. $\therefore X = \min(Y)$.

(b) Sea $S \subseteq X$ un segmento inicial de X tal que $X \backslash S \neq \emptyset$. Sea $z \in X \backslash S$: entonces $z \in C$ para algún $C \subseteq \mathbb{P}$ adecuado.

Dado cualquier $s \in S$, existe $D \subseteq \mathbb{P}$ adecuado con $s \in D$.
Casos $\begin{array}{l} D \text{ es segmento inicial de } C \implies s \in C \\ C \text{ es segmento inicial de } D : \text{ como } z \in C \text{ y } s < z \implies s \in C \end{array} \implies S \subseteq C$. Por lo tanto,

$$\min(X \backslash S) = \min(C \backslash S) = f\left(\left\{ p \in \mathbb{P} \;\middle|\; \begin{array}{l} p \text{ es cota} \\ \text{superior de } S \end{array} \right\}\right)$$

$\therefore X$ es adecuado; además para todo $C \subseteq \mathbb{P}$ adecuado, tenemos que $C \subseteq X$.

Supongamos que X tiene una cota superior estricta para $\mathbb{P}$, entonces $X \cup \left\{ f\left(\left\{ p \in \mathbb{P} \;\middle|\; \begin{array}{l} p \text{ es cota superior} \\ \text{estricta de } X \end{array} \right\}\right)\right\}$ también será adecuado, conteniendo propiamente a X, contradicción.

Por lo tanto, si p es cota superior para X, entonces $p \in X$. Si $q > p$, entonces q sería cota superior estricta de X, una contradicción. $\therefore p$ es maximal.
2. $\implies$ 3.
Sea X [P.D. $\exists R \subseteq X \times X$ que es buen orden.]
Sea $\mathbb{P} = \left\{ (A, R) \;\middle|\; \begin{array}{l} A \subseteq X \text{ y} \\ R \subseteq A \times A \text{ es buen orden} \end{array} \right\}$ Dados (A, R), $(B, S) \subseteq \mathbb{P}$ definimos

$$(A, R) \leq (B, S) \text{ ssi } \begin{array}{l} A \subseteq B \\ \text{y} \\ (A, R) \text{ es segmento inicial de } (B, S) \end{array}$$

Si $(A, R) \in \mathbb{P}$ y es maximal, entonces $A = X$: de lo contrario, tomando cualquier $x \in X \backslash A$, tendríamos que, definiendo $\begin{array}{l} B = A \cup \{x\} \\ S = R \cup \{(y, x) \mid y \in A\} \end{array}$ entonces

$$\begin{array}{l} (B, S) \in \mathbb{P} \\ \text{y } (A, R) < (B, S) \end{array}$$

Sea $\mathscr{C}$ una cadena. Hacemos $C = \bigcup_{(A,R) \in \mathscr{C}} A$ y $T = \bigcup_{(A,R) \in \mathscr{C}} R$
$C \supseteq A$ para todo $(A, R) \in \mathscr{C}$ y si algún $(A, R) \in \mathscr{C}$ tenemos $a \in A$ y $x \in C$

con $x < a$ entonces: hay $(B, S) \in \mathscr{C}$ tal que $x \in B$. Como $\mathscr{C}$ es cadena, o bien
A es segmento inicial de $B \implies x \in A$
B segmento inicial de $A \implies x \in A$
$\therefore (A, R)$ es segmento inicial de (C, T). Por lo tanto, (C, T) será cota superior de $\mathscr{C}$ tan pronto como demostremos que $(C, T) \in \mathbb{P}$.

Basta mostrar que T es buen orden sobre C. Sea $X \in C$,

$$X \neq \varnothing.$$

Hay un $(A, R) \in \mathscr{C}$ tal que $X \cap A \neq \varnothing$; sea $a_0 = \min(X \cap A)$.
Afirmamos que $a_0 = \min_T(X)$: de lo contrario, si $b < a_0$ con $b \in X \implies$ existe $(B, S) \in \mathscr{C}$ tal que $b \in B$. Al ser $\mathscr{C}$ una cadena,

$$\text{Dos casos} \quad \begin{array}{l} A \text{ segmento inicial de } B \therefore b \in A \implies b \in A \cap X_{\#_c} \\ B \text{ segmento inicial de } A \implies b \in A \therefore b \in A \cap X_{\#_c} \end{array}$$

$\therefore X$ admite un mínimo $\therefore T$ es un buen orden en $C \implies (C, T) \in \mathbb{P}$ y es cota superior para $\mathscr{C}$.
$\therefore$ por LZ, existe $(A, R) \in \mathbb{P}$ maximal, $\implies A = X \therefore R \subseteq X \times X$ es una relación de buen orden en X.

Nociones de Cardinalidad

Idea de Cantor: Formar parejas entre los elementos de A y los de B de manera biunívoca.

Conjuntos equipotentes

Dados dos A, B decimos que son equipotentes, $A \sim B$, si existe $f : A \to B$ biyectiva.

Ejemplos:

- $\{1, 2, 3\} \sim \{48, 52, 91\}$
- $\mathbb{N} \sim \left\{ m \in \mathbb{N} \;\middle|\; m \text{ es cuadrado perfecto} \right\}$

$$n \longleftrightarrow n^2$$

- $\mathbb{N} \sim \left\{ p \in \mathbb{N} \;\middle|\; p \text{ es primo} \right\}$

$$n \longleftrightarrow n\text{-esimo primo.}$$

- $\mathbb{N} \sim \mathbb{Z} \qquad 0, 1, -1, 2, -2, 3, -3, \ldots$

$$n \longmapsto \begin{cases} 0 & \text{si } n = 1 \\ m & \text{si } n = 2m \\ -m & \text{si } n = 2m + 1 \end{cases}$$

- $\mathbb{R} \sim (0, 1)$

$$x \longmapsto \frac{1}{\pi} \arctan(x) + \frac{1}{2}$$

- $(a,b) \sim (c,d)$

$$x \longmapsto \frac{d-c}{a-b}(a-x)+c$$

Observaciones:

1. $A \sim A$: $\quad id_A : A \to A$
2. $A \sim B \implies B \sim A$

$$f : A \to B \text{ biyectiva} \implies f^{-1} : B \to A \text{ biyectiva}$$

3. $(A \sim B \text{ y } B \sim C) \implies A \sim C$

$$\begin{matrix} f : A \to B \\ g : B \to C \end{matrix} \text{ biyectiva} \implies g \circ f : A \to C \text{ biyectiva.}$$

Nota: Estas observaciones son idénticas a las de una relación de equivalencia, pero $\sim$ no puede ser una relación de equivalencia pues si el conjunto fuese infinito, implicaría que existe un conjunto de todos los conjuntos.

Conjunto Finito e Infinito

Sea A

1. Si $\exists n \in \omega$ tal que $A \sim n$, decimos que A es finito.
2. Si A no es finito, decimos que es infinito.

Teorema

Sea $n \in \omega$ y sea $f : n \to n$. Si f es inyectiva $\implies$ f es suprayectiva.

Demostración: Inducción sobre n

$n = 0$ Se cumple por vacuidad.

Supongamos el enunciado cierto para n, y sea $f : n+1 \longrightarrow n+1$ inyectiva. Hay dos casos:

1. $f(n) = n$; entonces $f(k) < n \quad \forall k \neq n$
   $\therefore f \restriction n : n \to n$ es inyectiva. $\therefore$ por hipótesis de inducción es suprayectiva. $\implies$ f también es suprayectiva

$$\left[\text{Si } k \in n+1 \quad \begin{matrix} k = n \implies f(n) = n \\ k \neq n \implies \exists i \in n \; f(i) = k. \end{matrix}\right]$$

2. $f(n) = k < n$. Entonces sea

$$g : n \longrightarrow n$$

   dada por:

$$g(i) = \begin{cases} f(i) & \text{si } f(i) < k \\ f(i) - 1 & \text{si } f(i) \geq k \end{cases}$$

   Afirmamos que g es inyectiva: pues si $g(i) = g(j)$ dos casos:

$$\begin{matrix} g(i) = g(j) < k \implies f(i) = f(j) \implies i = j \\ g(i) = g(j) \geq k \implies f(i) - 1 = f(j) - 1 \implies i = j \end{matrix}$$

$\therefore$ por hipótesis de inducción, g es suprayectiva sobre n. Demostremos que f es suprayectiva: Sea $l \in n+1$, i.e. $l \leq n$. Hay tres casos

1. $l < k \implies$ como g es suprayectiva, $\exists i \in n$
$$f(i) = g(i) = l$$
2. $l = k$; entonces $f(n) = k = l$
3. $l > k$; entonces $k \leq l - 1 < n$ al ser g suprayectiva $\exists i \in n$
$$f(i) - 1 = g(i) = l - 1 \implies f(i) = g(i) + 1 = l.$$

Corolario

Si $n, m \in \omega$ y $n \neq m$ entonces,

1. $m \nsim m$
2. $n \nsim \omega$
   (En particular, $\omega, \mathbb{N}, \mathbb{Z}$ son infinitos)

Demostración:

1. De lo contrario, si $n < m$ y $n \sim m$, existiría una función biyectiva $f : m \to n \subseteq m$ Entonces $\text{ran}(f) = n \neq m$ pero $f : m \to m$ es inyectiva y $\implies \text{ran}(f) = m$ por el Teorema anterior, contradicción.
2. **Dem. 1** Sea $f : n \to \omega$ inyectiva. Sea $N = \max\{f(0), \dots, f(n-1)\} + 1$ $N \notin \text{ran}(f)$ $\therefore f$ no es suprayectiva.

   Dem. 2 Supongamos $f : \omega \to n$ biyectiva
   $$f \restriction n : n \to n$$
   seria inyectiva $\therefore$ suprayectiva, contradicción.

Corolario

Si A es finito, el $n \in \omega$ tal que $A \sim n$ es único.

Cardinalidad

Si A es finito, definimos
$$|A| = \text{único } n \in \omega \text{ tal que } A \sim n$$

Corolario

$\mathbb{R}$ es infinito

Demostración: De lo contrario, habría un $n \in \omega$ y $f : \mathbb{R} \to n$ biyectiva
$$f \restriction n : n \to n$$
seria inyectiva $\therefore$ suprayectiva, contradicción.

Teorema

Dado un conjunto A, los siguientes son equivalentes

1. A es infinito
2. Existe $f : \mathbb{N} \to A$ inyectiva
3. Existe $B \subsetneq A$ tal que $A \sim B$
4. Existe $f : A \to A$ que es inyectiva pero no suprayectiva.

Demostración: 1. $\implies$ 2.
Supongamos que A es infinito, y sea $h : \mathcal{P}(A)\backslash\{\varnothing\} \to A$ una función de elección. Por el teorema de recursión definimos

$$\begin{aligned} &f : \omega \to A \\ &f(0) = h(A) \\ &f(n+1) = h(A\backslash\{f(0), \dots, f(n)\}) \end{aligned}$$

Note que esto esta bien definido ($A \neq \varnothing$ pues es infinito): Si $A\backslash\{f(0), \dots, f(n)\} = \varnothing$

$$\begin{aligned} &\implies A = \{f(0), \dots, f(n)\} \\ &\implies A \sim n+1; \text{ contradicción.} \end{aligned}$$

$\therefore A\backslash\{f(0), \dots, f(n)\} \neq \varnothing$.

2. $\implies$ 3.
Sea $f : \mathbb{N} \to A$ Sea $B = A\backslash\left\{ f(2n-1) \,\middle|\, n \in \mathbb{N} \right\}$ y sea $g : A \to B$

$$g(a) = \begin{cases} a & \text{si } a \notin \operatorname{ran}(f) \\ f(2n) & \text{Si } a \in \operatorname{ran}(f) \text{ y } a = f(n) \end{cases}$$

g es biyectiva (ejercicio): Sean $a_1, a_2 \in A$ tres casos

1. $a_1, a_2 \notin \operatorname{ran}(f)$ entonces $g(a_1) = a_1$ y $g(a_2) = a_2$ si $g(a_1) = g(a_2) \implies a_1 = a_2$.
2. $a_1 \notin \operatorname{ran}(f)$, $a_2 \in \operatorname{ran}(f)$ entonces $g(a_1) = a_1$ y $g(a_2) = 2n$ para algún n tal que $f(n) = a_2$. Como $a_1 \notin \operatorname{ran}(f)$ pero $a_2 \in \operatorname{ran}(f)$ entonces $g(a_1) \neq g(a_2)$. Este caso no puede ocurrir si $g(a_1) = g(a_2)$
3. $a_1, a_2 \in \operatorname{ran}(f)$ entonces $a_1 = f(n_1)$ y $a_2 = f(n_2)$ para algunos $n_1, n_2 \in \mathbb{N}$

   $$\implies g(a_1) = f(2n_1) \wedge g(a_2) = f(2n_2)$$

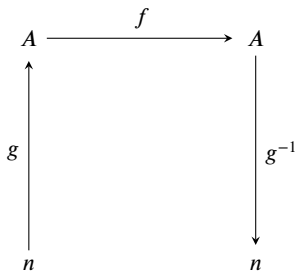
   Si $g(a_1) = g(a_2) \implies f(2n_1) = f(2n_2)$ por hipótesis f es inyectiva i.e. $2n_1 = 2n_2 \implies n_1 = n_2 \therefore a_1 = a_2$. Por lo que g es inyectiva.

Por demostrar g es suprayectiva [$\forall b \in B\ \exists a \in A$ tal que $g(a) = b$]
Dos casos

1. $b \notin \operatorname{ran}(f)$, entonces $b \in A$ y $b \notin \{f(2n-1) \mid n \in \mathbb{N}\}$. Como $b \notin \operatorname{ran}(f)$, por definición de g, $g(b) = b$ entonces $a = b \implies g(a) = b$
2. $b \in \operatorname{ran}(f)$ Sea $a = f(n)$. Entonces $g(a) = f(2n) = b$. Así $a = f(n)$ cumple que $g(a) = b$

3. $\implies$ 4.
Sea $B \subsetneq A$ tal que $A \sim B$, y sea $f : A \to B \subseteq A$ biyectiva. Entonces $f : A \to A$ es inyectiva, pero no suprayectiva ya que $\text{ran}(f) = B \neq A$.

4. $\implies$ 1.
Supongamos que A es finito, y sea $f : A \to A$ inyectiva. Sea $n = |A|$ y sea $g : n \to A$ biyectiva. Entonces $g^{-1} \circ f \circ g : n \to n$ es inyectiva y $\therefore$ es suprayectiva y $\therefore$ biyectiva. Esto implica que f es biyectiva.



Conjunto Numerable

X es numerable si

$$X \approx \mathbb{N} \quad \text{(equivalentemente } X \approx \omega\text{)}$$

$\aleph_0$

Si X es numerable, decimos que

$$|X| = \aleph_0$$

Conjunto no Numerable

X es no numerable si no es numerable.

Ejemplos de conjuntos numerables:

- $\mathbb{N} = \{1, 2, 3, \dots\}$
- $\omega = \{0, 1, 2, \dots\}$
- Pares=$\{2, 4, 6, \dots\}$
- Primos=$\{2, 3, 5, 7, \dots\}$
- $\mathbb{Z} = \{0, 1, -1, 2, -2, 3, -3, \dots\}$

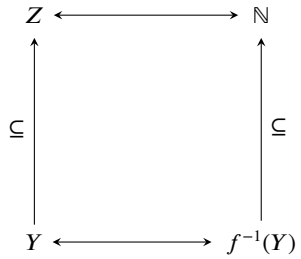
Proposición

Si $X \subseteq \mathbb{N}$ infinito, entonces X es numerable

Demostración: Sea $f : \mathbb{N} \to X$ definida mediante $f(1) = \min(X) \quad f(n+1) = \min(X \setminus \{f(1), \dots, f(n)\})$ es una biyección.

Corolario

Si Z es numerable y $Y \subseteq Z$ es infinito, entonces Y también es numerable.



Proposición

Si A y B son numerables, entonces $A \cup B$ también es numerable.

Demostración: Sea $f : \mathbb{N} \to A$ y $g : \mathbb{N} \to B$ biyectivas, entonces

$$\begin{aligned} h : \mathbb{N} &\to A \cup B \\ h(2n) &= f(n) \\ h(2n-1) &= g(n) \end{aligned}$$

(esto se ve como $A = \{f(1), f(2) \dots\}$, $B = \{g(1), g(2), \dots\}$, $A \cup B = \{g(1), f(1), g(2), f(2), \dots\}$)es una biyección.

Corolario

Si $A_1, \dots, A_n$ son numerables, entonces $\bigcup_{i=1}^{n} A_i$ es numerable.

Demostración: Empleando un argumento inductivo sobre la proposición anterior

$$\bigcup_{i=1}^{n} A_i = \left(\bigcup_{i=1}^{n} A_i \right) \cup A_{n+1}$$

Teorema

Si $\{A_n \mid n \in \mathbb{N}\}$ es una familia de conjuntos numerables, entonces $\bigcup_{n=1}^{\infty} A_n$ también es numerable.

Demostración: **Idea**

$$\begin{array}{lllll} A_1 \to & f_1(1), & f_1(2), & f_1(3), & \cdots \\ A_2 \to & f_2(1), & f_2(2), & f_2(3), & \cdots, \quad f_2(m) \\ A_3 \to & f_3(1), & f_3(2), & f_3(3), & \cdots, \quad f_3(m) \\ \vdots & \vdots & & & \\ A_n \to & f_n(1), & f_n(2), & f_n(3), & \cdots, \quad f_n(m) \end{array}$$

Ahora, si tomamos las diagonales, tenemos las parejas.

$$\begin{array}{l} 1 : (1,1) \\ 2 : (2,1),\ (1,2) \\ 3 : (3,1),\ (2,2),\ (1,3) \\ \vdots \end{array}$$

Considere la función:

$$f : \bigcup_{n=1}^{\infty} A_n \to \mathbb{N}$$

dada por

$$h(f_n(m)) = \frac{(n+m-2)(n-m-1)}{2} + m$$

es una biyección.

Teorema

$\mathbb{Q}$ es numerable.

Demostración: Note que

$$\mathbb{Q} = \dot{\bigcup_{n\in\mathbb{Z}}} \left\{ q \in \mathbb{Q} \;\middle|\; n < q \leq n+1 \right\}$$

y, para cada $n \in \mathbb{Z}$,

$$\left\{ q \in \mathbb{Q} \;\middle|\; n < q \leq n+1 \right\} \underset{q \longmapsto q-n}{\approx} \left\{ q \in \mathbb{Q} \;\middle|\; 0 < q \leq 1 \right\}$$

Por lo tanto, basta demostrar que $\{q \in \mathbb{Q} \mid 0 < q \leq 1\}$ es numerable.

Sea $f : \{q \in \mathbb{Q} \mid 0 < q \leq 1\} \to \mathbb{N}$

$$f\left(\frac{a}{b}\right) = \sum_{n=1}^{b-1} \phi(n) + \left| \left\{ i \;\middle|\; 1 \leq i < a \text{ y } (i,b) = 1 \right\} \right|$$

f es biyectiva, $\therefore \mathbb{N} \approx \{q \in \mathbb{Q} \mid 0 < q \leq 1\} \approx \{q \in \mathbb{Q} \mid n < q \leq n+1\}\ \forall n$
$\therefore \mathbb{Q}$ es la unión numerable de conjuntos contables, $\therefore \mathbb{Q}$ es numerable.

Teorema (Cantor 1891)

$\mathbb{R}$ no es numerable.

Demostración: Supongamos que $f : \mathbb{N} \to \mathbb{R}$ es una función biyectiva. Recursivamente definimos $a_1, a_2, \ldots, a_n, \cdots \in \mathbb{R}$ y $b_1, b_2, \ldots, b_n \cdots \in \mathbb{R}$ tales que

$$a_1 < a_2 < \cdots < a_n < \cdots < b_n < \cdots < b_2 < b_1$$

y además, tales que $f(n) \notin (a_n, b_n)$/ Esto lo hacemos como sigue:

a_1 es cualquier real $> f(1)$
b_1 es cualquier real $> a_1$. Si ya conocemos a_n, b_n. Dos casos

1. $f(n+1) \notin (a_n, b_n)$ entonces a_{n+1} es cualquier real en (a_1, b_n)
   b_{n+1} es cualquier real en (a_{n+1}, b_n)
2. $f(n+1) \in (a_n, b_n)$ entonces a_{n+1} es cualquier real en $(f(n+1), b_n)$
   b_{n+1} es cualquier real en (a_{n+1}, b_n)

Como $\{a_n \mid n \in \mathbb{N}\}$ esta acotado superiormente (por cualquier b_i), Sea $a = \sup\{a_n \mid n \in \mathbb{N}\}$. Entonces, $a \leq b_i$ para todo i, así que sea $b = \inf\{b_n \mid n \in \mathbb{N}\}$

$$\therefore a \leq b \text{ y } [a, b] \subseteq \bigcap_{n=1}^{\infty} (a_n, b_n)$$

Si $c \in [a, b]$, entonces $x \in (a_n, b_n)\ \forall n$

$$\therefore x \neq f(n)\ \forall n \in \mathbb{N}$$

$\Longrightarrow$ f no es suprayectiva, contradicción.

Continuo

Si $X \approx \mathbb{R}$, entonces decimos que X tiene la cardinalidad del continuo, simbolizado

$$|X| = \mathfrak{c}$$

Corolario

Los siguientes conjuntos tienen la cardinalidad del continuo:

1. $(0, 1)$ $\quad \mathbb{R} \to (0, 1)$
   $\quad \frac{1}{\pi} \arctan(x) + \frac{1}{2}$
2. (a, b) $\quad (0, 1) \to (a, b)$
   $\quad t \longmapsto tb + (1 = t)a$
3. $(0, \infty)$ $\quad \mathbb{R} \to (0, \infty)$
   $\quad x \longmapsto e^x$

Orden de cardinalidad

Si A, B son conjuntos, decimos que

1. $A \precsim B$ si existe una función inyectiva
$$f : A \to B$$
Equivalentemente
$$\exists X \subseteq B \quad A \approx X$$
2. $A \prec B$ si
$$A \precsim B \text{ y } A \not\approx B$$

Ejemplos

$$0 \prec 1 \prec 2 \prec \cdots \prec n \prec n+1 \prec \cdots \prec \aleph_0 \prec \mathfrak{c}$$

Proposición

$\precsim$ es reflexiva y transitiva.

Demostración:

1. **Reflexividad:** $id_A : A \to A$
2. **Transitividad:** Si $A \precsim B$ y $B \precsim C$.
$$f : A \to B, \quad g : B \to C \quad \text{inyectivas}$$
entonces $g \circ f : A \to C$ también es inyectiva.

Teorema (Cantor-Bernstein)

$\precsim$ es antisimétrica, es decir, si $A \precsim B$ y $B \precsim A$ implica que $A \approx B$

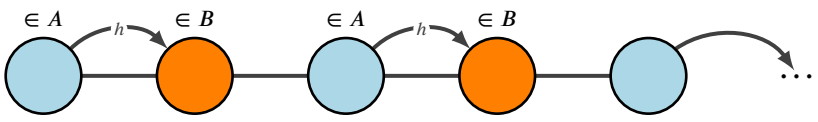
Demostración: Sean $f : A \to B$ y $g : B \to A$. Sea $G = (V, E)$ la gráfica dada por: $V = A \cup B$
$$E = \left\{ \{a, f(a)\} \;\middle|\; a \in A \right\} \cup \left\{ \{b, g(b)\} \;\middle|\; b \in B \right\}$$
Note que todo vértice de G tiene grado 1 o 2.

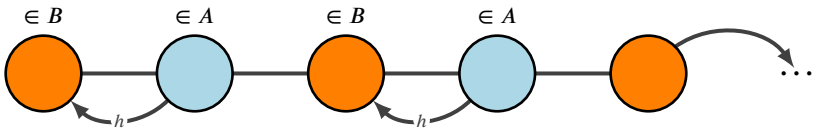
$$\left[\begin{array}{l} \text{Si } a \in A, \text{ al menos } f(a) \text{ es vecino de } a \\ \text{Si } b \in B, \text{ al menos } g(b) \text{ es vecino de } b \end{array} \right] \; d(x) \geq 1$$

$$\left[\begin{array}{l} \text{Si } a \in A, \text{ hay a lo mas un } b \in B \text{ tal que } a = g(b) \\ \text{Si } b \in B, \text{ hay a lo mas un } a \in A \text{ tal que } b = f(a) \end{array} \right] \; d(x) \leq 2$$

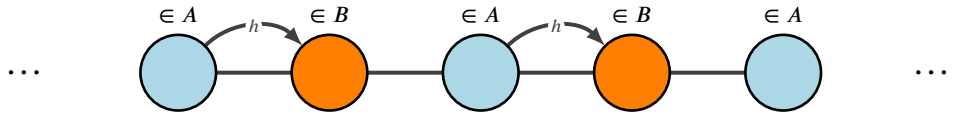
Entonces cada componente conexa puede ser una de las siguientes opciones:

1. Finita de un extremo

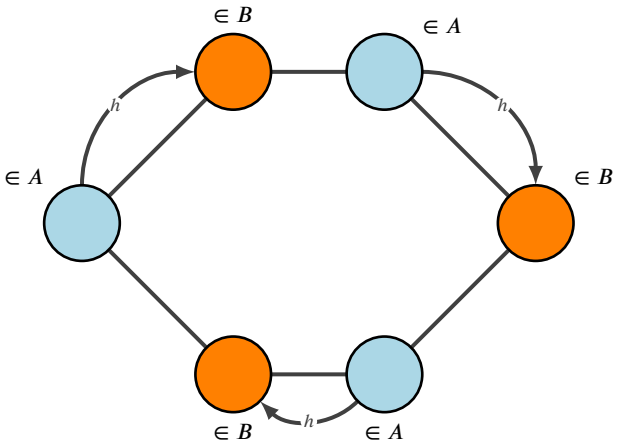




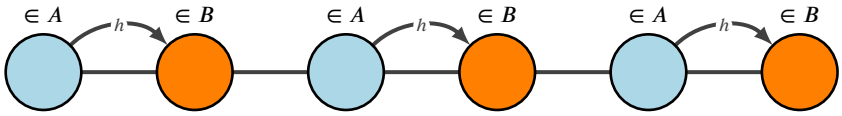
2. Infinita en ambos extremos:



3. Cualquier componente conexa, que sea un ciclo finito, debe ser un ciclo par.



4. Cualquier componente conexa que sea una trayectoria finita debe tener longitud par.



Así definimos $h : A \to B$, y por construcción h es biyectiva. $\therefore A \approx B$

Teorema

$\aleph_0$ es el mínimo cardinal infinito, es decir,

$$\forall X \ (X \text{ infinito} \implies \mathbb{N} \precsim X)$$

Demostración: Ya se demostró.

Teorema

En ZF, las siguientes son equivalentes:

1. AE
2. $\precsim$ es un orden lineal
3. $\precsim$ es un buen orden

Hipótesis del Continuo

No existe ningún A tal que

$$\mathbb{N} \prec A \prec \mathbb{R}$$

Teorema (Gödel, 1939)

En ZFE, es imposible demostrar ¬(Hipótesis del Continuo)

Demostración: La demostración es avanzada.

Teorema (Cohen, 1960)

En ZFE, es imposible demostrar la Hipótesis del Continuo.

Demostración: La demostración es avanzada.

Consecuencias del Teorema de Cantor-Bernstein

Tienen cardinalidad $\mathfrak{c}$: $\mathbb{R}, (0,1), (a,b), (0,\infty)$

$$(a,b) \subseteq [a,b] \subseteq \mathbb{R}$$

$$\mathbb{R} \precsim (a,b) \precsim [a,b] \precsim \mathbb{R} \therefore [a,b] \approx \mathbb{R}$$

(también $[a,b) \approx \mathbb{R}$ y $(a,b] \approx \mathbb{R}$)

$$(0,\infty) \subseteq [0,\infty) \subseteq \mathbb{R}$$

$$\mathbb{R} \precsim (0,\infty) \precsim [0,\infty) \precsim \mathbb{R} \therefore [0,\infty) \approx \mathbb{R}.$$

Corolario

$$|\mathbb{R}\backslash\mathbb{Q}| = \mathfrak{c}$$

Demostración:

$$\mathbb{R} = (\mathbb{R}\backslash\mathbb{Q}) \cup \mathbb{Q} \approx \mathbb{R}\backslash\mathbb{Q}.$$

Aritmética Cardinal

Suma de Cardinalidades

$$|X| + |Y| = |X \cup Y| \quad \text{si } X \cap Y = \varnothing.$$

Ejemplos:

1. $n + \aleph_0 = \aleph_0$
2. Si X es infinito,
$$|X| + \aleph_0 = |X|$$

En general,

$$|X| + |Y| = \max\{|X|, |Y|\}$$

si al menos uno de X, Y es infinito.

Producto de Cardinalidades

$$|X| \cdot |Y| = |X \times Y|$$

Ejemplos:

1. $n \cdot \aleph_0 = \aleph_0$
2. $\aleph_0 \cdot \aleph_0 = \aleph_0$

En general,

$$|X| \cdot |Y| = \max\{|X|,\ |Y|\}$$

si al menos uno de X, Y es infinito.

Antes de introducir la exponenciación nos preguntamos, ¿Cuántas $f : \{1, \dots, n\} \to \{1, \dots, m\}$?

$$\begin{array}{l} f(1) \to m \\ f(2) \to m \\ f(3) \to m \qquad \text{En general } m^n \\ \dots \\ f(n) \to m \end{array}$$

Exponenciación Cardinal

$$|X|^{|Y|} = \left|\left\{ f \in \mathcal{P}(Y \times X) \mid f : Y \to X \right\}\right|$$

Ejemplos:

1. $\aleph_0^{\aleph_0} = |\{f : \mathbb{N} \to \mathbb{N}\}|$
2. $\mathfrak{c}^{\aleph_0} = |\{f : \mathbb{N} \to \mathbb{R}\}|$ (Sucesiones Reales)

Propiedades de la Exponenciación Cardinal

1. $|X|^{|Y|+|Z|} = |X|^{|Y|} \cdot |X|^{|Z|}$
2. $\left(|X|^{|Y|}\right)^{|Z|} = |X|^{|Y| \cdot |Z|}$

Demostración:

1. Si $Y \cap Z = \varnothing$

$$\{f \mid f : Y \cup Z \to X\} \approx \{f \mid f : Y \to X\} \times \{f \mid f : Z \to X\}$$

$$\left.\begin{array}{l} f \longmapsto (f \restriction Y,\ f \restriction Z) \\ g \cup h \longmapsfrom (g, h) \end{array}\right\} \text{ Dos funciones, inversas una de la otra}$$

2.

$$\{f \mid f : Z \to \{g \mid g : Y \to X\}\} \approx \{h \mid h : Y \times Z \to X\}$$
$$z \longmapsto h(-, z) \longmapsfrom h$$
$$f \longmapsto (y, z) \longmapsto f(z)(y)$$

Un caso importante

$$2^{|X|} = |\{f \mid f : X \to \{0, 1\}\}|$$

Función característica

Dado X, definimos

$$\chi_A : X \to \{0,1\}$$

dada por

$$\chi_A(x) = \begin{cases} 1 & \text{si } x \in A \\ 0 & \text{si } x \notin A \end{cases}$$

Teorema

Para todo X,

$$\left|\mathcal{P}(X)\right| = 2^{|X|}, \text{ i.e.,}$$

$$\mathcal{P}(X) \approx \{f \mid f : X \to \{0,1\}\}$$

Demostración: Dado $A \subseteq X$, su función característica es

$$\begin{array}{l} \mathcal{P}(X) \longleftrightarrow \{f \mid f : X \to \{0,1\}\} \\ A \longmapsto \chi_A \\ \{x \in X \mid f(x) = 1\} \longmapsto f : X \to \{0,1\} \end{array}$$

Teorema

$$2^{\aleph_0} = \mathfrak{c},$$

es decir,

$$\mathbb{R} \approx \{f \mid f : \mathbb{N} \to \underset{2}{\{0,1\}}\}$$

Demostración: Sea

$$h : (0,1) \to \{f \mid f : \mathbb{N} \to \{0,1\}\}$$

dado por:

$$h(x) = \text{la función } n \longmapsto n\text{-esimo dígito de } x \text{ en binario}$$

Note que h es inyectiva, pero no suprayectiva.

$$\therefore (0,1) \precsim \{f \mid f : \mathbb{N} \to \{0,1\}\}$$

$$g : \{f \mid f : \mathbb{N} \to \{0,1\}\} \longrightarrow (0,1)$$

$$f \longmapsto \sum_{n=1}^{\infty} \frac{f(n)}{10^n}$$

Entonces g es inyectiva,

$$\therefore \{f \mid f : \mathbb{N} \to \{0,1\}\} \precsim (0,1)$$

Por Cantor-Bernstein

$$\{f \mid f : \mathbb{N} \to \{0,1\}\} \approx (0,1) \approx \mathbb{R}$$

Corolario

$$\mathbb{R} \approx \mathcal{P}(\mathbb{N})$$

Corolario

$$\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0}$$

Demostración:

$$\mathfrak{c}^{\aleph_0} = (2^{\aleph_0})^{\aleph_0} = 2^{\aleph_0 \cdot \aleph_0} = 2^{\aleph_0} = \mathfrak{c}$$

Es decir

$$\{S : \mathbb{N} \to \mathbb{R}\} \approx \mathbb{R}$$

Corolario

$$\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c},$$

es decir,

$$\mathbb{R} \times \mathbb{R} \approx \mathbb{R}$$

Demostración:

$$|\mathbb{R} \times \mathbb{R}| = 2^{|\mathbb{N}|} \cdot 2^{|\mathbb{N}|} = 2^{|\mathbb{N}|+|\mathbb{N}|} = |\mathbb{R}|$$

Corolario

$$\mathbb{R}^n \approx \mathbb{R} \quad \forall n$$

Teorema

Sea $C^0(\mathbb{R}) = \{f : \mathbb{R} \to \mathbb{R} \mid f \text{ es continua}\}$, entonces $C^0(\mathbb{R}) \approx \mathbb{R}$, i.e. $|C^0(\mathbb{R})| \approx \mathfrak{c}$

Demostración:

$$\mathbb{R} \hookrightarrow C^0(\mathbb{R})$$
$$x \mapsto \text{función con valor constante } x$$

$$C^0(\mathbb{R}) \hookrightarrow 2^{\mathbb{Q}}$$
$$f \longmapsto f \restriction \mathbb{Q}$$

(Dado x si $q_n \in \mathbb{Q}$ con $\lim_{n\to\infty} q_n = x$ entonces, $f(x) = \lim_{n\to\infty} f(q_n)$)

$$\therefore f \text{ es inyectiva}$$

$$\therefore C^0(\mathbb{R}) \lesssim 2^{\mathbb{Q}} \approx 2^{\mathbb{N}} \approx \mathbb{R}$$

$\therefore$ Por Cantor-Bernstein

$$\mathbb{R} \approx C^0(\mathbb{R}).$$

Teorema (Cantor)

Para todo X,

$$X \prec \mathcal{P}(X)$$

Demostración: La función

$$\begin{aligned} f \,:\, X &\to \mathcal{P}(X) \\ x &\longmapsto \{x\} \end{aligned}$$

es inyectiva $\therefore X \precsim \mathcal{P}(X)$.

Sea $g : X \to \mathcal{P}(X)$ arbitraria, demostremos que g no es suprayectiva. Sea

$$A = \{x \in X \mid x \notin g(x)\}$$

veamos que $A \notin \operatorname{ran}(g)$: De lo contrario, si $z \in X$ es tal que

$$A = g(z)$$

entonces:

$$\text{casos:} \quad \begin{array}{l} z \in A = g(z) \implies z \notin A \\ z \notin A \implies \neg(z \notin g(z)) \implies z \in g(z) = A \end{array}$$

contradicción. $\therefore g$ no es suprayectiva. $\implies x \not\approx \mathcal{P}(X)$.

Teorema (Paradoja de Cantor)

No existe un conjunto universal.

Demostración: De lo contrario, si V fuera conjunto universal, entonces: $V \precsim \mathcal{P}(V)$ y $\mathcal{P}(V) \subseteq V \implies \mathcal{P}(V) \precsim V \implies V \approx \mathcal{P}(V)$, contradicción.

Hipótesis Generalizada de Cantor (GCH)

$$\forall X, \neg\exists Y \; (X \prec Y \prec \mathcal{P}(X))$$

$$\forall x, \; 2^{\kappa} = \text{mínimo cardinal mayor a } \kappa$$

Teorema (Gödel, 1939)

En ZFE, no es posible demostrar $\neg GCH$.

Teorema (Cohen, 1960)

En ZFE, no es posible demostrar GCH.

Finalmente tenemos el diagrama de infinitos.

$$0 \prec 1 \prec 2 \prec \cdots \prec n \prec n{+}1 \prec \cdots \prec \aleph_0 \prec \aleph_1 \prec \aleph_2 \overset{2^{\aleph_0} \prec 2^{2^{\aleph_0}} \prec 2^{2^{2^{\aleph_0}}} \prec \cdots}{\prec} \ldots \aleph_n \prec \aleph_\omega \prec \aleph_{\omega+1} \prec \ldots \aleph_{\omega+n} \prec \cdots \prec \aleph_{2\omega} \prec \aleph_{2\omega+1} \cdots$$