Estructuras Algebraicas

Diego Rodriguez
Universidad Rey Juan Carlos
Matemáticas + Ingeniería Informática
Curso 2023-2024

26 de mayo de 2024

Parte I
Fundamentos y el principio de inducción

1 Métodos de trabajo en la ciencia

La forma de trabajo depende de la ciencia que se considere:

- En las ciencias experimentales se realizan **experimentos prácticos** y, a partir de resultados particulares obtenidos en ellos, se extraen resultados generales. Esto se llama **método inductivo**.
- En matematicas, se fijan unos axiomas, se definen unos objetos de trabajo (definiciones) y se combinan axiomas para obtener nuevos resultados llamados teoremas. Esto se denomina **método deductivo** (se parte de lo general a lo particular). Sus elementos son:
  - Un axioma es una afirmación cuya veracidad no se cuestiona y en la que se basan el resto de afirmaciones.
  - Una definición es una exposición rigurosa de un concepto y sus propiedades que lo diferencian de otros.
  - Un teorema es un resultado que se deduce, a través de la lógica, de los axiomas y otros teoremas. A continuación delteorema debe aparecer su demostración (si se cumple la hipotesis, deducimos que obligatoriamente se cumple la tesis). Un ejemplo es el siguiente:

    Teorema 1.1 (de Pitagoras)**.** *Si tenemos un triangulo rectangulo cuyos catetos miden a y b y la hipotenusa mide c, entonces* $a^2 + b^2 = c^2$

  - Un teorema sin demostracion no es un teorema, sino una conjetura (ejemplo: Conjetura de Goldbach (1742))

2 Técnicas de demostración

2.1 Demostracion directa

La **demostración directa** consiste en probar la tesis directamente a partir de la hipótesis.

Teorema 2.1. *Si n es un numero entero $n \geq 1$, entonces $n^2 + n$ es par.*

Demostración. Si n es un numero entero $n \geq 1$, hay dos casos:

1. Si n es par, se puede expresar como $n = 2m$ con $m \in \mathbb{Z}$. Así, tenemos:

$$n^2 + n = (2m)^2 + 2m = 4m^2 + 2m = \underbrace{2(2m^2 + m)}_{\text{numero par}}$$

2. Si n es impar, se puede expresar como $n = 2m + 1$ con $m \in \mathbb{Z}$. Así,

$$\begin{aligned} n^2 + n = (2m+1)^2 + (2m+1) = 4m^2 + 4m + 1 + 2m + 1 = \\ = 4m^2 + 6m + 2 = \underbrace{2(2m^2 + 3m + 1)}_{\text{numero par}} \end{aligned}$$

□

2.2 Demostración por contraposición

Si queremos demostrar por contrarreciproco el teorema $A \Rightarrow B$ basta con demostrar el teorema $\neg B \Rightarrow \neg A$ generalmente usando la técnica de demostración directa. Es decir, probamos que lo contrario de la tesis implica lo contrario de la hipótesis.

Teorema 2.2. *Si n es un numero entero de forma que n^2 es impar, entonces n es impar.*

Demostración. Lo demostraremos por contraposición.

Supongamos que n es un número par. Entonces $n = 2c$, $c \in \mathbb{Z}$. Sustituyendo,

$$n^2 = (2c)^2 = 4c^2 = 2(2c^2)$$

Luego n^2 también es un número par. Como $\neg B \Rightarrow \neg A$, se cumple el teorema que queríamos demostrar. □

2.3 Demostracion por reduccion al absurdo

Si queremos demostrar por reduccion al absurdo el teorema $A \Rightarrow B$ basta con que supongamos que se cumpla la hipotesis (A) y lo contrario de la tesis (no B). Si suponemos que se cumple a la vez A y no B haciendo deducciones llegamos a que algo es imposible.

Teorema 2.3. *Si n es un numero entero de forma que n^2 es par, entonces n es par.*

Demostración. Lo demostraremos por reduccion al absurdo. Supongamos que se cumple que n^2 es par y n es impar.

Como n es impar, entonces $n = 2c + 1,\ c \in \mathbb{Z}$ y llegamos a

$$n^2 = (2c+1)^2 = 4c^2 + 4c + 1 = \underbrace{2(2c^2 + c) + 1}_{\text{numero impar}}$$

Luego n^2 es impar, pero por hipótesis hemos supuesto que n^2 es par. Ningún número es impar y par a la vez, por lo que hemos llegado a una contradiccion.

Así tenemos que, si se cumple que n^2 es par, entonces obligatoriamente se cumple que n es par. □

Teorema 2.4. *Existe una cantidad infinita de numeros primos.*

Demostración. En primer lugar, reescribimos el teorema: Si A es el conjunto de todos los numeros primos, entonces su cardinal es infinito.

Lo demostramos por reduccion al absurdo. Suponemos que A es el conjunto de todos los numeros primos y que este conjunto es finito.

Como A es finito el conjunto de todos los numeros primos es $A = \{p_1, p_2, \ldots, p_n\}$. Ahora tomamos

$$x = 1 + p_1 p_2 \cdot \ldots \cdot p_n$$

x es un numero entero (suma y producto de numeros enteros) y no puede ser un numero primo porque es mayor que todos los numeros que pertenecen a A ya que si tomamos p_j en A:

$$x = 1 + \underbrace{p_1 p_2}_{\geq 1} \cdot \ldots \cdot p_j \cdot \ldots \cdot \underbrace{p_n}_{\geq 1} \geq 1 + p_j > p_j$$

Ademas, x no es divisible por ninguno de los primos. Supongamos que x es divisible por p_1. Entonces

$$x = cp_1 = 1 + p_1 p_2 \cdots p_n \Rightarrow 1 = cp_1 - p_1 p_2 \cdots p_n = p_1(c - p_2 \cdots p_n)$$

Por tanto, 1 es múltiplo de p_1. Esto es imposible, pues el 1 solo es múltiplo de si mismo. Esto se repite para el resto de los numeros del conjunto A.

Es decir, x es un numero entero que no es primo y tampoco es divisible por ningun numero primo. Como es imposible, llegamos a que el conjunto de los numeros primos no puede ser finito. □

2.4 Contraejemplos

Los **contraejemplos** no son un método de demostración, sino una técnica para demostrar que un teorema es falso.

Basta con encontrar un caso particular (contraejemplo) en el que se cumplen las hipotesis pero no la tesis para probar que el teorema es falso.

Ejemplo. Pierre de Fermat conjeturó en 1650 que todos los numeros de la forma $F_n = 2^{2^n} + 1$ son primos, cosa que es cierta si $n = 0, 1, 2, 3$ y 4, pero Leonard Euler demostró que si $n = 5$, el numero resultante no es primo. Asi, se demostró que la conjetura anterior era falsa.

3 El principio de inducción matemática

La induccion es un metodo de demostracion basado en uno de los axiomas de los numeros naturales:

Proposición 3.1 (Principio de induccion)**.** *Si P es una propiedad de forma que se cumple simultaneamente:*

- *el numero $n = 1$ cumple la propiedad P.*
- *siempre que un cierto numero $n \in \mathbb{N}$ cumple la propiedad P, el siguiente numero $(n + 1)$ también cumple la propiedad P.*

entonces todos los numeros naturales cumplen la propiedad P.

Este principio nos da una técnica para probar que un teorema es cierto para todos los numeros naturales, que basta con seguir los siguientes pasos:

1. Comprobar que el resultado es cierto para $n = 1$.
2. Suponiendo que el resultado es cierto para un numero natural n (se suele llamar «hipotesis de induccion»), demostramos que necesariamente el resultado tambien es cierto para $n + 1$.

Veamos un ejemplo:

Teorema 3.1. *Demostrar que para cualquier numero natural $n \in \mathbb{N}$ se cumple que*

$$1 + 2 + 3 + \cdots + n = \frac{n(n+1)}{2}$$

Demostración. Lo demostraremos por induccion sobre n . En primer lugar, veamos que se cumple para $n = 1$.

$$1 + 2 + 3 + \cdots + n \overset{n=1}{=} 1 = \frac{1(1+1)}{2} = \frac{n(n+1)}{2}$$

Suponiendo que es cierto para n, tenemos que demostrar que entonces es cierto para $n+1$ y que $1+2+\cdots+n+(n+1)=\dfrac{(n+1)(n+2)}{2}$

$$1+2+3+\cdots+n+(n+1)=\frac{n(n+1)}{2}+(n+1)=$$
$$=\frac{n(n+1)+2(n+1)}{2}=\boxed{\frac{(n+1)(n+2)}{2}}$$

□

Definición 3.1 (Sumatorio y productorio)**.** En las formulas relacionadas con sumas o productos de una sucesion de numeros, se utiliza una notacion especial para evitar ambiguedades: los sumatorios y productos. Esta notacion usa dos letras griegas mayusculas: sigma y pi.

1. Si queremos denotar la suma $a_1+a_2+\cdots+a_n$, en lugar de los puntos suspensivos escribimos
$$\sum_{i=1}^{n} a_i$$
Esta expresion quiere decir que sumamos los elementos de la sucesion (a_i) donde i recorre todos los valores enteros entre $i=1$ e $i=n$.

2. Si queremos denotar el producto $a_1\cdot a_2\cdot\ldots\cdot a_n$ en lugar de los puntos suspensivos escribiremos
$$\prod_{i=1}^{n} a_i.$$
Esta expresion quiere decir que multiplicamos los elementos de la sucesion (a_i) donde i recorre todos los valores enteros entre $i=1$ e $i=n$.

   Un ejemplo es el factorial de n:
$$\prod_{i=1}^{n} i = 1\cdot 2\cdot\ldots\cdot n = n!$$

Ejemplo. Demostrar que para todo $n\in\mathbb{N}$ se cumple que
$$\sum_{i=1}^{n}\frac{1}{k(k+1)}=\frac{n}{n+1}$$

Demostración. Lo demostraremos por induccion sobre n. En primer lugar, comprobamos si se cumple para $n = 1$.

$$\left.\begin{array}{l} \displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = \sum_{k=1}^{1} \frac{1}{k(k+1)} = \frac{1}{1(1+1)} = \frac{1}{2} \\ \displaystyle\frac{n}{n+1} = \frac{1}{1+1} = \frac{1}{2} \end{array}\right\} \Rightarrow \text{ Cierto para } n = 1$$

Ahora, demostramos que si es cierto para n entonces también es cierto para $n + 1$.

La hipotesis de induccion es: $\displaystyle\sum_{k=1}^{n} \frac{1}{k(k+1)} = \frac{n}{n+1}$.

La tesis de induccion es: $\displaystyle\sum_{k=1}^{n+1} \frac{1}{k(k+1)} = \frac{n+1}{n+2}$.

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

Asi, llegamos a que tambien se cumple para $n + 1$. Luego el principio de induccion es cierto para todo $n \in \mathbb{N}$. □

Ejemplo. Probar que si tenemos $r \neq 1$ y $n \in \mathbb{N}$ cualesquiera, entonces

$$1 + r + r^2 + \cdots + r^n = \sum_{j=0}^{n} r^j = \frac{r^{n+1} - 1}{r - 1}$$

Demostración. Lo demostraremos por induccion sobre n (numero natural). Para ello, comprobamos primero si se cumple para $n = 1$.

$$\sum_{j=0}^{n} r^j \overset{n=1}{=} \sum_{j=0}^{1} = 1 + r$$

Por otro lado,

$$\frac{r^{n+1} - 1}{r - 1} = \frac{r^2 - 1}{r - 1} = \frac{(r+1)(r-1)}{r-1} = r + 1 = 1 + r$$

Como se cumple para $n = 1$, supongamos que también se cumple para n y veamos si es cierto para $n+1$: $\sum_{j=0}^{n+1} r^j = \frac{r^{n+2}-1}{r-1}$.

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

$$= \frac{r^{n+1}-1+r^{n+2}-r^{n+1}}{r-1} = \boxed{\frac{r^{n+2}-1}{r-1}}.$$

Hemos llegado a que la proposicion es cierta para $n+1$. Por tanto, se cumple el principio de induccion para todo $n \in \mathbb{N}$ y todo $r \neq 1$. □

Ejemplo. Demostrar que para todo $n \in \mathbb{N}$ se cumple que $2^n \leq (n+1)!$

Demostración. Lo demostraremos por induccion sobre n. En primer lugar, comprobamos si es cierto para $n = 1$.

$$2^n \leq (n+1)! \Rightarrow 2^1 \leq (1+1)! = 2 \leq 1 \cdot 2 = 2 \leq 2$$

Como se cumple para $n = 1$, supongamos que es cierto para n y veamos que tambien se cumple para $n+1$.

$$2^{n+1} = 2^n \cdot 2 \leq (n+1)! \cdot 2$$

Tenemos que probar que $(n+1)! \cdot 2 \leq (n+2)!$

$$(n+1)! \cdot 2 = 1 \cdot 2 \cdot \ldots \cdot (n+1) \cdot 2$$

$$(n+2)! = 1 \cdot 2 \cdot \ldots \cdot (n+1) \cdot (n+2)$$

Como $2 \leq n+2 \Rightarrow (n+1)!2 \leq (n+2)!$.

Entonces, $2^{n+1} \leq (n+2)!$ y se cumple el teorema para todo $n \in \mathbb{N}$. □

Ejemplo. Probar que si $n \in \mathbb{N}$ entonces $2^{2n} + 5$ es un multiplo de 3.

Demostración. Lo probaremos por induccion sobre n. En primer lugar, comprobamos si es cierto para $n = 1$.

$$2^{2n} + 5 \overset{n=1}{=} 2^2 + 5 = 4 + 5 = 9 \Rightarrow \text{ multiplo de 3}$$

Ahora, tendremos que demostrar que si es cierto para n entonces es cierto para $n+1$.

Hipotesis de induccion: $2^{2n} + 5$ es multiplo de 3.

Tesis de induccion: $2^{2(n+1)} + 5$ es multiplo de 3.

En este caso:

$$2^{2(n+1)} + 5 = 2^{2n+2} + 5 = 2^{2n} \cdot 2^2 + 5 = 2^{2n} \cdot 4 + 5 = (2^{2n} + 5) + 2^{2n} \cdot 3 = \\ = 3 \cdot 2^n + 3q = \underbrace{3(2^{2n} + q)}_{\text{multiplo de 3}}$$

Por tanto, por el principio de induccion la formula es valida para todo $n \in \mathbb{N}$. $\square$

4 Extensiones del metodo de induccion matematica

Para probar algunas propiedades relacionadas con numeros enteros y subconjuntos de numeros naturales debemos emplear algunas extensiones del Principio de Induccion, como por ejemplo:

1. Si queremos probar que una cierta propiedad es valida para todo numero natural $n \geq n_0$ (siendo n_0 un numero natural fijo) usando el principio de induccion, debemos seguir los siguientes pasos:

   a) Comprobar que el resultado es cierto para $n = n_0$.

   b) Suponiendo que el resultado es cierto para un numero natural $n \geq n_0$, demostramos que necesariamente el resultado tambien es cierto para $n + 1$.

   Una vez probado esto, habremos demostrado que el resultado es cierto para todo numero natural $n \geq n_0$.

2. Si queremos probar que una cierta propiedades valida para todo numero entero $n \in \mathbb{Z}$ usando el principio de induccion, debemos seguir los siguientes pasos:

   a) Comprobar que el resultado es cierto para $n = 0$.

   b) Suponiendo que el resultado es cierto para un numero natural n, demostramos que necesariamente el resultado tambien es cierto para $n + 1$.

   c) Suponiendo que el resultado es cierto para un numero entero negativo $n \leq 0$, demostramos que necesariamente el resultado tambien es cierto para $n - 1$.

Ejemplo. Demostrar que si $n \in \mathbb{Z}$ entonces $n^3 - n$ es multiplo de 3.

Demostración. Lo demostraremos por induccion sobre $n \in \mathbb{Z}$. Para ello, primero probamos que se cumple para $n = 0$.

$$n^3 - n = 0^3 - 0 = 0 = 3 \cdot 0 \Rightarrow \text{Es multiplo de 3.}$$

Ahora, comprobamos que si vale para n entonces tambien vale para $n + 1$.

$$\begin{aligned}(n+1)^3 - (n+1) = n^3 + 3n^2 + 3n + 1 - n - 1 = n^3 - n + 3n^2 + 3n \overset{\text{H.I.}}{=} \\ = 3q + 3n^2 + 3n = 3(q + n^2 + n) \Rightarrow \text{Es multiplo de 3.}\end{aligned}$$

Por ultimo, demostramos que si es cierto para n entonces tambien lo es para $n - 1$.

$$\begin{aligned}(n-1)^3 - (n-1) = n^3 - 3n^2 + 3n - 1 - n + 1 = n^3 - n - 3n^2 + 3n \overset{\text{H.I.}}{=} \\ = 3q - 3n^2 + 3n = 3(q - n^2 + n) \Rightarrow \text{Es multiplo de 3.}\end{aligned}$$

Por tanto, por el principio de induccion hemos demostrado que se cumple el teorema para todo $n \in \mathbb{Z}$. □

Existe otra extension que se basa en el siguiente principio que se deduce trivialmente del principio de induccion:

Proposición 4.1 (Principio de induccion completa)**.** *Si P es una cierta propiedad de forma que se cumple simultaneamente:*

1. *el numero $n = 1$ cumple la propiedad P y*
2. *siempre que un cierto numero $n \in \mathbb{N}$ de forma que todos los numeros menores o iguales que el cumple la propiedad P, el siguiente numero tambien cumple la propiedad P*

entonces todos los numeros naturales cumplen la propiedad P.

Ejemplo. Vamos a demostrar el teorema fundamental de la aritmetica, que dice que todo numero natural $n > 1$ puede expresarse (de forma unica) como producto de potencias de numeros primos, es decir

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}$$

donde $k \in \mathbb{N}$, $p_1, \ldots, p_k$ son numeros primos y $e_1, \ldots, e_k \in \mathbb{N}$.

Demostración. Lo demostramos por induccion completa sobre n. Para ello, primero comprobamos que el resultado es cierto para $n = 2$.

Como 2 es numero primo, se puede expresar como $2 = 2^1$.

En segundo lugar, demostramos que si $1, 2, 3, \ldots, n$ cumplen la propiedad, entonces $n + 1$ cumple la propiedad. Para verlo, hay dos casos:

1. Si $n+1$ es primo, entonces $n+1 = (n+1)^1$ ($p_1 = n+1$, $e_1 = 1$). Cumple la tesis de induccion.

2. Si $(n+1)$ no es primo, entonces es divisible por algun numero menor que $n+1$, luego $n+1 = s \cdot t$ con s, t numeros enteros entre 1 y n.

   Como s y t son numeros enteros entre 1 y n, usando la hipotesis de induccion $s = p_1^{e_1} \cdot \ldots \cdot p_k^{e_k}$ y $t = q_1^{f_1} \cdot \ldots \cdot q_n^{f_n}$. Por tanto,

$$n+1 = s \cdot t = \underbrace{p_1^{e_1} \cdot \ldots \cdot p_k^{e_k} \cdot q_1^{f_1} \cdot \ldots \cdot q_n^{f_n}}_{\text{Producto de potencias de primos}}$$

La unicidad está demostrada en 7. □

Ejemplo. Ejercicio 8 - Probar que la suma de los cubos de tres numeros naturales consecutivos es multiplo de 9.

Demostración. Debemos probar que $n^3 + (n+1)^3 + (n+2)^3$ es multiplo de 9 para todo $n \in \mathbb{N}$. Lo demostraremos por induccion sobre n.

En primer lugar, comprobamos que es cierto para $n = 1$.

$$n^3 + (n+1)^3 + (n+2)^3 = 1^3 + 2^3 + 3^3 = 1 + 8 + 27 = 36 = 9 \cdot 4$$

Ahora, demostramos que si es cierto para n es cierto para $n+1$.

$$\begin{aligned}(n+1)^3 + (n+2)^3 + (n+3)^3 &= (n+1)^3 + (n+2)^3 + (n^3 + 9n^2 + 27n + 27) = \\ &= n^3 + (n+1)^3 + (n+2)^3 + 9n^2 + 27n + 27 = 9k + 9n^2 + 27n + 27 = \\ &= \boxed{9(k + n^2 + 3n + 3)}\end{aligned}$$

Por el principio de induccion, se cumple para todo $n \in \mathbb{N}$. □

Parte II
Combinatoria

5 Principios basicos

Proposición 5.1 (Principio del producto)**.** *Sea $\mathcal{A}$ una actividad que se puede realizar en $t \geq 2$ pasos secuenciales, de manera que el paso 1 se puede hacer*

de n_1 fofrmas distintas, el paso 2 se puede hacer de n_2 formas distintas, ..., y el paso t se puede hacer de n_t formas distintas.

Entonces el numero de posibles formas de realizar la actividad $\mathcal{A}$ es $n_1 \cdot n_2 \cdots n_t$.

Ejemplo. Sean $B_1, B_2, \ldots, B_t$ conjuntos finitos no vacios.

Calcula $|B_1 \times B_2 \times \cdots \times B_t|$.

$B_1 \times B_2 \times \cdots \times B_t = \{(b_1, b_2, \ldots, b_t) \mid \forall b_i \exists B_i\}$.

Por tanto, habra $|B_1|$ opciones de la primera coordenada, $|B_2|$ opciones de la segunda, ..., $|B_t|$ opciones de la t-esima.

$|B_1 \times B_2 \times \cdots \times B_t| = B_1 \cdot B_2 \cdots B_t$.

Ejemplo. El alfabeto español consta de 27 letras de las cuales 5 son vocales. Cuantas palabras (con o sin sentido) de 7 letras se pueden formar de manera que empiecen por vocal y que nunca tengan dos vocales ni dos consonantes seguidas?

Solucion: se pueden formar $5^4 \cdot 22^3$ palabras.

Ejemplo. Se lanzan simultaneamente dos dados de 6 caras, uno de color rojo y otro de color azul. Despues se suman los resultados. De cuantas formas se puede obtener un resultado total de 10 o mas?

Consideramos varios casos dependiendo de la suma de los dos dados:

- Caso 1: suma 12. Se puede sacar con un 6 en ambos dados (1 forma).
- Caso 2: suma 11. Se puede sacar un 6 en el rojo y 5 en el azul o 6 en el azul y 5 en el rojo (2 formas).
- Caso 3: suma 10. 5 rojo y 5 azul, 4 rojo y 6 azul, 6 rojo y 4 azul (3 formas).

La solucion es $1 + 2 + 3 = 6$ formas de obtener 10 o mas.

Proposición 5.2. *Sea $\mathcal{A}$ una actividad tal que las distintas formas de realizarla son los elementos de un conjunto finito B. Supongamos que B se puede escribir como union de subconjuntos disjuntos dos a dos, es decir,*

$$B = B_1 \cup B_2 \cup \cdots \cup B_t, \text{ y si } i \neq j \text{ entonces } B_i \cap B_j = \varnothing$$

Supongamos tambien que $|B_j| = n_j$.

Entonces el numero de posibles formas de realizar la actividad $\mathcal{A}$ es $n_1 + n_2 + \cdots + n_t$.

(Es decir, $|B| = |B_1 \cup B_2 \cup \cdots \cup B_t| = |B_1| + |B_2| + \cdots + |B_t|$).

Ejemplo. El alfabeto español consta de 27 letras de las cuales 5 son vocales. Cuantas palabras de 4 letras se pueden formar de manera que empiecen por "D" y acaben en consonante o que empiecen por "F" y acaben en vocal?

- Caso 1: $1 \cdot 27^2 \cdot 22$.
- Caso 2: $1 \cdot 27^2 \cdot 5$.

Todos los casos posibles son $27^2 \cdot 22 + 27^2 \cdot 5 = 27^3$ (como son casos disjuntos puedo aplicar la regla de la suma).

Ejemplo. Cuantas palabras de 4 letras se pueden formar de manera que empiecen por "D" o acaben en "F"?

- Caso 1: $1 \cdot 27^3$
- Caso 2: $1 \cdot 27^3$

En este caso, no son disjuntos (por ejemplo, DEEF esta en ambos).

Debemos restar la interseccion, que será $1 \cdot 27^2 \cdot 1 = 27^2$.

La solucion final es $27^3 + 27^3 - 27^2$.

Teorema 5.1. *Sean B, B_1, B_2 conjuntos finitos tales que $B = B_1 \cup B_2$. Entonces*

$$|B| = |B_1| + |B_2| - |B_1 \cap B_2|.$$

Demostración. Trivial. □

Ejemplo. Se lanzan dos dados de 6 caras, uno rojo y otro azul. Despues se suman los resultados. De cuantas formas se puede obtener un resultado total de 4 o mas?

Lo contrario de sacar ≥ 4 es sacar < 4, que es lo mismo que sacar 2 o 3.

Para que sume 2, el azul sera 1 y el rojo 1 (1 forma).

Para que sume 3, hay dos posibilidades: azul 1 y rojo 2, azul 2 y rojo 1.

En total, hay 4 formas. Podemos sacar el numero de opciones de ≥ 4 restando del total ($6 \cdot 6 = 36$). $36 - 3 = 33$.

Proposición 5.3 (Principio del complementario)**.** *Sea $\mathcal{A}$ una actividad tal que las distintas formas de realizarla son los elementos de un conjunto finito B. Supongamos que D es otro conjunto finito tal que $B \subseteq D$ y sabemos que $|D| = n$ y que $|D \setminus B| = m$.*

Entonces el numero de posibles formas de realizar la actividad $\mathcal{A}$ es $n-m$. Es decir, $|B| = |D| - |D \setminus B|$.

Observación. El principio del complementario es un corolario del principio de la suma.

$$|B| + |D \setminus B| = |D| \Rightarrow |B| = |D| - |D \setminus B|.$$

Ejemplo. Cuantas palabras de 6 letras se pueden formar de manera que contengan al menos una vocal?

Como tiene que haber ≥ 1 vocales, lo contrario es que no haya ninguna vocal, que es lo mismo que "todo consonantes". En ese caso, hay 22^6 posibilidades y el total es 27^6.

La solucion sera $27^6 - 22^6$.

Definición 5.1 (Variacion con repeticion)**.** Una variacion con repeticion de m elementos $a_1, a_2, \ldots, a_m$ tomados de k en k es una lista ordenada formada por k elementos (que pueden estar repetidos) elegidos cada uno de ellos entre $a_1, a_2, \ldots, a_m$.

Denotamos como $VR_{m,k}$ al numero de variaciones con repeticion de m elementos tomados de k en k.

Teorema 5.2. *Sean $m, k \in \mathbb{N}$. Entonces*

$$VR_{m,k} = m^k.$$

Demostración. Aplicacion inmediata de la regla del producto. □

En las variaciones con repeticion importa el orden de los elementos, puede haber elementos repetidos y es posible $k < m$ o $k = m$ o $k > m$.

Ejemplo. En una prueba de maraton participan 84 corredores. Se otorga una medalla de oro al primero, una de plata al segundo y una de bronce al tercero. De cuantas formas diferentes pueden quedar repartidas las medallas entre los 84 participantes?

Para el oro, tenemos 84 opciones. Para la plata, hay 83 opciones al no poder repetirse. Para el bronce, hay 82.

Por tanto, la solucion sera $84 \cdot 83 \cdot 82$. Difiere con los ejemplos anteriores al no poder haber repeticiones.

Definición 5.2. Una variacion de m elementos $a_1, a_2, \ldots, a_m$ tomados de k en k es una lista ordenada formada por k elementos distintos elegidos cada uno de ellos entre $a_1, a_2, \ldots, a_m$.

Denotamos como $V_{m,k}$ al numero de variaciones de m elementos tomados de k en k.

$$V_{m,k} = \prod_{j=m-k+1}^{n} j$$

Definición 5.3. Sea $n \in \mathbb{N}$. Se define el factorial de n como

$$n! \coloneqq \prod_{j=1}^{n} j = n \cdot (n-1) \cdot (n-2) \cdots 3 \cdot 2 \cdot 1.$$

Se define $0! \coloneqq 1$.

Teorema 5.3. *Sean $m, k \in \mathbb{N}$ tales que $k \leq m$. Entonces $V_{m,k}$ se puede expresar utilizando factoriales:*

$$V_{m,k} = \frac{m!}{(m-k)!}$$

Las variaciones se caracterizan porque importa el orden de los elementos, los elementos son distintos y necesariamente $k \leq m$.

Ejemplo. En el problema del maraton quiero decir la clasificacion completa. Es una variacion de 84 elementos tomados de 84 en 84: $V_{84,84} = \dfrac{84!}{(84-84)!} = \dfrac{84!}{0!} = \dfrac{84!}{1} = 84!$.

Definición 5.4. Una permutacion de m elementos $a_1, a_2, \ldots, a_m$ es una variacion de esos m elementos tomados de m en m.

Denotamos como P_m al numero de permutaciones de m elementos.

Teorema 5.4. *Sea $m \in \mathbb{N}$. Entonces:*

$$P_m = m!$$

Demostración. Es el resultado que se obtiene viendo una permutacion como una variacion. □

Ejemplo. Cuantas palabras pueden formarse reordenando las letras de la palabra "murcielago"?

Es una permutacion de 10 elementos: $V_{10,10} = P_{10} = 10!$

En las permutaciones importa el orden de los elementos, los elementos son distintos, son ordenaciones de m elementos y es un caso particular de variacion con $m = k$: intervienen todos los elementos.

Ejemplo. La loteria primitiva es un sorteo en el que se usan todos los numeros consecutivos del 1 al 49. Una apuesta consiste en marcar 6 de esos 49 numeros en un boleto. Cuantas apuestas diferentes existen en la loteria primitiva?

Si lo hago como una variacion, varias opciones iguales con diferente orden se consideran distintas.

Cada saco de 6! da una sola apuesta. El numero total de apuestas es el numero total de variaciones dividido entre el numero de variaciones que dan lugar a la misma apuesta:

$$\frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6!} = \frac{V_{49,6}}{P_6} = \frac{\frac{49!}{43!}}{6!} = \frac{49!}{43!6!} = \binom{49}{6}.$$

Definición 5.5. Una combinacion de m elementos $a_1, a_2, \ldots, a_m$ tomados de k en k es una coleccion no ordenada formada por k elementos distintos elegidos cada uno de ellos entre $a_1, a_2, \ldots, a_m$.

Denotamos como $C_{m,k}$ al numero de combinaciones de m elementos tomados de k en k. Una notacion alternativa para $C_{m,k}$ es $\binom{m}{k}$ (numero combinatorio, se lee m sobre k).

Teorema 5.5. *Sean $m, k \in \mathbb{N}$ tales que $k \leq m$. Entonces*

$$C_{m,k} = \frac{m!}{k! \cdot (m-k)!}$$

Demostración. Hay $V_{m,k} = \dfrac{m!}{(m-k)!}$ variaciones de m elementos tomados de k en k

Hay varias variaciones que dan la misma combinacion. ¿Cuantos? $P_k = k!$ que son las distintas formas de permutar los k elementos.

Por tanto, el numero de combinaciones

$$C_{k,m} = \frac{V_{m,k}}{P_k} = \frac{m!}{(m-k)! \cdot k!}$$

□

En las combinaciones, no importa el orden de los elementos, los elementos son distintos y necesariamente $k \leq m$.

Ejemplo. Cuantas palabras pueden formarse reordenando las letras de la palabra "SOCORRO"?

No se puede contar como una variacion porque se puede reordenar de forma distinta y de lugar a la misma palabra.

Para contar contar, vamos a pensar temporalmente que las letras son las 7 distintas. Ahora puedo considerar las permutaciones de estos 7 simbolos distintos: son 7!.

Por ejemplo, cuantas veces va a salir SOOCORR contando como permutaciones de 7 elementos distintos? En este caso, son 12 posibilidades porque hay 3 O y 2 R ($3! \cdot 2! = 12$). 3! son las formas de permutar las O y 2! las formas de permutar las R.

Luego el numero total de palabras que puedo obtener son $\frac{7!}{3!2!} = P_7^{3,2}$ (visto en la siguiente definicion).

Los parametros son el numero total de simbolos y el numero de repeticiones de cada uno (3,2,1,1).

$a_1 = O(n_1 = 3), a_2 = R(n_2 = 2), a_3 = S(n_3 = 1), a_4 = C(n_4 = 1)$.

Definición 5.6. Una permutacion con repeticion de n elementos $a_1, a_2, \ldots, a_m$ donde cada a_i se repite n_i veces es una lista ordenada de n elementos elegidos entre $a_1, a_2, \ldots, a_m$ donde el elemento a_i aparece repetido n_i veces.

Supongamos que $n_i > 1$ siempre que $i \leq k$ y que $n_i = 1$ siempre que $i > k$. Denotamos como $P_n^{n_1,n_2,\ldots,n_k}$ al numero de permutaciones con repeticion de n elementos donde hay k elementos que se repiten $n_1, n_2, \ldots, n_k$ veces respectivamente.

Teorema 5.6. *Sea* $n, n_1, n_2, \ldots, n_k \in \mathbb{N}$ *tales que* $\sum_{i=1}^{k} n_i \leq n$. *Entonces*

$$P_n^{n_1,n_2,\ldots,n_k} = \frac{n!}{\prod_{i=1}^{k} n_i!} = \frac{n!}{n_1! \cdot n_2! \cdots n_k!}$$

Demostración. Extrapolar las ideas del ejemplo que hemos visto. No lo escribimos. □

Ejemplo. De combinaciones con repeticion. Sabemos que la seleccion olimpica española ha obtenido un resultado final de 10 medallas en los ultimos juegos. De cuantas formas pueden estar distribuidas esas medallas entre oro, plata y bronce?

Genero 12 huecos (10 para medallas y 2 para separadores que van a separar las medallas de oro de las de plata y las de plata de las de bronce).

Dos hechos:

1. Hay el mismo numero de medallas posibles que de estructuras con separadores.

2. La estructura queda totalmente determinada si se conoce la posicion de los dos separadores.

De cuantas formas diferentes puedo poner los separadores? Como tengo que elegir los dos huecos para los dos separadores de entre 12 posibles y no importa el orden en el que lo haga:

$$C_{12,2} = \binom{12}{2} = \frac{12!}{2!10!} = \frac{12 \cdot 11}{2}$$

Como seria el caso general?

Hay m elementos $a_1, \ldots, a_m$ ($n = 3$). Hay que elegir k veces pudiendo repetir ($k = 10$).

Para el mismo argumento, necesitamos $m-1$ separadores. Habra $k+m-1$ huecos.

De cuantas formas se pueden elegir los huecos de los separadores? $\binom{k+m-1}{m-1} = \binom{k+m-1}{k}$.

Definición 5.7. Una combinacion con repeticion de m elementos $a_1, \ldots, a_m$ tomados de k en k es una coleccion no ordenada formada por k elementos (que pueden estar repetidos) elegidos cada uno de ellos entre $a_1, \ldots, a_m$.

Denotamos como $CR_{m,k}$ al numero de combinaciones de elementos tomados de k en k.

Teorema 5.7. *Sean $m, k \in \mathbb{N}$. Entonces*

$$CR_{m,k} = \binom{m+k-1}{m-1} = \frac{(m+k-1)!}{(m-1)! \cdot k!}.$$

6 Numeros combinatorios

Definición 6.1. Se amplia la definicion de numero combinatorio al caso $k = 0$ como

$$\binom{m}{0} := 1.$$

Triangulo de Pascal. El numero de una fila es la suma de los dos numeros superiores.

Teorema 6.1 (Simetria del triangulo de Pascal)**.** *Sean* $m \in \mathbb{N}$, $k \in \mathbb{N} \cup \{0\}, k \leq m$. *Entonces:*

$$\binom{m}{k} = \binom{m}{m-k}.$$

Demostración. Demostracion analitica con la formula.

$$\binom{m}{k} = \frac{m!}{(m-k)!k!}$$

$$\binom{m}{m-k} = \frac{m!}{(m-(m-k))!(m-k)!} = \frac{m!}{(m-k)!k!}.$$

□

Demostración. Demostracion con combinatoria.

$$\binom{m}{k} = \text{ las formas de elegir } k \text{ elementos de entre } m \text{ posibles.}$$

$$\binom{m}{m-k} = \text{ las formas de elegir } m-k \text{ elementos de entre } m \text{ posibles.}$$

Cada eleccion de k elementos lleva implicita una eleccion de $m-k$ elementos (el complementario del conjunto elegido). Por tanto, hay las mismas formas de elegir k elementos que de $m-k$. Luego

$$\binom{m}{k} = \binom{m}{m-k}.$$

□

Teorema 6.2 (Calculo iterativo de los numeros combinatorios)**.** *Sean* $m \in \mathbb{N}$, $k \in \mathbb{N} \cup \{0\}, k < m$. *Entonces:*

$$\binom{m+1}{k+1} = \binom{m}{k} + \binom{m}{k+1}$$

Demostración. Demostracion analitica.

$$\binom{m}{k} + \binom{m}{k+1} = \frac{m!}{(m-k)!k!} + \frac{m!}{(m-k-1)!(k+1)!} =$$
$$= \frac{m!(k+1)}{(m-k)!k!(k+1)} + \frac{m!(m-k)}{(m-k)(m-k-1)!(k+1)!} =$$
$$= \frac{m!(k+1)}{(m-k)!(k+1)!} + \frac{m!(m-k)}{(m-k)!(k+1)!} = \frac{m!(m+1)}{(m-k)!(k+1)!} =$$
$$= \boxed{\frac{(m+1)!}{(m-k)!(k+1)!}}.$$

□

Demostración. Demostracion combinatoria. Hecha en clase. □

Teorema 6.3 (Binomio de Newton)**.** *Sean $a, b \in \mathbb{R}$, $n \in \mathbb{N}$. Entonces:*

$$(a+b)^n = \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j}.$$

Demostración. Lo demostraremos por induccion sobre n. En primer lugar, comprobamos si se cumple para $n = 1$:

$$\sum_{j=0}^{1} \binom{1}{j} a^j b^{1-j} = \binom{1}{0} a^0 b^1 + \binom{1}{1} a^1 b^0 = b + a = (a+b)^1$$

Suponemos que se cumple para n y veamos si tambien para $n+1$. Es decir, $(a+b)^{n+1} = \sum_{j=0}^{n+1} \binom{n+1}{j} a^j b^{n+1-j}$ (tesis de induccion).

$$(a+b)^{n+1} = (a+b)^n \cdot (a+b) \overset{H.I.}{=} \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j} \cdot (a+b) =$$

$$= a\sum_{j=0}^{n} a^j b^{n-j} + b\sum_{j=0}^{n} a^j b^{n-j} = \sum_{j=0}^{n} \binom{n}{j} a^{j+1} b^{n-j} + \sum_{j=0}^{n} \binom{n}{j} a^j b^{n-j+1} =$$

$$= \binom{n}{n} a^{n+1} b^0 + \sum_{j=0}^{n-1} \binom{n}{j} a^{j+1} b^{n-j} + \sum_{j=1}^{n} \binom{n}{j} a^j b^{n-j+1} + \binom{n}{0} a^0 b^{n+1} =$$

$$= \binom{n}{n} a^{n+1} b^0 + \sum_{j=1}^{n} \binom{n}{j-1} a^j b^{n-(j-1)} + \sum_{j=1}^{n} \binom{n}{j} a^j b^{n-j+1} + \binom{n}{0} a^0 b^{n+1} =$$

$$= \binom{n}{n} a^{n+1} b^0 + \sum_{j=1}^{n} \left(\binom{n}{j-1} a^j b^{n-(j-1)} + \binom{n}{j} a^j b^{n-j+1} \right) + \binom{n}{0} a^0 b^{n+1} =$$

$$= \binom{n}{n} a^{n+1} b^0 + \sum_{j=1}^{n} \left(\left(\binom{n}{j} + \binom{n}{j-1} \right) a^j b^{n+1-j} \right) + \binom{n}{0} a^0 b^{n+1} =$$

$$= \boxed{\sum_{j=0}^{n+1} \binom{n+1}{j} a^j n^{n+1-j}}.$$

□

Teorema 6.4 (Suma de una fila del triangulo de Pascal)**.** *Sea $n \in \mathbb{N}$. Entonces:*

$$\sum_{j=0}^{n} \binom{n}{j} = 2^n.$$

Demostración. Lo demostramos con el binomio de Newton con $a = 1$ y $b = 1$.

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

Existe una demostracion alternativa al teorema usando combinatoria.

Supongamos que A es un conjunto con n elementos. Si pensamos en todos los subconjuntos posibles de A, sabemos que hay 2^n (demostrado en Logica).

Lo divido en casos:

1. Conjuntos con 0 elementos. $1 = \binom{n}{0}$
2. Conjuntos con 1 elemento. $\binom{n}{1}$

3. Conjunto con 2 elementos. $\binom{n}{2}$

n. Conjunto con n elementos. $\binom{n}{n}$

Luego $2^n = \binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n}$ □

Parte III
Aritmética entera y modular

7 Divisibilidad en $\mathbb{Z}$. Algoritmo de Euclides.

Definición 7.1. Sea $\mathbb{R}$ el conjunto de los numeros reales. Dado $a \in \mathbb{R}$, se define el valor absoluto de a como

$$|a| := \begin{cases} a \text{ si } a \geq 0 \\ -a \text{ si } a < 0 \end{cases}$$

Proposición 7.1. $\forall a, b \in \mathbb{R}$ *se cumple*

1. $|a + b| \leq |a| + |b|$ *(desigualdad triangular)*
2. $|a \cdot b| = |a| \cdot |b|$

Demostración. Demostrar por nuestra cuenta (facil). □

Definición 7.2 (Cotas superiores e inferiores, maximos y minimos)**.** Sea A un conjunto no vacio de una relacion de orden que denotaremos $\leq$. Sea $B \subseteq A$.

- $a \in A$ es cota superior de B si $\forall b \in B \quad b \leq a$.
- $a \in A$ es cota inferior de B si $\forall b \in B \quad a \leq b$.
- Si b es una cota superior de B y ademas $b \in B$, decimos que b es el maximo de B.
- Si b es una cota inferior de B y ademas $b \in B$, decimos que b es el minimo de B.

Ejemplo. Sea $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ el conjunto de los numeros enteros, dotado de la relacion de orden habitual que denotaremos $\leq$.

- $B = \{-1, 1, 3, 5\} \subseteq \mathbb{Z}$.
  - $-8, -5, -4, -1$ son ejemplos de cotas inferiores de B.
  - -1 es el minimo de B.
  - $5, 6, 9, 43$ son ejemplos de cotas superiores de B.
  - 5 es el maximo de B.
- $B = \mathbb{N} = \{1, 2, 3, 4, 5, \ldots\} \subseteq \mathbb{Z}$
  - $-8, -1, 0, 1$ son ejemplos de cotas inferiores de B.
  - 1 es el minimo de B.
  - B no esta acotado superiormente.
  - B no tiene maximo.

Proposición 7.2. *En $\mathbb{Z}$ se cumple que:*

- *Todo conjunto no vacio y acotado inferiormente tiene minimo.*
- *Todo conjunto no vacio y acotado superiormente tiene maximo.*

Demostración. Obvio. □

Ejemplo. Este resultado no es cierto en otros conjuntos ordenados. Por ejemplo $\mathbb{Q}$:

- Sea $B = (1, 3) \cap \mathbb{Q} := \{x \in \mathbb{Q} \mid 1 < x < 3\}$.
- $-3, 0, \frac{1}{2}, 1$ son ejemplos de cotas inferiores.
- B no tiene minimo. 1 es el infimo de B.
- $3, \frac{8}{3}, 9, 27$ son ejemplos de cotas superiores.
- B no tiene maximo.

Teorema 7.1 (de la división entera)**.** *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen $q, r \in \mathbb{Z}$ que cumplen*

1. $a = bq + r$
2. $0 \leq r \leq |b|$

Ademas q y r son los unicos enteros que cumplen simultaneamente las dos condiciones anteriores.

Demostración. No demostrada en clase. □

Ejemplo.

1. $a = 27, \quad b = 5$
   $q = 5, \quad r = 2$
   $0 \leq 2 \leq 5$
2. $a = -27, \quad b = 5$
   $q = -5$
   $-27 = (-5) \cdot 5 + (-2)$ X
   $-27 = \underbrace{(-6)}_{q} \cdot 5 + \underbrace{3}_{r}$
3. $a = 27, \quad b = -5$
   $27 = (-5)(-5) + 2$
   $q = -5, \quad r = 2$
4. $a = -27, \quad b = -5$
   $-27 = (-5) \cdot 6 + 3$
   $q = 6, \quad r = 3$

Definición 7.3 (Divisor, multiplo)**.** Sean $a, b \in \mathbb{Z}$. Decimos que b es divisor de a si existe $q \in \mathbb{Z}$ tal que $a = bq$.

Decimos tambien que b divide a a o que a es multiplo de b.

Notacion: $a|b$

Proposición 7.3 (Propiedades de la relacion de divisibilidad)**.** $\forall a, b, c, d, e \in \mathbb{Z}$ *se cumple*

1. $a \mid 0$
2. $a \neq 0 \Rightarrow 0 \nmid a$
3. $a|b, b|c \Rightarrow a|c$
4. $a|a,\ 1|a,\ -a|a,\ -1|a$
5. $a|b, c|d \Rightarrow ac|bd$

6. $a|b \Rightarrow a|bd$
7. $c \neq 0 \Rightarrow (a|b \Leftrightarrow ac|bc)$
8. $a|b, a|c \Rightarrow a|bd + ce$
9. $a|b, b \neq 0 \Rightarrow |a| \leq |b|$
10. $a|b, b|a \Rightarrow |a| = |b|$

Demostración.

1. $\forall a \in \mathbb{Z} \;\; a \mid 0$?

$$0 = 0 \cdot a \Rightarrow a \mid 0$$

2. Supongamos que $0 \mid a \Rightarrow \exists n \in \mathbb{Z}$ tal que $a = 0 \cdot n = 0$, pero tenemos que $a = 0$. Hemos llegado a una contradiccion, luego $0 \nmid a$ (revisar)
3. $a \mid b \Rightarrow \exists n \in \mathbb{Z}$ tal que $b = q \cdot n$

   $b \mid c \Rightarrow \exists m \in \mathbb{Z}$ tal que $c = b \cdot m$.

   $c = b \cdot m = q \cdot n \cdot m \Rightarrow a \mid c$
4. $a = 1 \cdot a \Rightarrow 1|a, a|a$

   $a = (-1)(-a) \Rightarrow -1 \mid a, -a \mid a$
5. $a|b \Rightarrow \exists n \in \mathbb{Z}$ tal que $b = a \cdot n$

   $c|d \Rightarrow \exists m \in \mathbb{Z}$ tal que $d = c \cdot m$

   $b \cdot d = a \cdot n \cdot c \cdot m \Rightarrow ac \mid bd$
6. $a|b \Rightarrow a|bd$

   Tomo $c = 1$ en 5) y obtengo el resultado.
7. $c \neq 0$

   a) $a|b \Rightarrow ac|bc$

   $$\begin{cases} a|b \\ c|c \end{cases} \overset{5)}{\Rightarrow} ac|bc$$

   b) $ac|bc \Rightarrow \exists m \in \mathbb{Z}$ tal que $bc = acm \Rightarrow b = a \cdot m \Rightarrow a|b$.

8. $a|b \Rightarrow \exists m \in \mathbb{Z}$ tal que $b = a \cdot m$

   $a|c \Rightarrow \exists n \in \mathbb{Z}$ tal que $c = a \cdot n$

   $bd + ce = a \cdot m \cdot d + a \cdot n \cdot e = a(md + ne) = a(md + ce)$

9. $a|b \Rightarrow \exists m \in \mathbb{Z}$ tal que $b = a \cdot m$

   Tomo valor absoluto: $|b| = |a \cdot m| = |a| \cdot |m| \geq |a|$

   Como $b \neq 0$, $m \neq 0$ y $|m| \geq 1$

10. Supongamos que $a|b$ y $b|a$.

    Caso 1 Si $a = b = 0 \Rightarrow |a| = |b|$

    Caso 2 Si $a \neq 0, b \neq 0$

    Por 4, $a|b \Rightarrow |a| \leq |b|$, $b|a \Rightarrow |b| \leq |a|$. Luego $|a| = |b|$.

    Obs: no puede pasar $a = 0, b \neq 0$ o $a \neq 0, b = 0$ por (2).

□

Corolario 7.1. *La relacion de divisibilidad es una relacion de orden parcial en* $\mathbb{N}$.

Definición 7.4 (Numero primo)**.** Sea $n \in \mathbb{N}, n \geq 2$. Decimos que n es primo si sus unicos divisores positivos son 1 y n. En caso contrario decimos que n es compuesto.

Teorema 7.2. *Sea* $n \in \mathbb{N}, n \geq 2$. *Se cumple*

$$n \text{ es compuesto} \Leftrightarrow \exists d \text{ divisor de } n \text{ tal que } 2 \leq d \leq \sqrt{n}$$

Demostración. $\Leftarrow$) Obvio. Si hay algun divisor $2 \leq d \leq \sqrt{n} \Rightarrow d \neq 1, d \neq n \Rightarrow n$ es compuesto.

$\Rightarrow$) n compuesto $\Rightarrow \exists d_1$ divisor positivo de n tal que $d_1 \neq 1, d_1 \neq n$.

Como d_1 es divisor de $n \Rightarrow \exists d_2 \in \mathbb{N}$ tal que $n = d_1 \cdot d_2$.

Sabemos que $d_1 \geq 2$. Tambien $d_2 \geq 2$ (porque, si no, d_1 seria n).

Lo demostramos por reduccion al absurdo. Supongamos que ambos, tanto d_1 como d_2 son mayores que $\sqrt{n}$:

$$n = d_1 \cdot d_2 > \sqrt{n} \cdot \sqrt{n} = n$$

Esto es una contradiccion. Luego uno de los dos es menor o igual que $\sqrt{n}$. □

Teorema 7.3 (Teorema fundamental de la aritmetica)**.** *Sea* $n \in \mathbb{N}$, $n \geq 2$. *Entonces n se puede escribir de manera unica (salvo el orden de los factores) como producto de factores primos. Mas formalmente:*

- *Existencia:* $\exists p_1, p_2, \ldots, p_k$ *primos tal que* $n = p_1 p_2 \cdots p_k$
- *Unicidad: Si* $n = p_1 p_2 \cdots p_k$ *y* $n = q_1 q_2 \cdots q_m$ *donde los* p_j *y* q_j *son primos, entonces:*
  - $k = m$
  - *Se pueden reordenar los factores de manera que* $\forall j \; p_j = q_j$

Demostración. La existencia se puede demostrar por induccion completa, como vimos en la demostración (4).

La unicidad se demuestra más adelante. □

Teorema 7.4. *Hay infinitos numeros primos.*

Demostración. Demostrado en (2.4). □

Definición 7.5 (Maximo comun divisor)**.** Sean $a, b \in \mathbb{Z}$ con $(a, b) \neq (0, 0)$. Se define el maximo comun divisor de a y b como el mayor divisor comun positivo de a y b.

Notacion: m.c.d.(a, b).

Por definicion se adopta m.c.d.$(0, 0) := 0$.

Proposición 7.4 (Existencia m.c.d)**.** $\forall a, b \in \mathbb{Z}$ *existe* m.c.d.(a, b).

Demostración. Sea $D = \{n \in \mathbb{N} \mid n \text{ es divisor comun de } a \text{ y } b\}$.

Supongamos, sin perdida de generalidad, que $a \neq 0$. Todos los elementos de D son $\leq |a|$.

Luego $|a|$ es una cota superior de D. Por tanto D tiene maximo.

Ese numero es el maximo comun divisor de a y b.

Observacion: Estamos usando que $D \neq 0$ porque $1 \in D$. □

Definición 7.6. Sean $a, b \in \mathbb{Z}$. Decimos que a y b son relativamente primos entre si o coprimos si m.c.d.$(a, b) = 1$.

Proposición 7.5.

1. $\forall a \in \mathbb{Z} \quad \text{m.c.d.}(a, 0) = |a|$
2. $\forall a, b \in \mathbb{Z} \quad \text{m.c.d.}(a, b) = \text{m.c.d.}(|a|, |b|)$
3. $\forall a, b \in \mathbb{N} \quad 1 \leq \text{m.c.d.}(a, b) \leq \min(a, b)$

Demostración.

1. $|a|$ es el divisor mas grande de a y ademas $|a|$ divide a $0 \Rightarrow$ m.c.d.$(a, 0) = |a|$

2. Es porque los divisores positivos de a son los mismos que los divisores positivos de b.

3. Se debe a que los divisores de un numero positivo son menores o iguales que ese numero.

□

Proposición 7.6. *Sean $a, b \in \mathbb{N}$. Sea r el resto de la division entera de a entre b. Entonces*

$$\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r)$$

Demostración. $a, b \in \mathbb{N}$, r es el resto de la division $a = bq + r$ y $a < r < b$.

Vamos a considerar $D_1 = \{d_1 \in \mathbb{N} \mid d_1 \text{ es divisor comun de a y b}\}$ y $D_2 = \{d_2 \in \mathbb{N} \mid d_2 \text{ es divisor comun de b y r}\}$.

Vamos a ver que $D_1 = D_2$.

$\subseteq$) Sea $d \in D_1 \Rightarrow d_1$ es divisor de a y $b \Rightarrow \exists m, n \in \mathbb{N}$ tal que $a = m \cdot d$ y $b = n \cdot d$.

Entonces $r = a - bq = m \cdot d - n \cdot d \cdot q \Rightarrow d(m - nq) \Rightarrow d|r$

Como tambien $d|b$, $d \in D_2$.

$\supseteq$) Sea $d \in D_2 \Rightarrow d|b$ y $d|r \Rightarrow \exists m, n \in \mathbb{N}$ tal que $b = d \cdot m,\ r = d \cdot n$.

Luego $a = bq + r = d \cdot q + d \cdot r = d(mq + n) \Rightarrow d|a$. Como tambien $d|b$, $d \in D_1$.

Como $D_1 = D_2 \Rightarrow \text{m.c.d.}(a, b) = \text{m.c.d.}(b, r)$ □

Ejemplo. Calcular el m.c.d. de 250 y 32.

$250 = 32 \cdot 7 + 26$

$\text{m.c.d.}(250, 32) = \text{m.c.d.}(32, 26)$

$32 = 26 \cdot 1 + 6$

$26 = 6 \cdot 4 + 2$

$6 = 2 \cdot 3 + 0$

$\text{m.c.d.}(32, 26) = \text{m.c.d.}(26, 6) = \text{m.c.d.}(2, 0) = 2$

Teorema 7.5 (Algoritmo de Euclides)**.** *Sean $a, b \in \mathbb{N}$ con $a > b$. Consideramos la siguiente sucesion construida recursivamente:*

- $r_0 \coloneqq a$
- $r_1 \coloneqq b$
- *Sea $k \geq 2$. Supongamos que ya hemos construido todos los elementos de la sucesion hasta r_{k-1}. Si $r_{k-1} > 0$ construimos r_k como el resto de la division entera de r_{k-2} entre r_{k-1}*

  (es decir, tal que $r_{k-2} = r_{k-1}q_k + r_k$ para algun $q_k \in \mathbb{N}$ y $0 \leq r_k \leq r_{k-1}$)

Entonces se cumple:

- $\exists n \in \mathbb{N} \mid r_n = 0$
- $\text{m.c.d.}(a, b) = r_{n-1}$

Demostración. Vamos a ver que $\exists n \in \mathbb{N}$ tal que $r_n = 0$.

Por reduccion al absurdo, supongamos que no existe. Tenemos una sucesion infinita de restos decrecientes

$$r_0 > r_1 > r_2 > r_3 > \cdots$$

Si consideramos el conjunto $R = \{r_i \mid i \in \mathbb{N} \cup \{0\}\}$

R es un conjunto de enteros acotado inferiormente (por 0) pero que no tiene minimo. Esto es imposible.

En cada paso de construccion de la sucesion, por la proposicion 7.6, tenemos que $\text{m.c.d.}(a, b) = \text{m.c.d.}(r_0, r_1) = \text{m.c.d.}(r_1, r_2) = \text{m.c.d.}(r_{n-1}, r_n) = \text{m.c.d.}(r_{n-1}, 0) = r_{n-1}$. □

Teorema 7.6 (Existencia de identidad de Bezout)**.** *Sean $a, b \in \mathbb{N}$ y $d = \text{m.c.d.}(a, b)$. Entonces $\exists u, v \in \mathbb{Z}$ tales que*

$$d = au + bv$$

Definicion: A cualquier igualdad de la forma anterior se le llama identidad de Bezout entre a y b.

Ejemplo. Vamos a ver como calcular una identidad de Bezout entre 224 y 92 (anteriormente hemos calculado $\text{m.c.d.}(224, 92) = 4$ con el algoritmo anterior)

$4 = 224 \cdot u + 92v$

Esto se puede hacer con el algoritmo extendido de Euclides.

La penultima division me permite encontrar una identidad de Bezout entre 40 y 12.

$40 = 12 \cdot 3 + 4$. Si despejo, se puede escribir $4 = 40 - 12 \cdot 3 = 40 + 12 \cdot (-3) = 40 \cdot 1 + 12 \cdot (-3)(*)$.

Ahora en la division anterior, tengo la igualdad $92 = 40 \cdot 2 + 12$. Despejando, $12 = 92 - 40 \cdot 2$. Sustituyo 12: $(*) = 40 \cdot 1 + (92 - 40 \cdot 2)(-3) = 40 \cdot 1 + 92 \cdot (-3) + 40 \cdot 6 = 40 \cdot 7 + 92(-3) = (*)$.

En la division anterior, tenemos que $224 = 2 \cdot 92 + 40 \Rightarrow 40 = 224 - 2 \cdot 92$

Sustituyo

$$(*) = (224 - 2 \cdot 92) \cdot 7 + 92 \cdot (-3) = 7 \cdot 224 - 14 \cdot 92 + 92 \cdot (-3) = 7 \cdot 224 + (-17) \cdot 92$$

Demostración. Despues de construir la sucesion de restos $r_0, r_1, r_2, \ldots, r_{n-1}$ del algoritmo de Euclides, sabemos que m.c.d.$(a, b) = r_{n-1}$ que por el teorema de la division $r_{n-1} = r_{n-3} + q_{n-1}r_{n-2}$.

Se puede escribir como combinacion lineal de r_{n-3} y r_{n-2}. A su vez, r_{n-2} se puede poner como combinacion lineal de r_{n-3} y r_{n-4}. Sustituyendo conseguimos r_{n-1} como combinacion lineal de r_{n-3} y r_{n-4}.

Y sucesivamente hasta obtener r_{n-1} como combinacion lineal de a y b. $\square$

Observación. Si queremos generalizar la existencia de identidades de Bezout para enteros $a, b \in \mathbb{Z}$.

- Si $a, b \neq 0$ basta con calcular una identidad de Bezout para $|a|$ y $|b|$ y luego "mover" los signos a los coefientes.
- Las identidades de Bezout si alguno o los dos enteros son 0 son triviales de obtener.

Ejemplo.

$$4 = 224 \cdot 7 + 92 \cdot (-17)$$

Supongamos que quiero una identidad de Bezout entre -224 y 92.

m.c.d.$(224, 92) = 4$.

$$4 = (-224)(-7) + 92 \cdot (-17)$$

Id. Bezout entre -224 y -92.

$$4 = -224 \cdot (-7) + 17 \cdot (-92)$$

Si quiero una identidad de Bezout entre 0 y 2023, m.c.d.$(0, 2023) = 2023$.

$$2023 = 2023 \cdot 1 + 0 \cdot 1$$

Sea $n \in \mathbb{Z}$. Se define $n\mathbb{Z}$ como el conjunto formado por todos los multiplos de n, es decir

$$n\mathbb{Z} \coloneqq \{nk \mid k \in \mathbb{Z}\}$$

Teorema 7.7. *Sean $a, b \in \mathbb{Z}$ y $d =$ m.c.d.(a, b). Entonces se cumple*

$$d\mathbb{Z} = \{au + bv \mid u, v \in \mathbb{Z}\}$$

Demostración. Tenemos que demostrar que $d\mathbb{Z} \stackrel{?}{=} \{au + bv \mid u, v \in \mathbb{Z}\} = E$, siendo $d =$ m.c.d.(a, b).

$\subseteq$) Sea $x \in d\mathbb{Z} \Rightarrow \exists y \in \mathbb{Z}$ tal que $x = dy$.

Por el teorema de existencia de identidades de Bezout, sabemos que existen $u_1, v_1 \in \mathbb{Z}$ tales que $d = a \cdot u_1 + b \cdot v_1$.

Entonces $x = (a \cdot u_1 + b \cdot v_1) \cdot y = a \cdot u_1 \cdot y + b \cdot v_1 \cdot y \Rightarrow x \in E$.

$\supseteq$) Sea $x \in E \Rightarrow \exists u, v \in \mathbb{Z}$ tales que $x = a \cdot u + b \cdot v$. Como d es divisor tanto de a como de $b \Rightarrow \exists m, n \in \mathbb{Z}$ tales que $a = m \cdot d, b = n \cdot d$.

$$x = m \cdot d \cdot u + n \cdot d \cdot v = d(m \cdot u + n \cdot v) \Rightarrow x \in d\mathbb{Z}$$

□

Lema 7.8 (de Euclides)**.**
Sean $a, b, c \in \mathbb{N}$ tales que $a|bc$ y m.c.d.$(a, b) = 1$.

Entonces $a|c$.

Demostración.

$$\left.\begin{array}{l} a|bc \\ \text{m.c.d.}(a,b) = 1 \end{array}\right\} \Rightarrow \exists m \in \mathbb{N} \text{ tal que } bc = a \cdot m$$

Por la existencia de identidades de Bezout, $\exists u, v \in \mathbb{Z} \mid 1 = a \cdot u + b \cdot v$.

Multiplico por c:

$$c = acu + bcv \overset{bc=am}{=} acu + amv = a(cu + mv) \Rightarrow a|c$$

□

Corolario 7.1. *Sean p un numero primo y $a_1, a_2, \ldots, a_n \in \mathbb{N}$ tales que $p|a_1 a_2 \cdots a_n$.*

Entonces $\exists i$ tal que $p|a_i$.

Demostración. Por induccion sobre el numero de factores.

Si $n = 1$, $p|a_1 \Rightarrow p|a_1$ (trivial).

H.I. Si $p|a_1 \cdots a_n \Rightarrow \exists i \in \mathbb{N} \mid p|a_i$.

T.I. Supongamos que $p|a_1 a_2 \cdots a_n a_{n+1}$.

Dos casos:

1. $p|a_{n+1}$. Ya esta.
2. $p \nmid a_{n+1}$.

   Voy a justificar que m.c.d.$(p, a_{n+1} = 1)$.

   Los unicos divisores posibles positivos de p son 1 y p (porque p es primo).

   Como $p \nmid a_{n+1}$ la unica opcion para el m.c.d.$(p, a_{n+1}) = 1$.

   Aplico el lema de Euclides $\Rightarrow p|a_1 \cdots a_n \Rightarrow \exists i \in \mathbb{N}$ tal que $p|a_i$.

□

Demostración. Unicidad del teorema fundamental de la aritmetica.

Supongamos $n = p_1 \cdots p_k = q_1 \cdots q_m$ con los p_i y q_i primos y supongamos que $m \geq k$.

Por el corolario 2 $\Rightarrow \exists i \in \mathbb{N}$ tal que $p_i \mid q_i$.

Sin perdida de generalidad, reordenando los factores voy a suponer que p_1 divide a q_1.

Como q_1 es primo, sus unicos divisores posibles son 1 y q_1. Como $p_1 > 1$ por ser primo, la unica opcion es $p_1 = q_1$.

Dividiendo la igualdad entre p_1, tenemos que $p_2 \cdot p_3 \cdots p_k = q_2 \cdot q_3 \cdots q_m$.

Repito el argumento con $p_2 = q_2$. Simplificando $p_3 \cdots p_k = q_3 \cdots q_m$.

Repitiendo el argumento tenemos $p_3 = q_3, p_4 = q_4, \ldots, p_k = q_k$ y $1 = q_{m+1} \cdot q_{m+2} \cdots q_m$.

Esto no puede pasar a menos que fuera $k = m$. Luego las dos factorizaciones tienen la misma cantidad de factores y las he podido reordenar para que $p_i = q_i$ para todo i.

□

Definición 7.7. Sean $a, b \in \mathbb{N}$. Se define el minimo comun multiplo de a y b como el menor multiplo comun positivo de a y b.

Notacion: m.c.m.(a, b)

Proposición 7.7. $\forall a, b \in \mathbb{N}$ *existe* m.c.m.(a, b)

Demostración. Los multiplos comunes positivos de a y b estan acotados inferiormente por 0.

Ademas, es un conjunto no vacio ya que ab es multiplo comun de ambos.

Por tanto, existe un minimo de los multiplos. □

Proposición 7.8. $\forall a, b \in \mathbb{N}$ *se tiene*

$$\text{m.c.m.}(a, b) = \frac{ab}{\text{m.c.d.}(a, b)}$$

Demostración. Llamamos $m = \text{m.c.m.}(a, b)$, $d = \text{m.c.d.}(a, b)$.

Quiero demostrar que $m = \dfrac{ab}{d}$.

Sea $x = \dfrac{a \cdot b}{d}$. Quiero probar que x es el m.c.m.(a, b).

$x = a \cdot \dfrac{b}{d} \Rightarrow a \mid x$

$x = \dfrac{a}{d} \cdot b \Rightarrow b \mid x$

Luego x es un multiplo comun de a y b.

Falta ver que es el minimo entre los multiplos comunes de a y b. Sea y un multiplo comun positivo de a y $b \Rightarrow \exists u, v \in \mathbb{N} \mid y = a \cdot u, y = b \cdot v$.

$a \cdot u = b \cdot v$. Dividiendo entre d: $\frac{a}{d} \cdot u = \frac{b}{d} \cdot v$.

Por el lema 7.9, m.c.d.$(\frac{a}{d}, \frac{b}{d}) = 1$.

Como $\frac{a}{d} \mid \frac{b}{d}$ y m.c.d.$(\frac{a}{d}, \frac{b}{d}) = 1$ por el lema de Euclides $\frac{a}{d} \mid 1 \Rightarrow \exists w \in \mathbb{N}$ tal que $v = w \cdot \frac{a}{d}$.

Ademas, $y = b \cdot v = b \cdot w \cdot \frac{a}{d} = x \cdot w \geq x \Rightarrow y \geq x$

Por tanto, todos los multiplos comunes positivos de a y b son mayores o iguales que x, luego $x =$ m.c.d.(a, b) □

Lema 7.9. *Sean $a, b \in \mathbb{Z}$ tales que $(a, b) \neq (0, 0)$. Sea $d =$ m.c.d.(a, b) mayor que 0. Se cumple*

$$\text{m.c.d.} \left(\frac{a}{d}, \frac{b}{d} \right) = 1$$

Demostración. Queremos probar que m.c.d.$(\frac{a}{d}, \frac{b}{d}) = 1$ donde $d =$ m.c.d.(a, b).

Sea x un divisor comun de a y b positivo.

$\exists u, v \in \mathbb{Z}$ tales que $\frac{a}{d} = x \cdot u$ y $\frac{b}{d} = x \cdot v \Rightarrow a = x \cdot u \cdot d, b = x \cdot d \cdot v$

Como xd es divisor comun de a y b tiene que ser menor o igual que su m.c.d.$(a, b) = d \Rightarrow xd \leq d$.

La unica opcion es $x = 1$. Luego m.c.d.$(\frac{a}{d}, \frac{b}{d}) = 1$ □

8 Ecuaciones diofanticas lineales

Definición 8.1 (Ecuacion diofantica lineal)**.** Una ecuacion diofantica lineal con dos incognitas es una ecuacion del tipo

$$ax + by = c$$

donde

- $a, b, c \in \mathbb{Z}$ son los coeficientes
- x, y son las incognitas que pueden tomar valores en $\mathbb{Z}$.

Teorema 8.1. *Sean $a, b, c \in \mathbb{Z}$ con $a, b \neq 0$, sea $d = \text{m.c.d.}(a, b)$ y consideremos la ecuacion*

$$ax + by = c$$

La ecuacion tiene solucion si y solo si $d \mid c$.

Ademas, si (x_0, y_0) es una solucion de la ecuacion, entonces el conjunto de todas las soluciones

$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ y = y_0 - \dfrac{a}{d}t \end{cases}$$

con $t \in \mathbb{Z}$ un parametro que recorre todo $\mathbb{Z}$.

Demostración. Considero $ax + by \;\; x, y \in \mathbb{Z}$.

Por el teorema de Bezout, $\{ax + by \mid x, y \in \mathbb{Z}\} = d\mathbb{Z}$. Luego $ax + by = c$ si y solo si c es multiplo de d.

Vamos a demostrar que si (x_0, y_0) es una solucion entonces

$$\begin{cases} x = x_0 + \dfrac{b}{d}t \\ y = y_0 - \dfrac{a}{d}t \end{cases} \quad t \in \mathbb{Z}$$

son todas las soluciones.

Tenemos que demostrar que todas esas parejas son soluciones y que no hay mas.

1. Veamos que son soluciones.

$$a(x_0 + \frac{b}{d}z) + b(y_0 - \frac{a}{d}t) = a \cdot x_0 + a \cdot \frac{b}{d} \cdot z + b \cdot y_0 - b\frac{a}{d}t = a \cdot x_0 + by_0 =$$
$$= a \cdot x_0 + a \cdot y_0 = c \text{ porque } (x_0, y_0) \text{ es solucion}$$

2. Voy a ver que todas las soluciones son asi.

   Sea (x_1, y_1) otra solucion de la ecuacion.

   Entonces $ax_1 + by_1 = c$. Como $ax_0 + by_0 = c \Rightarrow ax_1 + by_1 = ax_0 + by_0$
   $\Rightarrow ax_1 - ax_0 = by_0 - by_1$

   $a(x_1 - x_0) = b(y_0 - y_1)$

   $\dfrac{a}{d}(x_1 - x_0) = \dfrac{b}{d}(y_0 - y_1)$

   Entonces $\dfrac{a}{d} \mid \dfrac{b}{d}(y_0 - y_1)$

Ademas, por el lema 7.9 m.c.d.$(\frac{a}{d}, \frac{b}{d}) = 1$

Aplicando el lema de Euclides $\frac{a}{d} \mid (y_0 - y_1) \Rightarrow \exists t \in \mathbb{Z}$ tal que $y_0 - y_1 = t \cdot \frac{a}{d}$

Por tanto $y_1 = y_0 - t \cdot \frac{a}{d}$.

Voy a obtener x_1:

$$\frac{a}{d}(x_1 - x_0) = \frac{b}{d}t\frac{a}{d} \Rightarrow x_1 - x_0 = \frac{b}{d}t \Rightarrow x_1 = x_0 + \frac{b}{d}t$$

□

Ejemplo. Encuentra (si existen) todas las soluciones enteras de las ecuaciones:

1. $224x + 92y = 82$

   m.c.d.$(224, 92) = 4$

   Luego $4 \nmid 82 \Rightarrow \nexists$ sol de la ecuacion.

2. $224x + 92y = 44$

   m.c.d.$(224, 92) = 4 \mid 44 \Rightarrow \exists$ soluciones

   Para encontrar una solucion particular (x_0, y_0) nos apoyamos en una identidad de Bezout entre 224 y 92.

   $224 \cdot 7 + 92 \cdot (-17) = 4$ (7 y -17 calculado anteriormente con el algoritmo extendido de Euclides)

   Multiplico por 11: $224 \cdot 11 \cdot 7 + 92 \cdot 11 \cdot (-17) = 44$

   Luego $x_0 = 11 \cdot 7 = 77$, $y_0 = (-17) \cdot 11 = -187$

   El teorema que hemos demostrado me dice que el conjunto de soluciones es

   $$\begin{cases} x = x_0 + \frac{b}{d}t \\ y = y_0 - \frac{a}{d}t \end{cases} \Rightarrow \begin{cases} x = 77 + 23t \\ y = -187 - 56t \end{cases} \quad t \in \mathbb{Z}$$

3. $224x - 92y = -20$

   m.c.d.$(224, -92) =$ m.c.d.$(224, 92) = 4$

   $4 \mid -20 \Rightarrow \exists$ soluciones

   A partir de $4 = 224 \cdot 7 + 92 \cdot (-17)$ multiplicando por 5:

$-20 = 224 \cdot (-5) \cdot 7 + 92 \cdot (-5) \cdot (-17) \Rightarrow -20 = 224 \cdot (-35) - 92 \cdot (-85)$

Luego $x_0 = -35, y_0 = -85$ es una solucion.

$$\begin{cases} x = -35 - 23t \\ y = -85 - 56t \end{cases}$$

Observación. Si existen soluciones, encontrar una solucion particular (x_0, y_0) se hace facilmente a traves de una identidad de Bezout.

Si la ecuaicon es $ax+by = c$ y tenemos una identidad de Bezout $au+bv = d$ entonces $(x_0, y_0) = (um, vm)$ es una solucion particular, donde $m = \dfrac{c}{d}$.

9 La relacion de congruencia en $\mathbb{Z}$

Definición 9.1. Sea $n \in \mathbb{N}, n \geq 2$. Dados $a, b \in \mathbb{Z}$ decimos que son congruentes modulo n si $n|a - b$, es decir, si existe $k \in \mathbb{Z}$ tal que $a - b = kn$.

Notacion: $a \equiv b \pmod{n}$.

Proposición 9.1. *La relacion congruencia modulo n es una relacion de equivalencia en $\mathbb{Z}$.*

Demostración.

1. Reflexiva: $\forall a \in \mathbb{Z}\ a \equiv a \bmod n$?

   $a - a = 0 = 0 \cdot n \Rightarrow a \equiv a \bmod n$.

2. Simetrica: $\forall a, b \in \mathbb{Z}$ si $a \equiv b \bmod n\ \exists k \in \mathbb{Z}$ tal que $a - b = k \cdot n \Rightarrow b - a = (-k) \cdot n \Rightarrow b \equiv a \bmod n$.

3. Transitiva: $\forall a, b, c \in \mathbb{Z}$

   $$\left.\begin{array}{l} a \equiv b \bmod n \\ b \equiv c \bmod n \end{array}\right\} \Rightarrow \exists k, m \in \mathbb{Z} \mid a - b = k \cdot n, b - c = m \cdot n$$

   Luego $a - c = n \cdot (k + m) \Rightarrow a \equiv c \bmod n$.

□

Ejemplo. Congruencia modulo 6 (dibujada en la pizarra).

Los numeros que estan relacionados entre si son los que estan en la misma columna. Cada columna es una clase de equivalencia de la relacion.

Hay 6 clases de equivalencia. El conjunto cociente es:

$$\mathbb{Z}/\equiv \bmod n = \{[0], [1], [2], [3], [4], [5]\} = \mathbb{Z}_6$$

$[0] = \{\ldots, -6, 0, 6, 12, \ldots\}$
$[1] = \{\ldots, -5, 1, 7, 13, \ldots\}$
$[2] = \{\ldots, -4, 2, 8, 14, \ldots\}$, $\ldots$

Ejemplo. ¿Cual es la clase de 353?
$353 = 6 \cdot 58 + 5 \Rightarrow [353]_6 = [5]_6$
ya que $353 - 5 = 6 \cdot 58 \Rightarrow 353 \equiv 5 \bmod 6$.

Proposición 9.2. *Sean $a \in \mathbb{Z}$, $n \geq 2$ y r el resto de dividir a entre n. Entonces se cumple*

$$[a]_n = [r]_n$$

Demostración. Como $a = n \cdot q + r$ (teorema de la division), $a - r = n \cdot q \Rightarrow a \equiv r \bmod n \Rightarrow [a]_n = [r]_n$. □

Teorema 9.1. $|\mathbb{Z}_n| = n$.
Es mas, $\mathbb{Z}_n = \{[0]_n, [1]_n, [2]_n, \ldots, [n-1]_n\}$

Demostración. Dado $a \in \mathbb{Z}$ cualquiera por la proposicion 9 $\exists r \in \mathbb{Z}, 0 \leq r \leq n - 1$ tal que

$$[a]_n = [r]_n$$

Para demostrar que hay exactamente r clases, tengo que demostrar que las clases $[0], [1], [2], \ldots, [n-1]$ son todas distintas entre si.

Supongamos que r_1 y r_2 son restos modulo n, es decir, $0 \leq r_1, r_2 \leq n - 1$ y que $[r_1] = [r_2]$.

Luego $\exists k \in \mathbb{Z}$ tal que $r_1 - r_2 = k \cdot n \Rightarrow \underbrace{|r_1 - r_2|}_{\leq n-1} = |k| \cdot n$ Por ser la distancia entre 2 restos, $|k| \cdot n \leq n - 1 \Rightarrow k = 0 \Rightarrow r_1 = r_2$ □

Vamos a definir una suma y un producto en $\mathbb{Z}_n$, sumando y multiplicando representantes. Es necesario demostrar que la operacion esta bien definida:

Proposición 9.3. *Sean $n \in \mathbb{N}$, $n \geq 2$ y $a, b, c, d \in \mathbb{Z}$ tales que*

- $[a]_n = [c]_n$
- $[b]_n = [d]_n$

Entonces se cumple:

- $[a + b]_n = [c + d]_n$
- $[ab]_n = [cd]_n$

Demostración. $[a] = [c] \Rightarrow \exists k \in \mathbb{Z}$ tal que $a - c = k \cdot n$

$[b] = [d] \Rightarrow \exists m \in \mathbb{Z}$ tal que $b - d = m \cdot n$

Quiero ver que $[a+b] = [c+d]$, es decir, que $(a+b) - (c+d)$ es multiplo de n.

$(a+b)-(c+d) = (a-c)+(b-d) = k \cdot n + m \cdot n = (k+m) \cdot n \Rightarrow [a+b] = [c+d]$.

Ahora vamos a ver que $[a \cdot b] = [c \cdot d]$, es decir, que $ab - cd(*)$ es multiplo de n.

$(*) = ab - ad + ad - cd = a(b-d) + (a-c) \cdot d = a \cdot m \cdot n + k \cdot n \cdot d = n(am + kd) \Rightarrow [ab] = [cd]$ □

Ejemplo. Suma y multiplicacion en $\mathbb{Z}_6$:

- $[2] + [5] = [2 + 5] = [7] = [1]$
- $[4] \cdot [5] = [4 \cdot 5] = [20] = [2]$
- $[16] \cdot [-1] = \cdots = [2]$

Definición 9.2 (Anillo)**.** Un anillo es una terna $(A, \oplus, \otimes)$ donde:

- A es un conjunto no vacio.
- $\oplus : A \times A \to A$ es una operacion interna, denominada suma.
- $\otimes : A \times A \to A$ es una operacion interna, denominada producto.

que cumplen:

1. Suma asociativa: $\forall a, b, c \in A (a \oplus b) \oplus c = a \oplus (b \oplus c)$
2. Existencia de neutro: $\exists 0_A \in A$ tal que $\forall a \in A \quad a \oplus a \oplus 0_A = 0_A \oplus a = a$
3. Existencia de opuestos: $\forall a \in A \; \exists b \in A$ tal que $a \oplus b = b \oplus a = 0_A$
4. Suma conmutativa: $\forall a, b \in A \; a \oplus b = b \oplus a$
5. Producto asociativo: $\forall a, b \in A \; (a \otimes b) \otimes c = a \otimes (b \otimes c)$
6. Distributivas: $\forall a, b, c \in A \; a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ y $(b \oplus c) \otimes a = (b \otimes a) \oplus (c \otimes a)$

Definición 9.3. Un anillo A es conmutativo si el producto $\otimes$ es conmutativo.

Definición 9.4. Un anillo A es unitario o anillo con unidad si existe un netro para el producto $\otimes$ distinto del neutro para la suma $\oplus$, es decir

$$\exists 1_A \in A \setminus \{0_A\} \text{ tal que } \forall a \in A \quad a \otimes 1_A = 1_A \otimes a = a$$

Definición 9.5. Definimos en $\mathbb{Z}_n$ una suma y un producto como:

- $[a]_n + [b]_n = [a+b]_n$
- $[a]_n \cdot [b]_n = [a \cdot b]_n$

La proposicion 11 garantiza que estas operaciones estan bien definidas

Proposición 9.4. $(\mathbb{Z}_n, +, \cdot)$ *es un anillo conmutativo con unidad.*

Demostración. Veamos que la suma es asociativa

Sea $[a], [b], [c] \in \mathbb{Z}_n \Rightarrow [a] + ([b] + [c]) \stackrel{?}{=} ([a] + [b]) + [c]$.

Por definicion, $[a] + ([b] + [c]) = [a] + [b+c] = [a + (b+c)] = [(a+b)+c]$ porque la suma en $\mathbb{Z}$ es asociativa.

Es decir, la asociatividad se "hereda" de la asociatividad de la suma en $\mathbb{Z}$.

Son analogas las demostraciones de que la suma y el producto son conmutativos, el producto es asociativo, y la distributiva.

Se heredan de $\mathbb{Z}$ y no las escribimos.

Tenemos que demostrar que existe un neutro de la suma: $\forall [a] \in \mathbb{Z}_n$ se cumple que $[a] + [0] = [a]$. Luego $[0]$ es el neutro de la suma.

Tambien, $\forall [a] \in \mathbb{Z}_n$ tenemos $[-a] \in \mathbb{Z}_n$ tal que $[a] + [-a] = [0]$. Luego $[-a]$ es el opuesto de $[a]$.

Por otro lado $\forall a \in \mathbb{Z}$, $[a][1] = [a]$. Asi, $[1]$ es el neutro del producto en $\mathbb{Z}_n$.

Como cumple todas las propiedades, $\mathbb{Z}_n$ es un anillo conmutativo unitario. □

Ejemplo. $\mathbb{Z}_n$ no es siempre un cuerpo. Por ejemplo, veamos si $\mathbb{Z}_6$ lo es.

Tenemos que ver si existe un $x \in \mathbb{Z}$ tal que $[2] \cdot [x] = [1]$. Esto es lo mismo que $2x - 1 = 6x$, pero no tiene solucion en $\mathbb{Z}$. Luego no es cierto que todos los elementos tengan inverso y por tanto no es un cuerpo.

¿Es $\mathbb{Z}_5$ cuerpo?

$[2] \cdot [3] = [1]$, $[1] \cdot [1] = [1]$, $[4] \cdot [4] = [1]$.

Luego $[1], [2], [3], [4]$ son invertibles en $\mathbb{Z}_5 \Rightarrow \mathbb{Z}_5$ es un cuerpo

Definición 9.6. Decimos que $a \in A$ es invertible si $\exists b \in A$ tal que $ab = ba = 1$.

Definición 9.7. Un cuerpo es un anillo conmutativo con unidad A tal que todo elemento distinto de 0 es invertible.

Proposición 9.5. *Sea* $[a]_n \in \mathbb{Z}_n$. *Se tiene que*

$$[a]_n \text{ es invertible} \Leftrightarrow \text{m.c.d.}(a, n) = 1$$

Demostración. $[a]_n$ es invertible $\Leftrightarrow \overset{DEF}{\Rightarrow} \exists b \in \mathbb{Z}$ tal que $[a]_n \cdot [b]_n = [1]_n \Leftrightarrow$

$\Leftrightarrow \exists b, k \in \mathbb{Z}$ tal que $1 - ab = k \cdot n \Leftrightarrow$

$\Leftrightarrow$ La ecuacion diofantica $n \cdot x + a \cdot y = 1$ tiene solucion en x e y.

Por el teorema 8, tiene solucion si y solo si m.c.d.$(n, a)|1 \Leftrightarrow$ m.c.d.$(n, a) = 1$.

Obs: Ademas, hemos dado una forma de encontrar el inverso, si existe, resolviendo una ecuacion diofantica. □

Ejemplo. ¿Es invertible [17] en $\mathbb{Z}_{12}$? En caso de que exista hallalo.

m.c.d.$(17, 12) = 1 \overset{\text{Prop } 13}{\Rightarrow}$ [17] es invertible en $\mathbb{Z}_{12}$.

$[17][x] = [1]$

$32x + 17y = 1$. Lo resolvemos por el algoritmo extendido de Euclides: $32 = 17 \cdot 1 + 15$, $17 = 16 \cdot 1 + 2$, $15 = 2 \cdot 7 + 1$, $2 = 1 \cdot 2$.

Luego $15 - (17 \cdot 15) \cdot 7 = 8 \cdot 15 - 7 \cdot 17 = 8 \cdot (32 - 17) - 7 \cdot 17 = 8 \cdot 32 - 8 \cdot 17 - 7 \cdot 17 = 8 \cdot 32 + (-15) \cdot 17$

Luego $[-15]$ es el inverso de [37] en $\mathbb{Z}_{12}$.

$1 = 8 \cdot 32 + (-15) \cdot 17$ Id Bezout

$1 - (-15) \cdot 17 = 8 \cdot 32$.

$[1] = [-15] \cdot [17] = [-15 \cdot 17]$ $[-15] = [17]$ $(-15 + 32 = 17)$, $[1] = [17][17]$.

Proposición 9.6. *$\mathbb{Z}_n$ es cuerpo $\Leftrightarrow$ n es primo*

Demostración. $\Leftarrow$) n es primo. Tengo que ver que $[1], [2], [3], \ldots, [n-1]$ son invertibles.

$\forall a$ tal que $1 \leq a \leq n - 1$ se cumple que m.c.d.$(a, n) = 1$ (porque n es primo)

Luego por la proposicion 13, $[a]$ es invertible.

$\Rightarrow$) Veamos que si $\mathbb{Z}_n$ es un cuerpo entonces n es primo. Lo demostramos por contraposicion. (n compuesto $\Rightarrow \mathbb{Z}_n$ no es un cuerpo)

n compuesto $\Rightarrow n = d_1 \cdot d_2$ con $2 \leq d_1, d_2 \leq n - 1$.

Por tanto m.c.d.$(n, d_1) \geq d_1 \geq 2 \Rightarrow \mathbb{Z}_n$ no es un curpo por la proposicion 13. □

10 La ecuacion lineal en $\mathbb{Z}_n$

Ejemplo. $\mathbb{Z}_7$.

$[3][x] = [4]$

El inverso de [3] es [5] porque $[3][5] = [15] = [1]$.

$[5][3][x] = [5][4] \Rightarrow [1][x] = [20] \Rightarrow x = [6]$

Observación. Que pasa si $\mathbb{Z}_n$ no es un cuerpo?

Por ejemplo con $\mathbb{Z}_{10}$, $[2][x] = [3] \Rightarrow 2x - 3 = 10k \Rightarrow \nexists$ solucion.

$[4] \cdot [x] = [2]$, $[x] = [3]$ es solucion, $[x] = [8]$ es solucion.

Definición 10.1. Sean $n \in \mathbb{N}, n \geq 2$ y $a, b \in \mathbb{Z}$. Una ecuacion lineal modulo n con una incognita es una expresion

$$ax \equiv b \pmod{n}$$

donde x es la incognita que toma valores en $\mathbb{Z}$.

Tambien puede expresarse como una ecuacion en $\mathbb{Z}_n$:

$$[a]_n[x]_n = [b]_n$$

donde $[x]_n$ es la incognita que toma valores en $\mathbb{Z}_n$.

Ejemplo.

- $6x \equiv 3 (\text{mod} 8)$

  No tiene solucion porque no existen x y k tal que $\underbrace{6x - 3}_{\text{par}} = \underbrace{8k}_{\text{par}}$

- $6x \equiv 2 (\text{mod } 8)$

  $6 \cdot 0 = 0, 6 \cdot 1 = 6, 6 \cdot 2 = 12 \equiv 4 \bmod 8, \boxed{6 \cdot 3 = 18 \equiv 2 \bmod 8}, 6 \cdot 4 =$
  $24 \equiv 0 \bmod 8, 6 \cdot 5 = 30 \equiv 7 \bmod 8, 6 \cdot 6 = 36 \equiv 4 \bmod 8, \boxed{6 \cdot 7 = 42 \equiv 2 \bmod 8}$

  $x = 3, 8$ son soluciones.

  Si me interesan las soluciones en $\mathbb{Z}$, hay infinitas.

  $[3] =$

Proposición 10.1. *Sean $n \in \mathbb{N}, n \geq 2$, $a, b \in \mathbb{Z}$ y $d = \text{m.c.d.}(a, n)$.*

$$ax \equiv b (mod\ n) \text{ tiene solucion} \Leftrightarrow d|b$$

Demostración. $ax \equiv b \bmod n$ tiene solucion $\Leftrightarrow \exists x \in \mathbb{Z} \mid ax \equiv b \bmod n \Leftrightarrow$ $\exists x \in \mathbb{Z} \mid \exists k \in \mathbb{Z} \mid ax - b = k \cdot n \Leftrightarrow \exists x \in \mathbb{Z}\ \exists k \in \mathbb{Z} \mid ax + n(-k) = b \Leftrightarrow$ La ecuacion $a \cdot x + n \cdot y = b$ tiene solucion en $\mathbb{Z} \underset{\text{Teorema 8}}{\Leftrightarrow} \text{m.c.d.}(a, n)|b$ $\square$

Proposición 10.2. *Sean $n \in \mathbb{N}, n \geq 2, a, b \in \mathbb{Z}$ y $d \equiv \text{m.c.d.}(a, n)$ tales que $d|b$. Entonces las ecuaciones*

- $ax \equiv b\ mod\ n$
- $\frac{a}{d}x \equiv \frac{b}{d} (mod\ \frac{n}{d})$

tienen el mismo conjunto de soluciones.

Demostración. Si c es solucion de $ax \equiv b \bmod n \Rightarrow ac \equiv b \bmod n \Rightarrow \exists k \in \mathbb{Z} \mid ac - b = k \cdot n \Rightarrow \exists k \in \mathbb{Z} \mid \frac{ac-b}{d} = \frac{k \cdot n}{d} \Rightarrow \exists k \in \mathbb{Z} \mid \frac{a}{d}c - \frac{b}{d} = k \cdot \frac{n}{d} (\in \mathbb{Z}$ porque $d =$ m.c.d.(a, n) y $d|b) \Leftrightarrow \frac{a}{d} \cdot c \equiv \frac{b}{d} \bmod \frac{n}{d} \Leftrightarrow$ k es solucion de $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{n}{d}$ □

Lema 10.1. *Sean* $n \in \mathbb{N}, n \geq 2$ *y* $a, b, c \in \mathbb{Z}$ *tales que* m.c.d.$(a, n) = 1$. *Entonces*

$$b \equiv c \ (mod\ n) \Leftrightarrow ab \equiv ac \ (mod\ n)$$

Demostración. $\Rightarrow$) Si $b \equiv c \bmod n \Rightarrow \exists k \mid b - c = k \cdot n \Rightarrow \exists k \mid ab - ac = a \cdot k \cdot n \Rightarrow ab \equiv ac \bmod n$

$\Leftarrow$) Si $ab \equiv ac \bmod n \Rightarrow \exists k \in \mathbb{Z} \mid ab - ac = k \cdot n \Rightarrow a(b-c) = k \cdot n \Rightarrow n|a(b-c)$. Por el lema de Euclides, como m.c.d.$(a, n) = 1$, $n|b - c \Rightarrow b \equiv c \bmod n$. □

Proposición 10.3. *Sean* $n \in \mathbb{N}, n \geq 2$ *y* $a, b \in \mathbb{Z}$ *tales que m.c.d.*$(a, n) = 1$.

Entonces la ecuacion

$$ax \equiv b \ (mod\ n)$$

tiene como solucion $x = ub$, *donde* u *es el inverso de* a *modulo* n. *Ademas la solucion es unica modulo* n.

Expresado en $\mathbb{Z}_n$, *la ecuacion*

$$[a][x] = [b]$$

tiene solucion unica, que es $[x] = [a]^{-1}[b]$

Demostración. $ax \equiv b \bmod n$ con m.c.d.$(a, n) = 1$

Es lo mismo que resolver $[a]_n \cdot [x]_n = [b]$

Sabemos que $[a]_n$ tiene inverso mod n porque $m.c.d.(a, n) = 1$

$[a]_n[x]_n = [b]_n \Rightarrow [x]_n = [b]_n \cdot [a]_n^{-1}$ □

Ejemplo. Calcular todas la soluciones en $\mathbb{Z}$ de la ecuacion

$$59x + 9 \equiv -9 + 11x \pmod{34}$$

$59x - 11x + 9 - 9 \equiv -9 + 11x - 11x - 9 \bmod 34$

$48x \equiv -18 \bmod 34$

Reducimos los coeficientes modulo 34

$14x \equiv 16 \bmod 34$

m.c.d.$(14, 34) = 2|16 \overset{Prop15}{\Rightarrow} \exists$ solucion

Tiene las mismas soluciones que $\frac{14}{2}x \equiv \frac{16}{2} \mod \frac{34}{2} \Rightarrow 7x \equiv 8 \mod 17$.

m.c.d.$(7, 17) = 1 \Rightarrow 7$ es invertible modulo 17.

Para hallar el inverso de 7, buscamos una identidad de Bezout entre 7 y 17. $17 = 7 \cdot 2 + 3, 7 = 3 \cdot 2 + 1$.

$1 = 7 - 3 \cdot 2 = 7 - (17 - 7 \cdot 2) \cdot 2 = 7 - 2 \cdot 17 + 4 \cdot 7 = 5 \cdot 7 + (-2) \cdot 17$.

$1 \equiv 5 \cdot 7 + (-2) \cdot \underbrace{17}_{0} \mod 17 \Rightarrow 1 \equiv 5 \cdot 7 \mod 17 \Rightarrow 5$ es el inverso de 7 modulo 17.

En el lenguaje de bloques $[5]_{17}[7]_{17} = [1]_{17}$.

$[7]_{17}^{-1} = [5]_{17}$.

Luego si tomo la ecuacion $7 \cdot x \equiv 8 \mod 17$ y multiplico por 5 a los dos lados, $5 \cdot 7 \cdot x \equiv 5 \cdot 8 \mod 17 \Rightarrow x \equiv 40 \mod 17$ (lema 3 o prop 17). Produzco $x \equiv 6 \mod 17$.

Todas las soluciones en $\mathbb{Z}$ son $x = 6 + 17 \cdot k$ con $k \in \mathbb{Z}$.

Si pienso en las soluciones de $[7]_{17} \cdot [x]_{17} = [8]_{17}$ en $\mathbb{Z}_{17}$ hay una unica solucion que es $[x]_{17} = [6]_{17}$

11 Sistemas de ecuaciones lineales modulo n

Vamos a estudiar sistemas de varias ecuaciones modulares con una sola incognita x del tipo:

Una herramienta teorica importante por si misma y que, ademas, nos permite resolver algunos de estos sistemas es el teorema chino de los restos.

Teorema 11.1 (chino de los restos)**.** *Sean $n_1, n_2, \ldots, n_k \in \mathbb{Z}$ con cada $n_i \geq 2$ y relativamente primos entre si dos a dos, es decir, si $i \neq j$ entonces* m.c.d.$(n_i, n_j) = 1$.

Sean $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ y consideramos el sistema de ecuaciones

$$\begin{cases} x \equiv a_1 (mod\ n_1) \\ x \equiv a_2 (mod\ n_2) \\ \vdots \\ x \equiv a_k (mod\ n_k) \end{cases}$$

donde x es la incognita que toma valores en $\mathbb{Z}$.

Entonces el sistema tiene solucion.

Es mas, si definimos, para cada j,

- $Q \coloneqq \prod_{i=1}^{n} n_i$

- $Q_j \coloneqq Q/n_j$
- *y_j como una solucion de la ecuacion $Q_i y \equiv i (mod\ n_j)$*

entonces el siguiente valor es solucion del sistema:

$$x_0 = y_1 Q_1 a_1 + y_2 Q_2 a_2 + \cdots + y_k Q_k a_k$$

Y el conjunto de todas las soluciones del sistema viene dado por:

$$x = x_0 + tQ, \quad t \in \mathbb{Z}$$

(por lo que la solucion es unica modulo Q).

Demostración. Vamos a empezar viendo que las ecuaciones

$$Q_j \cdot y \equiv 1 \bmod n_j$$

tienen solucion.

Como $Q_j = \frac{\prod_{i=1}^{k} n_i}{n_j}$, por la hipotesis de que los modulos son relativamente primos dos a dos, tenemos que m.c.d.$(Q_j, n_j) = 1 \Rightarrow Q_j \cdot y \equiv 1 \bmod n_j$ tiene solucion.

Vamos a ver que $x_0 = \sum_{i=1}^{k} y_i Q_i a_i$ es solucion del sistema.

Voy a calcular $x_0 \bmod n_j$.

Si $i \neq j \Rightarrow nj | Q_2$. Todos los sumandos $y_i Q_i a_i$ son 0 mod n cuando $i \neq j$.

Luego $x_0 \equiv y_j Q_j a_j \equiv 1 a_j \equiv a_j \bmod n_j$

Luego x_0 es solucion de la ecuacion $x \equiv a_j \bmod n_j \forall j \Rightarrow x_0$ es solucion del sistema original.

Falta ver que el conjunto de todas las soluciones es

$$x = x_0 + t \cdot Q, \quad t \in \mathbb{Z}$$

donde x_0 es cualquier solucion particular.

Supongamos que $x = x_0 + t \cdot Q$ es uno de esos valores. ¿Cuanto vale modulo n_j?

$$x = x_0 + t \cdot Q \equiv x_0 \equiv a_j \bmod n_j$$

$x_0 \equiv a_j$ porque x_0 es solucion.

Luego x es solucion del sistema.

Veamos que no hay mas soluciones que esos valores.

Sean x_0 una solucion particular y x' otra solucion cualquiera $\Rightarrow x_0 \equiv a_1 \bmod n_1$ y $x' \equiv a_1 \bmod n_1 \Rightarrow x \equiv x' \bmod n_1 \Rightarrow \exists k_1 \in \mathbb{Z} \mid x_0 - x' = k_1 \cdot n_1$.

Tambien $x_0 \equiv a_2 \bmod n_2$, $x' \equiv a_2 \bmod n_2$.

Luego $x_0 \equiv x' \bmod n_2 \Rightarrow \exists k_2 \in \mathbb{Z} \mid x_0 - x' = k_2 \cdot n_2 \Rightarrow k_1 n_1 = k_2 \cdot n_2$.

Por el lema de Euclides, como m.c.d.$(n_1, n_2) = 1$ y $n_1 | k_2 n_2 \Rightarrow n_1 | k_2 \Rightarrow k_2 = n_1 \cdot k \Rightarrow x_0 - x' = n_1 \cdot k n_2$

Sigo con la tercera ecuacion: $x_0 \equiv x' \equiv a_3 \bmod n_3 \Rightarrow x_0 - x = k_3 \cdot n_3$.

Luego $k_2 \cdot n_2 = k_3 \cdot n_3$

Repitiendo el argumento para cada ecuacion, llego a que $x_0 - x' = t \cdot n_1 \cdot n_2 \cdots n_k \Rightarrow x' = x_0 + (-t) n_1 \cdot n_2 \cdots n_k \Rightarrow x' = x_0 + s \cdot Q$.

Por tanto, no hay mas soluciones que las del enunciado. □

Observación. Que pasa si no podemos aplicar el teorema chino de los restos?

Podemos ir resolviendo el sistema por sustitucion: hallar la solucion general en $\mathbb{Z}$ de la primera ecuacion y sustituir en la segunda para obtener una solucion comun de las dos. Sustituir esa solucion en la tercera para hallar una solucion comun de las tres. Y asi sucesivamente hasta encontrar la solucion general comun a todas las ecuaciones.

En el caso general no esta garantizada la existencia de solucion al sistema, se notara si en alguno de los pasos se encuentra una ecuacion que no tiene solucion.

Este metodo es general y tambien sirve para el caso en el que si se puede aplicar el teorema chino de los restos.

Parte IV
Teoria de grafos

Definición 11.1 (Grafo simple)**.** Un grafo simple G es un par $G = (V, E)$ formado por un conjunto finito de vertices V y un conjunto E de pares no ordenados de vertices distintos, es decir,

$$E \subseteq \{\{u, v\} \mid u, v \in V, u \neq v\}$$

A los elementos de E se les denomina aristas (no dirigidas o no orientadas).

Podemos representar geometricamente los grafos en el plano, identificando cada vertice con un punto del plano y cada arista con una linea que une los vertices correspondientes, dando una representacion pictorica del grafo (no unica).

Ejemplo. Un grafo simple es, por ejemplo, el grafo $G = (V, E)$ donde $V = \{1, 2, 3, 4\}$ y $E = \{\{1, 2\}, \{1, 4\}, \{1, 3\}\}$.

Definición 11.2 (Multigrafo)**.** Un multigrafo es un par (V, E) formado por un conjunto finito de vertices V y una familia finita E de aristas no orientadas

$$E = \{e_i\}_{i \in I}$$

donde I es un conjunto finito y $\forall i \in I$ se verifica que $e_i = \{u_i, v_i\}$ con $u_i, v_i \in V$, posiblemente iguales (puede pasar que $u_i = v_i$ o $e_i = e_k$).

Definición 11.3 (Digrafo)**.** Un digrafo es un par (V, E) donde V es un conjunto finito y $E \subset (V \times V) - \Delta$, siendo $\Delta = \{(x, x) \colon x \in V\}$. A los elementos de V se les denomina vertices y a los de E aristas (dirigidas u orientadas).

Definición 11.4 (Multidigrafo)**.** Un multidigrafo es un par (V, E) formado por un conjunto finito de vertices V y una familia finita E de aristas orientadas

$$E = \{e_i\}_{i \in I}$$

donde I es un conjunto finito y $\forall i \in I$ se verifica que $e_i \in V \times V$.

Tipo	Aristas	Aristas multiples?	Lazos?
Grado simple	No dirigidas	No	No
Multigrafo	No dirigidas	Si	Si
Digrafo	Dirigidas	No	No
Multigrafo	Dirigidas	Si	Si

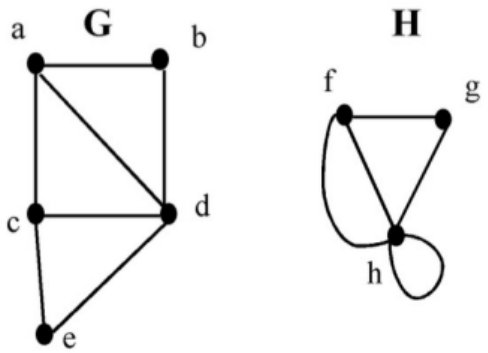
12 Grado y sucesion de grados

Definición 12.1. Se dice que dos vertices u y v de un grafo no dirigido $G = (V, E)$ son adyacentes si $\{u, v\} \in E$. En ese caso se dice que la arista $e = \{u, v\}$ conecta los vertices u y v.

Definición 12.2. Si $G = (V, E)$ es un (multi)grafo no dirigido y $u \in V$, el grado del vertice u es el numero de aristas incidentes con el, imponiendo por conveniencia que un lazo en un vertice contribuye dos veces al grado de ese vertice. Denotaremos el grado de un vertice u por $gr(u)$. Si un vertice tiene grado cero se dice que es un vertice aislado.

La sucesion de grados del grafo G es la lista no ordenada de numeros $\{gr(v_1,), gr(v_2), \ldots, gr(v_n)\}$, donde $v_1, \ldots, v_n$ son todos los vertices de V.

Ejemplo. Considerense los grafos G y H de la figura. En el grafo G se verifica que $gr(a) = 3 = gr(c)$, $gr(b) = 2 = gr(e)$ y $gr(d) = 4$. En el grafo H se verifica que $gr(f) = 3$, $gr(g) = 2$ y $gr(h) = 5$.



Teorema 12.1 (de Euler)**.** *Sea $G = (V, E)$ un grafo no dirigido. Se verifica que*

$$\sum_{v \in V} gr(v) = 2 \cdot |E|$$

Demostración. La demostracion es consecuencia de que cada arista contribuye dos veces a la suma de los grados de los vertices ya que una arista es incidente con exactamente dos vertices (que para los lazos son iguales). □

Corolario 12.1. *Cualquier grafo no dirigido tiene un numero par de vertices de grado impar.*

Demostración. Sean V_1 y V_2 los conjuntos de vertices de grado par e impar respectivamente del grafo $G = (V, E)$.

V_1 y V_2 es particion de V ya que $V = V_1 + V_2$ y $V_1 \cap V_2 = \varnothing$.

En ese caso, y aplicando el teorema de Euler (12.1),

$$2|E| = \sum_{v \in V} gr(v) = \sum_{v \in V_1} gr(v) + \sum_{v \in V_2} gr(v) \text{ (porque son una particion).}$$

o equivalentemente

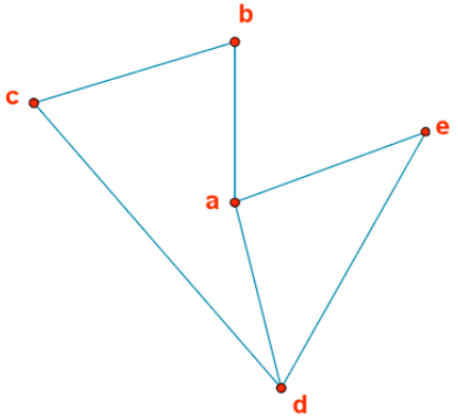
$$2|E| - \sum_{v \in V_1} gr(v) = \sum_{v \in V_2} gr(v).$$

Puesto que para cada $v \in V_1$ se tiene que $gr(v)$ es un numero par y $2|E|$ es par entonces necesariamente $\sum_{v \in V_2} gr(v)$ es un numero par. Por tanto, en el sumatorio debe haber una cantidad par de sumandos. □

13 Representacion matricial de grafos

Dado un grafo simple $G = (V, E)$, para construir una de sus matrices de adyacencias, necesitamos ordenar sus vertices. Si el grafo tiene n vertices, $|V| = n$, y los ordenamos como $V = \{v_1, v_2, \ldots, v_n\}$, la matriz de adyacencias de G con respecto a esa ordenacion de los vertices es la matriz $A = (a_{ij})$ de n filas y n columnas determinadas por la siguiente condicion:

$$a_{ij} = \begin{cases} 1 \text{ si } \{v_i, v_j\} \in E \\ 0 \text{ si } \{v_i, v_j\} \notin E \end{cases}$$



	a	b	c	d	e
a	0	1	0	1	1
b	1	0	1	0	0
c	0	1	0	1	0
d	1	0	1	0	1
e	1	0	0	1	0

Observación. Las matrices de adyacencias tambien se pueden utilizar para representar grafos no dirigidos con lazos y aristas multiples. Asi, un lazo en el vertice v_i viene representado por un 1 en la posicion a_{ii} de la matriz de adyacencia. Si se trata de multigrafos, en la posicion a_{ij} de la matriz colocaremos el numero de aristas que conectan el vertice v_i y el v_j. Asi, si tenemos 3 aristas entre el vertice v_i y el v_j, pondremos $a_{ij} = 3$. En cualquier caso, todos los grafos no dirigidos tienen asociadas matrices simetricas.

Observación. En el caso de los grafos dirigidos la situacion es similar. En la posicion a_{ij} aparecera un 1 si hay una arista dirigida cuyo vertice inicial es v_i y cuyo vertice final es v_j y un cero en caso contrario. Observese que las matrices de adyacencias asociadas a grafos dirigidos no son necesariamente simetricas.

Para dar un grafo basta con dar su matriz de adyacencia y muchas propiedades del grafo se pueden obtener directamente de propiedades de sus matrices de adyacencia, como por ejemplo:

- El numero de vertices de un grafo es el numero de filas (o columnas) de sus matrices de adyacencia.
- El grado de un vertice es la suma de los elementos de la fila (o columna) correspondiente de la matriz de adyacencia.
- Un grafo es no dirigido si su matriz de adyacencia es simetrica.
- Un grafo contiene lazos si algun elemento de la diagonal de la matriz de adyacencia es no nulo.
- Un grafo tiene mas de una arista entre dos vertices si alguno de los elementos de su matriz de adyacencia es mayor que 1.
- Si el grafo es no dirigido y no contiene lazos, usando el Teorema de Euler, el numero de aristas es la mitad de la suma de todos los elementos de su matriz de adyacencia.
- ...

14 Algunos grafos notables

Definición 14.1. Se denomina grafo completo de n vertices al grafo simple de n vertices $K_n = (\{1, 2, \ldots, n\}, \{\{i, j\}; 1 \leq i < j \leq n\})$. Esto significa que cada par de vertices distintos son adyacentes.

Proposición 14.1. *El grafo completo K_n tiene las siguientes propiedades:*

- *El numero de vertices es n*
- *El grado de cada vertice es $gr(v_1) = \cdots = gr(v_n) = n - 1$*
- *El numero de aristas, usando el Teorema de Euler es*

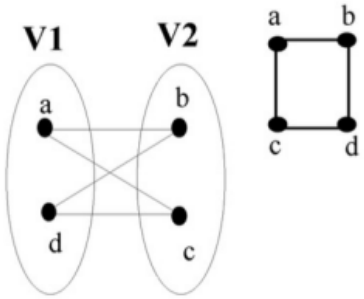
$$|E| = \frac{1}{2}\sum_{i=1}^{n} gr(v_i) = \frac{1}{2}\sum_{i=1}^{n}(n-1) = \frac{n(n-1)}{2}$$

- *Su matriz de adyacencia es*

$$\begin{pmatrix} 0 & 1 & 1 & \cdots & 1 \\ 1 & 0 & 1 & \cdots & 1 \\ 1 & 1 & 0 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & 1 & \cdots & 0 \end{pmatrix}$$

o equivalentemente $1_{n\times n} - I_n$.

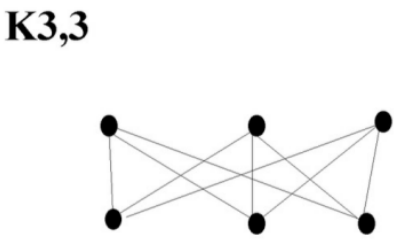
Definición 14.2 (Grafo bipartido)**.** Se dice que un grafo simple $G = (V, E)$ es bipartido si su conjunto de vertices V se puede expresar como la union de dos subconjuntos no vacios disjuntos V_1 y V_2 de manera que cada arista del grafo conecta un vertice de V_1 con un vertice de V_2. Esto es, no existe una arista entre dos vertices de V_1 ni entre dos vertices de V_2: si $\{u, v\} \in E$ entonces $|\{u, v\} \cap V_i| = 1$, $i = 1, 2$.



¿Como saber si un grafo es bipartido?

- Si contiene un ciclo con una cantidad impar de vertices NO puede ser bipartido.
-

Definición 14.3 (Grafo bipartido completo)**.** Sea $V_1 = \{1, \ldots, m\}$ y $V_2 = \{1', \ldots, n'\}$. El grafo bipartido completo $K_{m,n} = (V, E)$ se define como $V = V_1 \cup V_2$ y $E = \{\{j, k'\} : j \in V_1, k' \in V_2\}$. Esto es, V se puede expresar como la union de dos subconjuntos disjuntos V_1 de m vertices y V_2 de n vertices, de manera que cada vertice de V_1 esta conectado con todos los vertices de V_2 y ninguna arista conecta un par de vertices de V_1 ni de V_2.



- En general los grafos bipartidos son diferentes de los grafos bipartidos completos.

Ejemplo. Calcular el numero de vertices, grados, numero de aristas y matriz de adyacencia del grafo $K_{n,m}(n, m \in \mathbb{N})$

- Numero de vertices: Si $K_{n,m} = (V, E)$, entonces $V = V_1 \cup V_2$ particion de V con V_1 conjunto de n vectores y V_2 conjunto de m vectores $\Rightarrow$ el numero de vertices es $|V| = |V_1| + |V_2| = n + m$
- Grado de los vertices: Si $v \in V_1 \Rightarrow gr(v) = m$. Si $v \in V_2 \Rightarrow gr(v) = n$.
- Numero de aristas: Usando el teorema de Euler, $2|E| = \sum_{v \in V} gr(v) = \sum_{v \in V_1} gr(v) + \sum_{v \in V_2} gr(v) = m \cdot n + n \cdot m = 2 \cdot m \cdot n \Rightarrow |E| = n \cdot m$
- Matriz de adyacencia: Si denotamos $V_1 = \{v_1, \ldots, v_n\}$ y $V_2 = \{w_1, \ldots, w_m\}$.

  Tomando el orden de vertices $v_1, \ldots, v_n, w_1, \ldots, w_m$ la matriz de adyacencia es

$$A = \begin{pmatrix} 0 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 0 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 0 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 & 0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & 1 & \cdots & 1 & 0 & \cdots & 0 \end{pmatrix} = \left(\begin{array}{c|c} 0_{n\times n} & 1_{n\times m} \\ \hline 1_{m\times n} & 0_{m\times m} \end{array}\right)$$

15 Caminos y conexion

Definición 15.1 (Camino)**.** Un camino de longitud n entre los vertices a y b de un grafo no dirigido es una sucesion finita $(e_0, \ldots, e_{n-1})$ de aristas del grafo

$$e_0 = \{v_0, v_1\}, e_1 = \{v_1, v_2\}, \ldots, e_{n-1} = \{v_{n-1}, v_n\},$$

de manera que $v_0 = a$, $v_n = b$ y cada arista sucesiva empieza donde termino la anterior. Si el grafo es simple, el camino $(e_0, \ldots, e_{n-1})$ queda perfectamente determinado por la sucesion de vertices

$$(a, v_1, v_2, \ldots, v_{n-1}, b).$$

Diremos que el camino anterior pasa por (o atraviesa) los vertices $a, v_1, v_2, \ldots, v_{n-1}, b$.

Se dice que un camino es un circuito si es cerrada, esto es, empieza y termina en el mismo vertice, es decir, si $a = b$.

Se dice que un camino es simple si no contiene a la misma arista mas de una vez.

Un circuito que no pasa dos veces por el mismo vertice (salvo el inicial por el que pasa dos veces) se llama ciclo.

Definición 15.2 (Conexo)**.** Se dice que un grafo no dirigido G es conexo si para cualquier par de vertices a y b de G existe un camino entre a y b.

Si un grafo no es conexo, se puede expresar como la union de dos o mas subgrafos conexos de manera que los conjuntos de vertices y de aristas de cada par de estos subgrafos son disjuntos entre si. A estos subgrafos se les denomina componentes conexas del grafo dado. De esta manera un grafo es conexo si y solo si tiene una unica componente conexa.

Teorema 15.1. *Sea G un grafo (dirigido o no dirigido, con aristas multiples y lazos o no) y sea $A = (a_{ij})$ su matriz de adyacencias con respecto al orden $v_1, v_2, \ldots, v_{n-1}, v_n$ de su conjunto de vertices. En estas condiciones el numero de caminos de longitud m entre el vertice v_i y el vertice v_j es igual al coeficiente situado en el lugar (i, j) de la potencia m-esima de la matriz A (con respecto al producto de matrices usual).*

Demostración. No la hacemos, pero se puede hacer por induccion sobre la longitud del camino entre dos vertices cualesquiera v_i y v_j de un grafo G. □

Corolario 15.1. *Dado un grafo $G = (V, E)$ tal que $|V| = n$, se verifica que G es conexo si y solo si la matriz*

$$I_n + A + A^2 + \cdots + A^{n-1}$$

tiene todos los coeficientes distintos de cero.

Ejemplo. Sea G un grafo cuya matriz de adyacencia es:

$$A = \begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

Entonces su cuadrado es

$$A^2 \coloneqq \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix}$$

Por tanto $I_3 + A + A^2$ tiene todas sus entradas no nulas y el grafo es conexo.

Definición 15.3 (Camino euleriano)**.** Un camino euleriano en un grafo no dirigido G es un camino simple que contiene a todas las aristas de G. Un circuito euleriano en G es un circuito simple que contiene todas las aristas del grafo G.

Definición 15.4 (Grafo euleriano)**.** Se dice que un grafo no dirigido es euleriano si contiene un circuito euleriano.

Un camino euleriano es un camino que recorre todas las aristas del grafo y sin repetir ninguna.

Teorema 15.2. *Un grafo $G = (V, E)$ con aristas no dirigidas es euleriano si y solo si todas las aristas estan en la misma componente conexa y todos los vertices tienen grado par.*

El siguiente resultado nos da una condicion para la existencia de un camino euleriano no cerrado:

Proposición 15.1. *Un grafo $G = (V, E)$ con aristas no dirigidas tal que todas sus aristas estan en la misma componente conexa admite un camino euleriano no cerrado si y solo si contiene exactamente dos vertices de grado impar.*

Proposición 15.2 (Algoritmo de Fleury)**.** *Para calcular caminos/ciclos eulerianos en un grafo que los admite, usamos el algoritmo de Fleury:*

- *Comprobacion previa: Todas las aristas estan en la misma componente conexa y a lo sumo hay dos nodos de grado impar (necesario para que existan cambios eulerianos).*
- *Paso inicial: elegimos un vertice (v_0) del siguiente modo:*
  - *Si hay vertices de grado impar, elegimos uno de grado impar al azar.*
  - *Si no hay vertices de grado impar, elegimos uno de grado par al azar.*
- *Elegimos al azar una arista incidente en el vertice elegido en el paso anterior que no desconecte el grafo. Si no es posible hacerlo, elegimos una de las aristas incidentes al azar. En ambos casos borramos la arista elegida del grafo y nos movemos al vertice del otro extremo de la arista eliminada.*
- *Repetimos el proceso hasta que no queden aristas.*

La sucesion de aristas construidas antes es un camino/ciclo euleriano.

Definición 15.5 (Camino hamiltoniano)**.** Se denomina camino hamiltoniano en un grafo con aristas no orientadas $G = (V, E)$ a cualquier camino simple que contenga a todos los vertices de G pasadno una sola vez por cada uno de ellos, pero permitiendo que el vertice inicial de dicho camino sea igual al vertice final. Si el camino hamiltoniano es cerrado, a dicho camino se le denomina circuito hamiltoniano.

Definición 15.6 (Grafo hamiltoniano)**.** Se dice que un grafo no dirigido $G = (V, E)$ es hamiltoniano si contiene un circuito hamiltoniano.

Pese a la aparente similitud con la definicion de los grafos eulerianos encontrar un circuito hamiltoniano en un grafo puede no ser tarea facil pues no se conoce una caracterizacion de los grafos hamiltonianos.

Como se ha comentado, no siempre es sencillo determinar si un grafo simple y conexo dado es hamiltoniano pues, para ello, el unico criterio que tenemos a priori es nuestra habilidad para encontrar o no un circuito hamiltoniano en el grafo dado. La siguiente proposicion nos aporta un resutlado que permite concluir que ciertos grafos son hamiltonianos.

Teorema 15.3 (de Dirac)**.** *Sea $G = (V, E)$ un grafo simple conexo de n vertices ($n \geq 3$) tal que para cualquier vertice $v \in V$ se cumple que*

$$gr(v) \geq \frac{n}{2}.$$

entonces G es hamiltoniano.

El Teorema de Dirac da una condicion suficiente para saber si un grafo es hamiltoniano, pero esta condicion no es una condicion necesaria (en general).

Hasta el momento no existe ninguna caracterizacion de los grafos hamiltonianos en terminos de los grados del grafo.

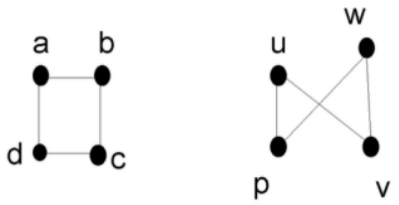
Definición 15.7 (Isomorfismo de grafos)**.** Se dice que dos grafos simples $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$ son isomorfos si existe una biyeccion $f\colon V_1 \to V_2$ tal que $\forall u, v \in V_1$

$$\{u, v\} \in E_1 \Leftrightarrow \{f(u), f(v)\} \in E_2$$

De la funcion f que satisface dicha condicion se dice que es un isomorfismo de grafos entre los grafos G_1 y G_2.

En otras palabras, dos grafos simples son isomorfos si existe una funcion biyectiva entre los dos conjuntos de vertices que preserva las adyacencias. Naturalmente esta definicion se puede extender a multigrafos y multidigrafos teniendo en cuenta el numero de aristas entre cada par de vertices y, en su caso, la orientacion de las aristas.

Ejemplo. Los dos grafos de la figura son isomorfos. Para verlo basta comprobar que la funcion $f\colon \{a,b,c,d\} \to \{u,v,w,p\}$, tal que $f(a) = u$, $f(b) = v$, $f(c) = w$, $f(d) = p$ es un isomorfismo de grafos.



A menudo es dificil determinar si dos grafos simples son isomorfos. De hecho, empleando herramientas de combinatoria, puede comprobarse que hay $n!$ aplicaciones biyectivas entre los conjuntos de vertices de dos grafos con n vertices, por lo que comprobar una por una si dichas biyecciones preservan las adyacencias no es un buen metodo, sobre todo si n es un numero grande.

Debemos encontrar criterios para determinar si dos grafos simples son isomorfos o no lo son que no precisen una comprobacion exhaustiva.

Estos criterios se apoyan en el hecho de que hay ciertas propiedades, denominadas invariantes por isomorfismo, que, si un grafo las verifica, cualquier otro grafo isomorfo a el las debe tambien verificar. Por ejemplo:

1. Dos grafos isomorfos deben tener el mismo numero de vertices y el mismo numero de aristas.

2. Si $f\colon V_1 \to V_2$ establece un isomorfismo entre los grafos $G_1 = (V_1, E_1)$ y $G_2 = (V_2, E_2)$, entonces para cada $u \in V_1$ se tiene que $gr(u) = gr(f(u))$.

Este tipo de resultados sirve para comprobar con cierta facilidad que algunos grafos no son isomorfos.

Teorema 15.4. *Si tenemos dos grafos que son isomorfos, entonces comparten todos los invariantes.*

Por tanto, si tenemos dos grafos que no comporten algun invariante, entonces no pueden ser isomorfos.