Matemática Discreta 2

Santiago Sierra

Índice general

Capítulo 1

Divisibilidad

1.1. Introducción

Teorema 1.1.1 Teorema de División Entera

Dados $a,\ b \in \mathbb{Z}$, con $b \neq 0$, existen únicos $q,\ r \in \mathbb{Z}$ con $0 \leq r < |b|$ y $a = bq + r$.

1. A q se le llama el cociente, y a r el resto de dividir a entre b.
2. Basta con suponer que $b > 0$, ya que si $a = bq + r$ entonces $a = (-b)(-q) + r$.
3. Basta con suponer que $a \geq 0$, ya que si $a = bq + r$ (con $b > 0$ y $0 \leq r < b$) entonces $-a = -bq - r$, pero aquí si $r \neq 0$ no obtuvimos un resto positivo. Sumando y restando b, tenemos que: $-a = b(-q) - b + b - r = b(-q-1) + (b-r)$ y si $r \neq 0$ al ser $0 < r < b$, tenemos que $0 < b - r < b$.

Demostración: Vamos a suponer que $a \geq 0$ y $b > 0$, veamos primero la existencia:
Consideremos el conjunto

$$S = \{s \in \mathbb{N} :\ s = a - bx \text{ para algún } x \in \mathbb{Z}\}$$

Entonces, como $a \geq 0$ tomando $x = 0$, tenemos que $a \in S$ y, por lo tanto $\emptyset \neq S \subset \mathbb{N}$. Como todo conjunto de naturales no vació tiene mínimo, llamamos $r = min\ S$. Así que por la definición de S tenemos que $r \geq 0$ y que existe un $q \in \mathbb{Z}$ con $r = a - bq$ y, por lo tanto $a = bq + r$. Entonces solo queda probar qué $r < b$.

Supongamos lo contrario, que $r \geq b$; en este caso tendríamos que $r = b + s$ con $0 \leq s < r$. Pero en este caso tendríamos que $s = r - b = a - bq - b = a - b(q+1)$ y tendríamos que $s \in S$ lo cual es absurdo pues $s < r = min\ S$.

Veamos la unicidad: supongamos que $a = bq_1 + r_1$ y $a = bq_2 + r_2$ con $0 \leq r_1, r_2 < b$, entonces $bq_1 + r_1 = bq_2 + r_2$, por lo tanto $r_2 = b(q_1 - q_2) + r_1$.
Si $q_1 - q_2 \geq 1$ tendríamos que $r_2 \geq b$, y si $q_1 - q_2 \leq -1$ tendríamos que $r_2 < 0$ (pues $r_1 < b$). Así que $q_1 - q_2 = 0$, y sustituyendo, nos queda qué $r_1 = r_2$. 😄

Corolario 1.1.1

Sean $b \in \mathbb{N}$, con $b \geq 2$ y $x \in \mathbb{N}$, entonces existen $a_0, a_1, \ldots, a_n$ enteros tales que podemos escribir a x en base b como

$$x = b^n a_n + b^{n-1} a_{n-1} + \cdots + b^1 a_1 + b^0 a_0 = \sum_{i=0}^{n} b^i a_i,\ \text{y } 0 \leq a_i < b,\ a_n \neq 0$$

Demostración: Lo probamos por inducción en $x \in \mathbb{N}$. Sí $x = 0$ es claro porque $x = b^0 \times 0$.
Sí $x > 0$, por el teorema anterior existen q y r tales que $x = bq + r$ con $0 \leq r < b$. Como $q < x$ aplicamos la

hipótesis inductiva para obtener

$$q = \sum_{i=0}^{n} b^i a'_i$$

con $0 \leq a'_i < b$. Entonces

$$x = b\left(\sum_{i=0}^{n} b^i a'_i\right) + r = \left(\sum_{i=0}^{n} b^{i+1} a'_i\right) + r = \sum_{i=1}^{n+1} b^i a'_{i-1} + r = \sum_{i=0}^{n+1} b^i a_i$$

con $a_0 = r$ y $a_{i+1} = a'_i$ para $i = 0, 1, \ldots, n$, demostrado así el corolario. 😊

Ejemplo 1.1.1

Escribamos $n = 233$ en base 4.

$$\begin{aligned} 233 &= 4 \times 58 + 1 \\ &= 4 \times (4 \times 14 + 2) + 1 \\ &= 4 \times (4 \times (4 \times 3 + 2) + 2) + 1 \\ &= 4^3 \times 3 + 4^2 \times 2 + 4^1 \times 2 + 4^0 \times 1 \\ &= (3221)_4 \end{aligned}$$

Definición 1.1.1

Dados $n, m \in \mathbb{Z}$ decimos que m divide a n si existe $q \in \mathbb{Z}$ tal que $n = qm$. En este caso escribimos $m \mid n$, y en caso contrario escribiremos $m \nmid n$.

Corolario 1.1.2

1. Tenemos que m divide a n si y solo si, el resto de dividir n entre m es cero.
2. $\pm 1 \mid a,\ \forall a \in \mathbb{Z}$. Ademas si un entero x cumple que $x \mid a,\ \forall a \in \mathbb{Z}$, entonces $x = \pm 1$.
3. $b \mid 0,\ \forall b \in \mathbb{Z}$. Ademas, si un entero x cumple que $b \mid x,\ \forall b \in \mathbb{Z}$, entonces $x = 0$.
4. $\pm n \mid n\ \forall n \in \mathbb{Z}$.
5. Si $b \mid a$ y $a \neq 0$ entonces $|b| \leq |a|$.
6. Si $a \mid b$ y $b \mid a$ entonces $a = \pm b$.
7. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$ (transitiva).
8. Si $db \mid da$ y $d \neq 0$ entonces $b \mid a$ (cancelativa).
9. Si $b \mid a$, entonces $db \mid da$ para todo $d \in \mathbb{Z}$
10. En particular, si d divide a n y a m, entonces d divide al resto de dividir n entre m.

1.2. Máximo Común Divisor

Definición 1.2.1

Si $a \in \mathbb{Z}$ escribiremos $Div(a)$ al conjunto de divisores de a y $Div_+(a)$ al conjunto de divisores positivos de a. Es decir $Div(a) = \{x \in \mathbb{Z} : \ x \mid a\}$ y $Div_+(a) = \{x \in \mathbb{Z}^+ : \ x \mid a\}$.

Corolario 1.2.1

Observar que si $a \neq 0$ y $x \mid a$ entonces como $|x| \leq |a|$, $Div(a) \subset \{\pm 1, \pm 2, \ldots, \pm a\}$, y por lo tanto $Div(a)$ es un conjunto finito (y en particular acotado).
Dados $a, b \in \mathbb{Z}$ diremos que $x \in \mathbb{Z}$ es un divisor común de a y b si $x \mid a$ y $x \mid b$; es decir, el conjunto de divisores comunes de a y b es $Div(a) \cap Div(b)$.
Observar que si $a \neq 0$ o $b \neq 0$ entonces el conjunto de divisores comunes de a y b es finito y por lo tanto tiene máximo.

Definición 1.2.2

Sean $a, b \in \mathbb{Z}$, definimos el máximo común divisor de a y b, que escribiremos $mcd(a, b)$, de la siguiente manera:

- Si $a \neq 0$ o $b \neq 0$, definimos

$$mcd(a, b) = max(Div(a) \cap Div(b)) = max\{x \in \mathbb{Z} : \ x \mid a \text{ y } x \mid b\}$$

- En caso contrario definimos $mcd(0, 0) = 0$.

Proposición 1.2.1

1. $mcd(1, a) = 1 \ \forall a \in \mathbb{Z}$.
2. $mcd(0, b) = |b| \ \forall b \in \mathbb{Z}$.
3. $mcd(a, b) = mcd(|a|, |b|) \ \forall a, b \in \mathbb{Z}$.
4. Cuando $mcd(a, b) = 1$ decimos que a y b son coprimos o primos entre sí.

Corolario 1.2.2

Dados $a, b \in \mathbb{Z}$ con $a, b \neq 0$ entonces:

1. $mcd(a, b) = mcd(b, a - bx) \ \forall x \in \mathbb{Z}$.
2. En particular, si r es el resto de dividir a entre b, se tiene que $mcd(a, b) = mcd(b, r)$.

Demostración: Por la propiedad 3 que mencione anteriormente, basta con probarlo para a y b positivos. Llamemos $d = mcd(a, b)$ y $d' = mcd(b, a - bx)$. Como $d|a$ y $d|b$, por lo visto en las propiedades del Corolario 1.2 tenemos que d divide a cualquier combinación lineal entera de a y b, en particular, $d|a - bx$.
Por lo tanto $d \in Div(b) \cap Div(a - bx)$, y entonces $d \leq max(Div(b) \cap Div(a - bx)) = d'$.

Por otro lado, $d'|b$ y $d'|a - bx$; utilizando el mismo razonamiento, tenemos que d' divide a $(a - bx) + x(b) = a$. Así que $d' \in Div(a) \cap Div(b)$ y tenemos qué $d' \leq max(Div(a) \cap Div(b)) = d$. 😊

Definición 1.2.3: Algoritmo de Euclides

Dados $a, b \in \mathbb{Z}$ con $a \geq b > 0$. Y sea $r(a,b)$ el resto de dividir a entre b:

- Fijamos $r_0 = b$.
- Sea $r_1 = r(a,b)$; por lo tanto tenemos que $mcd(a,b) = mcd(b,r_1)$ y que $0 \leq r_1 < b$.
- Si $r_1 = 0$, entonces $mcd(a,b) = mcd(b,r_1) = mcd(b,0) = b$; y si no, sea $r_2 = r(b,r_1)$. Por lo tanto $0 \leq r_2 < r_1 < b$ y $mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2)$.
- Se sigue de esta forma, definiendo en el paso $i+1$, $r_{i+1} = r(r_{i-1}, r_i)$, en particular tenemos que $0 \leq r_{i+1} < r_i$ y que $mcd(r_{i-1}, r_i) = mcd(r_i, r_{i+1})$. De esta forma, vamos construyendo enteros, hasta conseguir $r_n = 0$, para obtener

$$mcd(a,b) = mcd(b,r_1) = mcd(r_1,r_2) = \cdots = mcd(r_{n-1}, r_n) = mcd(r_{n-1}, 0) = r_{n-1}$$

Teorema 1.2.1 Igualdad de Bezout

Sean $a,\ b \in \mathbb{Z}$ con $(a,b) \neq (0,0)$, entonces:

1. $mcd(a,b) = min\{s \in \mathbb{Z}^+ : s = ax + by \text{ para algún } x, y \in \mathbb{Z}\}$
2. (Identidad de Bezout) $\exists x, y \in \mathbb{Z} \ / \ mcd(a,b) = ax + by$.

Nota:-

Alcanza probarlo para $a, b \in \mathbb{Z}^+$.

Proposición 1.2.2

Los números $x, y \in \mathbb{Z}$ de la segunda parte se llaman "coeficientes de Bezout"(no son únicos).

Demostración: Llamemos $S = \{s \in \mathbb{Z}^+ : \ s = ax + by \text{ con } x, y \in \mathbb{Z}\}$, por definición, tenemos que $S \subset \mathbb{Z}^+$ y además $S \neq \emptyset$ ya que tomando $x = a$ e $y = b$, tenemos que $s = ax + by = a^2 + b^2 > 0$ así que $a^+b^{\in}S$.
Entonces por el principio de buen orden, S tiene mínimo, y lo llamamos $s_0 = min\ S$.
Queremos probar que $s_0 = mcd(a,b)$ y lo haremos probando las dos desigualdades. Tenemos entonces que $s_0 > 0$ y que existen $x_0, y_0 \in \mathbb{Z}$ tales qué $s_0 = ax_0 + by_0$.
Llamemos $d = mcd(a,b)$. Como $d|a$ y $d|b$, tenemos $d|ax_0 + by_0 = s_0$. Por lo tanto $d \leq s_0$.

Probemos ahora que s_0 divide a a y b. Por el teorema de división entera, tenemos que existen $q, r \in \mathbb{Z}$ con $a = qs_0 + r$ y $0 \leq r < s_0$.
Luego $r = a - qs_0 = a - q(ax_0 + by_0) = a(1 - qx_0) + b(-qy_0)$. Por lo tanto, si r fuera positivo tendríamos que $r \in S$; pero como s_0 es el menor entero positivo en S y $r < s_0$, tenemos qué $r = 0$. Resulta entonces que $a = qs_0$ y, por lo tanto $s_0|a$. De igual modo se muestra qué $s_0|b$.
Hemos obtenido que s_0 es un divisor común de a y b, luego $s_0 \leq d$. 😊

Proposición 1.2.3

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

1. Si $e \in \mathbb{Z}$ es tal que $e|a$ y $e|b$ entonces $e|mcd(a,b)$.
2. $mcd(a,b) = 1 \Leftrightarrow \exists x, y \in \mathbb{Z}$ tal que $ax + by = 1$.
3. Si $n \in \mathbb{Z}$ entonces $mcd(na, nb) = |n|mcd(a,b)$.
4. Sea $d \in \mathbb{Z}^+$ tal que $a = da^*$ y $b = db^*$ con $a^*, b^* \in \mathbb{Z}$. Entonces $d = mcd(a,b) \Leftrightarrow mcd(a^*, b^*) = 1$.
   A los enteros a^* y b^* tales que $a = mcd(a,b)a^*$ y $b = mcd(a,b)b^*$ se les llama cofactores de a y b.

Corolario 1.2.3

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

Demostración: Por la igualdad de Bezout, tenemos que existen $x, y \in \mathbb{Z}$ tales que $1 = ax + by$. Multiplicando por c tenemos que $c = cax + cby$. Ahora, $a|a$ y por hipótesis $a|cb$ y, por lo tanto $a|a(cx) + cb(y) = c$. 😄

Corolario 1.2.4

Sea p un entero primo y $b, c \in \mathbb{Z}$. Si $p|bc$ entonces $p|b$ o $p|c$.

Demostración: Si $p \nmid b$, entonces (al ser p primo) tenemos que $mcd(p,b) = 1$, y por el Lema de Euclides concluimos que $p|c$. 😄

Corolario 1.2.5

Sea $p \in \mathbb{N}$ que cumple que si $p|bc$ entonces $p|b$ o $p|c$, luego p es primo.

Demostración: Supongamos por absurdo que p no es primo, entonces existen b y c tales que $1 < b,\ c < p$ y $p = bc$. Por hipótesis, como $p|p = bc$, se tiene que $p|b$ o $p|c$. Además $b|p$ y $c|p$. Concluimos que $p = b$ o $p = c$, pero $b, c < p$. Por lo tanto, p tiene que ser primo. 😄

Corolario 1.2.6

Sea p un entero primo, y $a_1, \ldots, a_n$ enteros, tales que $p|a_1 a_2 \ldots a_n$. Entonces $p|a_i$ para algún $i \in \{1, \ldots, n\}$.

Definición 1.2.4

Dados $a, b \in \mathbb{Z}$ no nulos, definimos el mínimo común múltiplo de a y b como:

$$mcm(a,b) = min\{x \in \mathbb{Z}^+ :\ a|x \text{ y } b|x\}$$

En el caso de que alguno sea nulo, definimos $mcm(0,b) = 0,\ \forall b \in \mathbb{Z}$.

Definición 1.2.5

Dados $a, b \in \mathbb{Z}$ no nulos, se cumple que

$$mcm(a,b) = \frac{|ab|}{mcd(a,b)}$$

Demostración: Llamemos $m = mcm(a,b)$ y sean a^* y b^* los cofactores de a y b. Claramente $\frac{|ab|}{mcd(a,b)} > 0$ y $\frac{|ab|}{mcd(a,b)} = |ab^*| = |a^*b|$ es múltiplo de a y b; así que $m \leq \frac{|ab|}{mcd(a,b)}$.
Por otro lado, como $a|m$, existe $k \in \mathbb{Z}$ tal que

$$m = ak = mcd(a,b)a^*k$$

Como $b|m$ y $b = mcd(a,b)b^*$ tenemos que $mcd(a,b)b^*|mcd(a,b)a^*k$. Como $mcd(a,b) \neq 0$, por la cancelativa tenemos que entonces $b^*|a^*k$. Ahora como $mcd(a^*, b^*) = 1$, por el Lema de Euclides, tenemos que $b*|k$. Por lo tanto, existe $k' \in \mathbb{Z}$ tal que $k = b^*k'$ y sustituyendo, obtenemos que $m = ab^*k'$ y, por lo tanto $\frac{|ab|}{mc(a,b)} = |ab^*| \leq m$. 😄

1.3. Pruebas de Irracionalidad

Corolario 1.3.1

Si p es primo entonces $\sqrt{p}$ no es racional.

1.4. Algoritmo de Euclides Extendido

Veamos ahora un método para hallar coeficientes de Bezout; es decir, $x, y \in \mathbb{Z}$ tales que $mcd(a,b) = ax+by$. Escribimos los datos de cada paso del Algoritmo de Euclides en forma de vector.

En general, si partimos del dato inicial $B_0 = \begin{pmatrix} a \\ b \end{pmatrix}$:

1. En el primer paso del algoritmo de Euclides realizamos $a = bq_1 + r_1$, y obtenemos los nuevos datos

$$B_1 = \begin{pmatrix} b \\ r_1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} B_0$$

   Llamemos $M_1 = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix}$.

2. Luego realizamos lo mismo con estos nuevos datos: $b = q_2 r_1 + r_2$, y obtenemos los nuevos datos

$$B_2 = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} \text{ y } M_2 = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix}$$

   con la relación

$$B_2 = \begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} B_1 = M_2 M_1 B_0$$

3. Y seguimos el algoritmo, donde cada paso con los datos $B_i = \begin{pmatrix} r_{i-1} \\ r_i \end{pmatrix}$ escribiendo $r_{i-1} = q_{i+1} r_i + r_{i+1}$ obtenemos los nuevos datos $B_{i+1} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix}$ y la matriz $M_{i+1} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix}$, con la relación

$$B_{i+1} = \begin{pmatrix} r_i \\ r_{i+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{i+1} \end{pmatrix} B_i = M_{i+1} B_i = M_{i+1} M_i \dots M_1 B_0$$

4. Al obtener el primer resto nulo, $r_n = 0$ tendremos que en el paso anterior

$$B_{n-1} = \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix} = \begin{pmatrix} r_{n-2} \\ mcd(a,b) \end{pmatrix} = M_{n-1} \dots M_1 B_0$$

   Llamando $M = M_{n-1} \dots M_1$ tenemos que

$$B_{n-1} = \begin{pmatrix} r_{n-2} \\ mcd(a,b) \end{pmatrix} = M \; B_0 = M \begin{pmatrix} A \\ B \end{pmatrix} :$$

   por lo tanto, si $M = \begin{pmatrix} z & w \\ x & y \end{pmatrix}$, la ultima fila nos dice que $mcd(a,b) = xa + yb$; es decir, la segunda fila de M son coeficientes de Bezout para a y b.

Ejemplo 1.4.1

El dato inicial del algoritmo es el vector $B_0 = \begin{pmatrix} 132 \\ 28 \end{pmatrix}$.

- En el primer paso, a partir de $132 = 4 \times 28 + 20$, cambiamos los datos del algoritmo a $B_1 = \begin{pmatrix} 28 \\ 20 \end{pmatrix}$, observar que:

$$B_1 = \begin{pmatrix} 28 \\ 20 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 132 \\ 28 \end{pmatrix}$$

- En el segundo paso, a partir de $28 = 1 \times 20 + 8$, cambiamos los datos del algoritmo a $B_2 = \begin{pmatrix} 20 \\ 8 \end{pmatrix}$, queda:

$$B_2 = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 28 \\ 20 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 132 \\ 28 \end{pmatrix}$$

- En el segundo paso, a partir de $20 = 2 \times 8 + 4$, cambiamos los datos del algoritmo a $B_3 = \begin{pmatrix} 8 \\ 4 \end{pmatrix}$, observamos que:

$$B_3 = \begin{pmatrix} 8 \\ 4 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 132 \\ 28 \end{pmatrix}$$

  Ahora, como $8 = 2 \times 4 + 0$, es decir el resto es 0, ya podemos hacer el producto

$$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} = \begin{pmatrix} -1 & 5 \\ 3 & -14 \end{pmatrix}$$

  Obteniendo

$$\begin{pmatrix} 8 \\ 4 \end{pmatrix} = \begin{pmatrix} -1 & 5 \\ 3 & -14 \end{pmatrix} \begin{pmatrix} 132 \\ 28 \end{pmatrix}$$

  En particular, obtenemos que $4 = 3(132) - 14(28)$. Obtuvimos entonces que $x = 3$ e $y = -14$ verifican que $4 = 132x + 28y$.

1.5. Ecuaciones diofánticas lineales

Definición 1.5.1

Una ecuación diofántica lineal en las variables x, y es una ecuación de la forma $ax+by=c$, con $a,b,c \in \mathbb{Z}$. Nos interesa buscar todas las soluciones enteras a la ecuación, por lo tanto, diremos que el conjunto solución es:

$$S = \{(x,y) \in \mathbb{Z}\times\mathbb{Z} : \ ax+by=c\}$$

A partir de ahora, cuando hablamos de una solución a la ecuación, nos referimos a un par $(x,y) \in S$.

Teorema 1.5.1

Sean a,b,c enteros con $(a,b) \neq (0,0)$. Entonces la ecuación diofántica $ax+by=c$

- Tiene solución si y solo si $mcd(a,b)|c$.
- Ademas, si tiene una solución, tiene infinitas. Es mas, si (x_0,y_0) es una solución, entonces el conjunto de soluciones es

$$S = \{\left(x_0 + \frac{b}{mcd(a,b)}k, y_0 - \frac{a}{mcd(a,b)}k\right) : k \in \mathbb{Z}\} = \{(x_0+b^*k, y_0-a^*k) : k \in \mathbb{Z}\}$$

Demostración: Llamemos $d = mcd(a,b)$. Al ser $(a,b) \neq (0,0)$, tenemos que $d \neq 0$.

1. Si la ecuación tiene solución, entonces existen $x_0, y_0 \in \mathbb{Z}$ tales que $ax_0+by_0=c$. Como $d|a$ y $d|b$, entonces $d|ax_0+by_0=c$.
   Supongamos ahora que $d|c$ y veamos que la ecuación tiene solución: como $d|c$, existe $e \in \mathbb{Z}$ tal que $c=de$. Por la igualdad de Bezout, existen $x', y' \in \mathbb{Z}$ tales que $ax'+by'=d$. Multiplicando por e tenemos que $a(x'e)+b(y'e)=de=c$, y por lo tanto el par $(x,y)=(x'e,y'e)$ es solución de la ecuación $ax+by=c$.

2. Sea (x_0,y_0) una solución. Veamos primero que para todo $k \in \mathbb{Z}$, el par

   $$\left(x_0 + \frac{b}{mcd(a,b)}k, y_0 - \frac{a}{mcd(a,b)}k\right)$$

   es solución de la ecuación. Para esto simplemente sustituimos:

   $$a\left(x_0 + \frac{b}{mcd(a,b)}k\right) + b\left(y_0 - \frac{a}{mcd(a,b)}\right) = ax_0 + \frac{abk}{d} + by_0 - \frac{abk}{d} = ax_0+by_0 = c$$

   donde la ultima igualdad vale porque (x_0,y_0) es solución.
   Veamos ahora que para cualquier solución (x_1,y_1) de la ecuación, existe un $k \in \mathbb{Z}$ tal que $(x_1,y_1) = \left(x_0 + \frac{b}{d}k, y_0 - \frac{a}{d}k\right) = (x_0+b^*k, y_0-a^*k)$. Al ser $(a,b) \neq (0,0)$ podemos suponer que $b \neq 0$ (y en consecuencia $b^* = \frac{b}{d} \neq 0$).
   Sea entonces (x_1,y_1) una solución, tenemos pues que

   $$ax_1+by_1 = c \text{ y}$$
   $$ax_0+by_0 = c$$

   Por lo tanto $ax_1+by_1 = ax_0+by_0$, entonces $a(x_1-x_0) = b(y_0-y_1)$. Al ser $d \neq 0$, podemos dividir entre d y obtenemos $a^*(x_1-x_0) = b^*(y_0-y_1)$.
   Tenemos en particular que $b^*|a^*(x_1-x_0)$ y como $mcd(a^*,b^*)=1$, por el Lema de Euclides tenemos que $b^*|(x_1-x_0)$. Por lo tanto existe un $k \in \mathbb{Z}$ tal que $x_1-x_0 = b^*k$ y por lo tanto $x_1 = x_0+b^k$. Si ahora sustituimos en la ecuación anterior obtenemos:

   $$a^*b^*k = b^*(y_0-y_1)$$

   y como supusimos $b^* \neq 0$, cancelando obtenemos $a^*k = y_0-y_1$, y por lo tanto $y_1 = y_0-a^*k$.

😊

Ejemplo 1.5.1

Una barraca vende ladrillos a 12 pesos la unidad y baldozas a 21 pesos cada una. Tenemos 333 pesos y queremos gastarlo todo en baldozas y ladrillos (y que no sobre nada). De cuantas formas podemos hacerlo? Si llamamos x a la cantidad de ladrillos que compramos, e y la cantidad de baldozas, tenemos que $x, y \in \mathbb{N}$ y la condición de gastar los 333 pesos se traduce a

$$12x + 21y = 333$$

Algunas observaciones:

- La primera es que como tanto 12 y 21 son múltiplos de 3, el dinero que gastamos tendrá que ser múltiplo de 3, es decir, si en vez de 333 pesos quisiéramos gastar 100 pesos, no podríamos hacerlo.
- La segunda observación es que como $3 = mcd(12, 21)$, por la igualdad de Bezout podemos hallar $x', y' \in \mathbb{Z}$ tales que $12x' + 21y' = 3$.
- Por ejemplo $x' = 2$ e $y' = -1$ cumplen la ultima ecuación: $12(2) + 21(-1) = 3$.
- Si multiplicamos la ultima igualdad por 111, obtenemos que $12(222) + 21(-111) = 333$, es decir, que $x = 222$ e $y = -111$ verifican la ecuación; pero estos valores de x e y no nos resuelven el problema original, ya que buscamos que $x, y \geq 0$. No nos interesa entonces hallar TODOS los pares de enteros (x, y) que son solución, hay que buscar los que no sean negativos.
- Como ya tenemos una solución, viendo el ultimo teorema, sabemos que el conjunto solución es $\{(x, y) = (222 - 7k, -111 + 4k) : k \in \mathbb{Z}\}$, siendo $x_0 = 222$, $\frac{b}{mcd(a,b)} = \frac{21}{3} = 7$, $y_0 = -111$, y $\frac{a}{mcd(a,b)} = \frac{12}{3} = 4$.

Entonces, para terminar de resolver el problema original, necesitamos las soluciones tales que $x = 222 - 7k \geq 0$, e $y = -111 + 4k \geq 0$, es decir las soluciones para valores de k tales que $222 \geq 7k$ y $4k \geq 111$. O sea, necesitamos $k \in \mathbb{Z}$ con $\frac{111}{4} \leq k \leq \frac{222}{7}$, así que los valores de k son $k = 28, 29, 30, 31$, y por lo tanto, las soluciones al problema son $(x = 26, y = 1), (x = 19, y = 5), (x = 12, y = 9), (x = 5, y = 13)$.

1.6. El problema de los sellos

Proposición 1.6.1

Sean $a > 1,\ b > 1$ enteros, primos entre si. Entonces no hay enteros $x,\ y$ no negativos con $ax+by = ab-a-b$.

Proposición 1.6.2

Sean a y b enteros positivos tales que $mcd(a,b) = 1$. Si $n \geq ab - a - b + 1$, entonces existen enteros no negativos x, y tales que $ax + by = n$.

Demostración: Por el teorema 1.5 como $mcd(a,b) = 1$, existe un par de enteros (x_0, y_0) que cumplen

$$ax_0 + by_0 = n \geq ab - a - b + 1$$

que nos permite expresar todas las soluciones en la forma

$$x = x_0 + bk,\ y = y_0 - ak,\ k \in \mathbb{Z}$$

Usando el algoritmo de división, podemos dividir y_0 por a y escribir $y_0 = at + y_1$, con $0 \leq y_1 \leq a - 1$, para algún entero t. Probaremos que $x_1 = x_0 + bt$ es no negativo. Si $x_1 \leq -1$, entonces, como $y_1 \leq a - 1$,

$$\begin{aligned} n &= ax_0 + by_0 \\ &= a(x_1 - bt) + b(y_1 + at) \\ &= ax_1 + by_1 \\ &\leq a(-1) + b(a - 1) \\ &\leq ab - a - b \end{aligned}$$

que contradice la hipótesis $n \geq ab-a-b+1$. Concluimos que (x_1, y_1) es una solución de enteros no negativos. 😄

1.7. Teorema Fundamental de la Aritmética

Teorema 1.7.1 Teorema Fundamental de la Aritmética

Sea $n \in \mathbb{N},\ n > 1$; entonces

1. Existen primos $p_1, \ldots, p_k$ (no necesariamente distintos) con $k \geq 1$, tales que $n = p_1 \ldots p_k$.
2. Hay unicidad en la factorización. Es decir, k (la cantidad de factores primos) es único y la lista de primos (contando repeticiones), $p_1, \ldots, p_k$ es única.

Demostración:

1. Demostraremos la existencia de la factorización en primos por inducción en n.
   - Si $n = 2$, al ser 2 primo, tomando $p_1 = 2$ tenemos que $2 = p_1$.
   - Sea $n > 2$. Supongamos que las factorizaciones en productos de primos existen para todo natural m con $2 \leq m < n$ (hipótesis inductiva) y probemoslo para n (tesis inductiva):
     Si n es primo, entonces tomando $p_1 = n$ tenemos lo deseado. Si n no es primo, entonces n tiene un divisor positivo a, con $1 < a < n$. Entonces existe $b \in \mathbb{Z}$ tal que $n = ab$ y luego $1 < b < n$. Por lo tanto a y b se encuentran en nuestra hipótesis inductiva, y por lo tanto existen primos $p_1, \ldots, p_k$ y $p'_1, \ldots, p'_r$ tales que $a = p_1 \ldots p_k$ y $b = p'_1 \ldots p'_r$. Al ser $n = ab$ tenemos que $n = p_1 \ldots p_k p'_1 \ldots p'_r$ y hemos probado la tesis inductiva.
2. Para probar la unicidad supongamos que existe un natural $n > 1$ que se escribe de dos formas distintas como producto de primos. Podemos considerar n_0, el menor natural que verifica lo anterior. Entonces existen primos $p_1, \ldots, p_k, q_1, \ldots, q_r$ tales que $n_0 = p_1 \ldots p_k,\ n_0 = q_1 \ldots q_r$ con $\{p_1, \ldots, p_k\} \neq \{q_1, \ldots, q_r\}$ (y como claramente n_0 no puede ser primo, tenemos que $k, r \geq 2$.)
   Tenemos entonces que $p_1 \ldots p_k = q_1 \ldots q_r$ y por lo tanto $p_1 | q_1 \ldots q_r$. Al ser p_1 primo, por el corolario 1.2 existe $j \in \{1, \ldots, r\}$ tal que $p_1 | q_j$; y al ser $p_1 > 1$ y q_j primo, debe ser $p_1 = q_j$. Podemos asumir que $j = 1$. Así que ahora tenemos que $p_1 \ldots p_k = p_1 q_2 \ldots q_r$ y cancelando p_1 obtenemos $p_2 \ldots p_k = q_2 \ldots q_r$ es un entero > 1 que se escribe de dos formas distintas como producto de primos, y esto es absurdo ya que $m = \frac{n_0}{p_1} < n_0$ y n_0 era el menor entero mayor que uno que se podía escribir de dos formas distintas como producto de primos.

😄

Corolario 1.7.1

Existen infinitos primos.

Demostración: Supongamos por absurdo que existe una cantidad finita de primos y sea $\{p_1, \ldots, p_k\}$ el conjunto de todos los primos. Consideremos el entero $n = p_1 p_2 \ldots p_k + 1$. Al ser $n > 1$, por el Teorema Fundamental de la Aritmética, n se escribe como producto de primos. En particular, existe algún primo p que divide a n, y como supusimos que todos los primos son $\{p_1, \ldots, p_k\}$ tenemos que $p_i | n$ para algún $i \in \{1, \ldots, k\}$. Tenemos entonces que $p_i | p_1 p_2 \ldots p_k + 1$, pero como $p_i | p_1 p_2 \ldots p_k$, tenemos que $p_i | 1$ lo cual es absurdo al ser $p_i > 1$. 😄

Nota:-

Si en la descomposición de un entero positivo a, tomamos primos distintos, entonces estos pueden aparecer con exponentes. Por lo tanto, todo entero $a > 1$ se escribe (de forma única, al menos del orden) como $a = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$, con p_i primos distintos y $e_i \in \mathbb{Z}^+$.

Proposición 1.7.1

Sean a, b enteros positivos con descomposición en factores primos

$$a = 2^{a_2}3^{a_3}5^{a_5} \text{ y } b = 2^{b_2}3^{b_3}5^{a_5}$$

entonces:

1. $a|b$ si y solo si $a_p \leq b_p$ para todo p (cabe aclarar que estamos notando como $a = p^{a_p}$ como lo hice arriba)
2. $mcd(a,b) = 2^{d_2}3^{d_3}5^{d_5}\dots$ siendo $d_p = min\{a_p, b_p\}$ para todo primo p.
3. $mcm(a,b) = 2^{m_2}3^{m_3}5^{m_5}\dots$ siendo $m_p = max\{a_p, b_p\}$ para todo primo p.

Demostración:

1. Si $a|b$, existe $c \in \mathbb{Z}^+$ tal que $ac = b$. Escribimos $c = 2^{c_2}3^{c_3}5^{c_5}\dots$ y tenemos

   $$2^{a_2+c_2}3^{a_3+c_3}5^{a_5+c_5}\dots = ac = b = 2^{b_2}3^{b_3}5^{b_5}\dots$$

   Por la unicidad de la descomposición factorial debe ser $a_p + c_p = b_p$ para todo primo p y en particular (al ser $c_p \geq 0$) $a_p \leq b_p$.

2. Por lo visto en la parte anterior, tenemos que

   $$Div_+(a) = \{c = 2^{c_2}3^{c_3}5^{c_5}\dots \text{ con } 0 \leq c_p \leq a_p,\ \forall p\}$$

   $$Div_+(b) = \{c = 2^{c_2}3^{c_3}5^{c_5}\dots \text{ con } 0 \leq c_p \leq b_p,\ \forall p\}$$

   Por lo tanto, los divisores comunes de a y b son:

   $$\begin{aligned} Div_+(a) \cap Div_+(b) &= \left\{c = 2^{c_2}3^{c_3}5^{c_5}\dots \text{ con } 0 \leqslant c_p \leqslant a_p, \text{ y } c_p \leqslant b_p,\ \forall p\right\} \\ &= \left\{c = 2^{c_2}3^{c_3}5^{c_5}\dots \text{ con } 0 \leqslant c_p \leqslant min\{a_p, b_p\},\ \forall p\right\} \end{aligned}$$

   El máximo de este conjunto es claramente $c = 2^{d_2}3^{d_3}5^{d_5}\dots$ siendo $d_p = min\{a_p, b_p\}$ para cada primo p.

3. Se deduce de la parte anterior y del hecho de que para enteros positivos a y b se tiene que $mcm(a,b) = \frac{ab}{mcd(a,b)}$.

😄

Corolario 1.7.2

Sea $n = p_1^{e_1}p_2^{e_2}\dots p_k^{e_k}$, con p_i primos distintos y $e_i \in \mathbb{Z}^+$. Entonces:

1. $Div_+(n) = \{p_1^{c_1}p_2^{c_2}\dots p_k^{c_k} : \ c_i \in \mathbb{N} \text{ y } c_i \leq e_i,\ \forall i = 1, \dots, k\}$.
2. La cantidad de divisores positivos de n es $\#Div(n) = (e_1+1)(e_2+1)\dots(e_k+1)$.
3. El entero n es un cuadrado perfecto (es decir, existe $m \in \mathbb{Z}$ tal que $n = m^2$) si y solo si $2|e_i\ \forall i = 1\dots, k$.
4. Existe $m \in \mathbb{Z}^+$ y $k \in \mathbb{Z}^+$ tales que $n = m^k$ si y solo si, todos los e_i son múltiplos de k.

Capítulo 2

Congruencias

2.1. Definiciones y primeras propiedades

Definición 2.1.1

Fijado $n \in \mathbb{Z}$, y dados $a, b \in \mathbb{Z}$, decimos que a es congruente con b módulo n y escribimos $a \equiv b \pmod{n}$ si $n|a-b$. En caso contrario, escribiremos $a \not\equiv b \pmod{n}$.

Proposición 2.1.1

1. La congruencia módulo n es una relación de equivalencia.
2. $a \equiv b \pmod{n}$ si y solo si $a \equiv b \pmod{(-n)}$.
3. $a \equiv b \pmod{n}$ si y sólo si a y b tienen el mismo resto al dividirlos entre n.
4. Dado $n \in \mathbb{Z}^+$, y $a \in \mathbb{Z}$ existe un único $r \in \{0, 1, \ldots, n-1\}$ tal que $a \equiv r \pmod{n}$ (r es el resto de dividir a entre n).

Ejemplo 2.1.1 (Propiedad cancelativa)

Observemos por ejemplo que $6 \equiv 16 \pmod{5}$; es decir, $2\times 3 \equiv 2\times 8 \pmod{5}$. En este caso podemos cancelar el 2 ya que claramente $3 \equiv 8 \pmod{5}$.
Ahora, porque podemos cancelar el 2?
La congruencia $6 \equiv 16 \pmod{5}$ es cierta pues $5|(16-6)$; factorizando el 2, tenemos que $5|2(8-3)$, y como 5 y 2 son coprimos, por el Lema de Euclides, obtenemos entonces $5|(8-3)$ y por lo tanto $3 \equiv 8 \pmod{5}$. Aquí utilizamos que $mcd(5,2) = 1$; esto es absolutamente necesario para poder cancelar y obtener una congruencia con el mismo modulo.

Ejemplo 2.1.2

Observar que $5 \equiv 10 \pmod{5}$; es decir $5\times 1 \equiv 5\times 2 \pmod{5}$ y sin embargo $1 \not\equiv 2 \pmod{5}$. Aquí no podemos cancelar el 5 pues el hecho de que $5|(10-5) = 5(2-1)$ no implica que $5|(2-1)$.

Proposición 2.1.2 Propiedades Cancelativas

Sea $a, b, c, n \in \mathbb{Z}$ con $c \neq 0$.

1. Si $ca \equiv cb \pmod{n}$ y $mcd(c, n) = 1$ entonces $a \equiv b \pmod{n}$.
2. Si $c|n$ y $ca \equiv cb \pmod{n}$ entonces $a \equiv b \pmod{\frac{n}{c}}$.
3. Si $ca \equiv cb \pmod{n}$ entonces $a \equiv b \pmod{\frac{n}{mcd(c,n)}}$.

Demostración:

1. Tenemos que $ca \equiv cb \pmod{n}$, es decir $n|(ca - cb)$. Entonces $n|c(a - b)$ y como $mcd(c, n) = 1$ por el Lema de Euclides obtenemos que $n|(a - b)$ y por lo tanto $a \equiv b \pmod{n}$.
2. Si $c|n$, existe un $k \in \mathbb{Z}$ tal que $n = ck$. Si ademas $ca \equiv cb \pmod{n}$ entonces $ck = n|c(a - b)$. Por lo tanto existe $e \in \mathbb{Z}$ tal que $c(a - b) = cke$, y como $c \neq 0$, por la cancelativa en $\mathbb{Z}$ tenemos que $a - b = ke$. Por lo tanto $k|(a - b)$ y entonces $a \equiv b \pmod{k}$, es decir $a \equiv b \pmod{\frac{n}{c}}$.
3. Si llamamos $d = mcd(c, n)$ tenemos que $c = dc^*$ y $n = dn^*$, con c^*, n^* enteros coprimos. Si $ca \equiv cb \pmod{n}$, entonces $dc^*a = dc^*b \pmod{dn^*}$, y por la parte anterior tenemos que $c^*a \equiv c^*b \pmod{n^*}$. Ahora como $mcd(c^*, n^*) = 1$, utilizando la primer parte para estos enteros obtenemos que $a \equiv b \pmod{n^*}$; es decir $a \equiv b \pmod{\frac{n}{mcd(c,n)}}$.

2.2. Algunas aplicaciones

Proposición 2.2.1

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

1. $a \equiv b \pmod{n}$ y $c \equiv b \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$ y $ac \equiv bd \pmod{n}$.
2. $b \equiv c \pmod{n} \Rightarrow a + b \equiv a + c \pmod{n}$.
3. $a \equiv b \pmod{n}$ y $m|n \Rightarrow a \equiv b \pmod{m}$.
4. $a \equiv b \pmod{m} \Rightarrow na \equiv nb \pmod{m}$.
5. $a \equiv b \pmod{m}$ y $n \in \mathbb{N} \Rightarrow a^n \equiv b^n \pmod{m}$.

2.2.1. Criterios de divisibilidad

Proposición 2.2.2

Si los dígitos de a son $a = a_k \dots a_1 a_0$. Entonces $3|a$ si y sólo si $3|a_0 + a_1 + \cdots + a_k$.

Demostración: Tenemos que $a = a_k 10^k + \dots a_1 10 + a_0$. Tenemos que $3|a$ si y sólo si $a \equiv 0 \pmod{3}$; es decir, si y solo si $a_k 10^k + \cdots + a_1 10 + a_0 \equiv 0 \pmod{3}$.
Ahora $10 \equiv 1 \pmod{3}$, y entonces (por la ultima propiedad de la proposición anterior) $10^i \equiv 1^i \pmod{3}$ para todo $i \in \mathbb{N}$. Así que $10^i \equiv 1 \pmod{3}$ y por lo tanto para todo $i = 0, \dots k$ tenemos que $a_i 10^i \equiv a_i \pmod{3}$ (por la propiedad (4)); y sumando, utilizando la propiedad (1) obtenemos que $a = a_k 10^k + \cdots + a_1 10 + a_0 \equiv a_k + \cdots + a_1 + a_0 \pmod{3}$.
Entonces (por la transitividad de la congruencia) $a \equiv 0 \pmod{3} \Leftrightarrow a_k + \cdots + a_1 + a_0 \equiv 0 \pmod{3}$; es decir 3 divida a a, si y sólo si 3 divide a la suma de sus dígitos. 😊

Proposición 2.2.3

Si los dígitos de a son $a = a_k \dots a_1 a_0$. Entonces $9|a$ si y sólo si $9|a_0 + a_1 + \cdots + a_k$.

2.2.2. Dígitos Verificadores

Definición 2.2.1: Código ISBN

El ISBN (International Standard Book Number) es una cadena de diez símbolos que identifica a los libros. Los primeros nueve símbolos con dígitos, y el ultimo el símbolo verificador.
Es entonces una cadena $x_1, x_2, \ldots, x_9 - x_{10}$, donde cada $x_1, x_2, \ldots, x_9$ es un dígito de 0 a 9, mientras que $x_{10} \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, X\}$. Al símbolo x_{10} se llama el símbolo verificador y se calcula de la siguiente manera:

$$c = \sum_{i=1}^{9} i \cdot x_i$$

y sea $r \in \{0, 1, \ldots, 10\}$ tal que $r \equiv c \pmod{11}$ (es decir, r el resto de dividir c entre 11). Entonces:

$$x_{10} = \begin{cases} r & \text{si } 0 \leq r \leq 9 \\ X & \text{si } r = 10 \end{cases}$$

Proposición 2.2.4

Sean $x_1 x_2 \ldots x_9 - x_{10}$ y $y_1 y_2 \ldots y_9 - y_{10}$ dos códigos ISBN. Sea k un entero tal que:

- $1 \leq k \leq 9$.
- $x_k \neq y_k$.
- $x_i = y_i$ para todo $i \leq 9, i \neq k$.

Entonces $x_{10} \neq y_{10}$.

Demostración: Supongamos que $x_{10} = y_{10}$; entonces tendríamos que

$$\sum_{i=1}^{9} i \cdot x_i \equiv \sum_{i=1}^{9} i \cdot y_{10} \pmod{11}$$

Pero en estas sumas tenemos que para $i \neq k$, $i \cdot x_i = i \cdot y_i$, y por lo tanto cancelando tendríamos que

$$k \cdot x_k \equiv k \cdot y_k \pmod{11}$$

y como $mcd(k, 11) = 1$, por la propiedad cancelativa tendríamos que $x_k \equiv y_k \pmod{11}$ lo cual es absurdo pues $x_k \neq y_k$ y son números entre 0 y 9. 😄

2.3. Ecuaciones con congruencias

Teorema 2.3.1

Dados $a, b, n \in \mathbb{Z}$ y sea $d = mcd(a, n)$. Entonces la ecuación $ax \equiv b \pmod{n}$ tiene solución si y sólo si $d|b$. Ademas, si $d|b$ existen exactamente d soluciones distintas al modulo n.

Demostración: Tenemos que $ax \equiv b \pmod{n}$ si y sólo si $n|(ax - b)$, si y sólo si $ax - b = ny$ para algún $y \in \mathbb{Z}$. Por lo tanto, la ecuación $ax \equiv b \pmod{n}$ tiene solución, si y solo si existen $x, y \in \mathbb{Z}$ tales que $ax - ny = b$. Por el Teorema de Ecuaciones Diofánticas, sabemos que esto sucede si y sólo si $d|b$.
Ahora, en el caso que $d|b$, si (x_0, y_0) es solución de la ecuación diofántica, tenemos (por el mismo teorema) que el conjunto de soluciones de la diofántica es $\{(x, y) = \left(x_0 + \frac{n}{d}k, y_0 + \frac{a}{d}k;\ k \in \mathbb{K}\right)\}$. Por lo tanto, las soluciones de la ecuación $ax \equiv b \pmod{n}$ son $x = x_0 + \frac{n}{d}k$, con $k \in \mathbb{Z}$.
Observar que $x_0, x_1 = x_0 + \frac{n}{d}, x_2 = x_0 + 2\frac{n}{d}, \ldots, x_{d-1} = x_0 + (d-1)\frac{n}{d}$ son d soluciones que no son congruentes entre ellas modulo n. Esto es porque si $i \neq j$, $0 \neq |x_i - x_j| = |x_0 + i\frac{n}{d} - x_0 - j\frac{n}{d}| = |(i-j)\frac{n}{d}| \leq (d-1)\frac{n}{d} < n$; por lo tanto $n \nmid x_i - x_j$ y entones $x_i \not\equiv x_j \pmod{n}$. Veamos ahora que cualquier otra solución es congruente (modulo n) a una de estas.
Si $x = x_0 + \frac{n}{d}k$, dividiendo k entre d, tenemos que $k = dq + i$ con $0 \leq i < d$, y por lo tanto $x = x_0 + \frac{n}{d}k = x_0 + \frac{n}{d}(dq + i) = x_0 + i\frac{n}{d} + qn = x_i + qn \equiv x_i \pmod{n}$. 😊

Definición 2.3.1

Decimos que un entero a es invertible modulo n, si existe otro entero x tal que $ax \equiv 1 \pmod{n}$. Al entero x se le llama inverso de a modulo n.

Corolario 2.3.1

Un entero a es invertible modulo n si y sólo si $mcd(a, n) = 1$. Ademas, si a es invertible, el inverso de a modulo n es único modulo n.

2.4. Teorema Chino del Resto

Teorema 2.4.1 Teorema Chino del Resto

Sean $m_1, m_2, \ldots, m_n$ enteros coprimos dos a dos y $a_1, a_2, \ldots, a_k \in \mathbb{Z}$. Entonces el sistema

$$\begin{cases} x \equiv a_1 & (mod\ m_1) \\ x \equiv a_2 & (mod\ m_2) \\ \quad \vdots & \\ x \equiv a_k & (mod\ m_k) \end{cases}$$

tiene solución, y hay una única solución modulo $m_1 m_2 \ldots m_k$. Es decir, si x_0 es solución, entonces todas las soluciones son $x \equiv x_0\ (mod\ m_1 m_2 \ldots m_k)$.

Demostración: Haremos la demostración por inducción en k (la cantidad de ecuaciones) partiendo del caso $k = 2$. Consideremos dos enteros m_1, m_2 coprimos $a_1, a_2 \in \mathbb{Z}$ y el sistema

$$\begin{cases} x \equiv a_1 & (mod\ m_1) \\ x \equiv a_2 & (mod\ m_2) \end{cases}$$

La primer congruencia equivale a que exista $s \in \mathbb{Z}$ tal que

$$x = a_1 + m_1 s$$

y la segunda equivale a que exista $t \in \mathbb{Z}$ tal que

$$x = a_2 + m_2 t$$

Por lo tanto, debemos encontrar $x \in \mathbb{Z}$ que verifique estas dos ultima condiciones, es decir, que existe $x \in \mathbb{Z}$ que verifica las congruencias si y solo si

$$\exists s, t \in \mathbb{Z} :\ a_1 + m_1 s = a_2 + m_2 t$$

Es decir, si y solo si

$$\exists s, t \in \mathbb{Z} :\ m_1 s - m_2 t = a_2 - a_1$$

Como $mcd(m_1, m_2) = 1$, por el teorema de Ecuaciones Diofánticas, esta ultima ecuación tiene solución.
Ademas, dada una particular (s_0, t_0), todas las soluciones de la diofántica son $(s, t) = (s_0 + m_2 k, t_0 + m_1 k)$ tal que $k \in \mathbb{Z}$. Ahora sustituyendo el s de estas soluciones, obtenemos que $x = a_1 + m_1 s = a_1 + m_1(s_0 + m_2 k) = a_1 + m_1 s_0 + m_1 m_2 k,\ k \in \mathbb{Z}$.
Si llamamos $x_0 = a_1 + m_1 s_0$, tenemos que las soluciones de las dos congruencias son

$$x = x_0 + m_1 m_2 k,\ k \in \mathbb{Z}$$

Es decir, que el sistema tiene solución x_0 y todas las soluciones son $x \equiv x_0\ (mod\ m_1 m_2)$.
Así que obtuvimos una única solución módulo $m_1 m_2$.
Ahora, el paso inductivo: sea $k > 2$ y asumamos que el teorema es cierto para $k - 1$, probemos que es cierto para k ecuaciones. Por la hipótesis inductiva tenemos que el sistema

$$\begin{cases} x \equiv a_1 & (mod\ m_1) \\ x \equiv a_2 & (mod\ m_2) \\ \quad \vdots & \\ x \equiv a_{k-1} & (mod\ m_{k-1}) \end{cases}$$

tiene solución x_1 y que ademas cualquier solución cumple que $x \equiv x_1\ (mod\ m_1 m_2 \ldots m_{k-1})$; por lo tanto, este sistema con $k - 1$ ecuaciones es equivalente a la ecuación $x \equiv x_1\ (mod\ m_1 m_2 \ldots m_{k-1})$.

Entonces el sistema con k ecuaciones

$$\begin{cases} x \equiv a_1 & (mod\ m_1) \\ x \equiv a_2 & (mod\ m_2) \\ \quad \vdots & \\ x \equiv a_{k-1} & (mod\ m_{k-1}) \\ x \equiv a_k & (mod\ m_k) \end{cases}$$

es equivalente al sistema

$$\begin{cases} x \equiv x_1 & (mod\ m_1 m_2 \dots m_{k-1}) \\ x \equiv a_k & (mod\ m_k) \end{cases}$$

Como los enteros $m_1, m_2 \dots, m_k$ son coprimos dos a dos, tenemos que $mcd(m_1 m_2 \dots m_{k-1}, m_k) = 1$. Por lo tanto tenemos un sistema con 2 ecuaciones que involucran módulos coprimos. Por lo ya probado para $k = 2$, tenemos entonces que este ultimo sistema tiene solución $x_0 \in \mathbb{Z}$ y ademas que toda solución cumple $x \equiv x_0\ (mod(m_1 m_2 \dots m_{k-1}) \cdot k)$.
Por lo tanto el sistema tiene solución x_0, y las soluciones son $x \equiv x_0\ (mod\ m_1 m_2 \dots m_{k-1} m_k)$; es decir, la solución es única módulo $m_1 m_2 \dots m_k$. 😊

Corolario 2.4.1

Generalizando el teorema, tenemos que si $m_1, \dots, m_k$ no son coprimos dos a dos, entonces el sistema puede o no tener solución.
En caso de que tenga una solución x_0, todas las soluciones son

$$x \equiv x_0\ (mod\ mcm(m_1, m_2, \dots, m_k))$$

2.5. Exponenciación y Teoremas de Fermat y Euler

Definición 2.5.1

La función de Euler es $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ dada por

$$\varphi(n) = \#\{a \in \{1, \ldots, n\} : mcd(a, n) = 1\}$$

Es decir, que la función de Euler cuenta la cantidad de naturales coprimos con n y menores que n.

Proposición 2.5.1

Si p es primo, entonces $\varphi(p) = \#\{1, 2, \ldots, p-1\} = p - 1$.

Proposición 2.5.2

Si p es primo, obtengamos una formula para obtener $\varphi(p^k)$, tenemos que

$$\varphi(p^k) = \#\{a \in \{1, 2, \ldots, p^k\} : mcd(a, p^k) = 1\} = \#\{a \in \{1, 2, \ldots, p^k\} : mcd(a, p) = 1\}$$

Entonces:

$$\varphi(p^k) = \#\{1, 2, \ldots, p^k\} - \#\{a \in \{1, 2, \ldots, p^k\} : mcd(a, p) \neq 1\}$$

Por lo tanto

$$\varphi(p^k) = p^k - \#\{a \in \{1, 2, \ldots, p^k\} : mcd(a, p) \neq 1\}$$

Ahora, como p es primo, tenemos que $mcd(a, p) \neq 1 \Leftrightarrow a = pk$ para algún $k \in \mathbb{Z}$. Por lo tanto $\{a \in \{1, \ldots, p^k\} : mcd(a, p) \neq 1\} = \{a = pk \text{ con } k \in \{1, 2, \ldots, p^{k-1}\}\}$ y el cardinal de este conjunto es p^{k-1}. Sustituyendo obtenemos que

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

Teorema 2.5.1

Si $mcd(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

Demostración: Como la tesis es obvia si m o n es 1, demostremoslo para $m, n > 1$. La idea de la demostración es la siguiente: daremos dos conjuntos C y D tales que tales que $\#C = \varphi(mn)$ y $\#D = \varphi(m)\varphi(n)$, y lego construiremos una función biyectiva $f : C \to D$ lo cual terminaría probando que $\#C = \#D$; es decir que $\varphi(mn) = \varphi(m)\varphi(n)$.
Sea $C = \{c \in \{0, \ldots, mn-1\} : mcd(c, mn) = 1\}$; claramente $\#C = \varphi(mn)$. Ademas, tenemos que

$$mcd(c, mn) = 1 \Leftrightarrow mcd(c, m) = 1 \text{ y } mcd(c, n) = 1$$

Así que $C = \{c \in \{0, \ldots, mn\} : mcd(c, m) = 1 \text{ y } mcd(c, n) = 1\}$.
Sea $A = \{a \in \{0, \ldots, m-1\} : mcd(a, m) = 1\}$ y $B = \{b \in \{0, \ldots, n-1\} : mcd(b, n) = 1\}$; tenemos que $\#A = \varphi(m)$ y $\#B = \varphi(n)$ y por lo tanto si $D = A \times B = \{(a, b) : a \in A,\ b \in B\}$ tenemos que $\#D = \varphi(m)\varphi(n)$.
Consideramos ahora la función $f : C \to D$ dada por $f(c) = (a, b)$ siendo a el resto de dividir c entre m y b el resto de dividir c entre n. Es decir $f(c) = (a, b)$ con $a \in \{0, \ldots, m-1\}, b \in \{0, \ldots, n-1\}$ y

$$\begin{cases} c \equiv a \pmod{m} \\ c \equiv b \pmod{n} \end{cases}$$

Veamos primero que efectivamente, si $c \in C$ y $f(c) = (a, b)$, entonces $(a, b) \in D$. Como $c = mq + a$ y $c = nq' + b$ tenemos que

$$mcd(c, m) = mcd(a, m) \text{ y } mcd(c, n) = mcd(b, n)$$

Por lo tanto si $mcd(c,m) = 1$ y $mcd(c,n) = 1$ tenemos que $mcd(a,m) = 1$ y $mcd(b,n) = 1$. Como ademas claramente $a \in \{0,\dots,m-1\}$ y $b \in \{0,\dots,n-1\}$ concluimos que $(a,b) \in D$.
Veamos ahora que la función f es biyectiva. Para esto tenemos que ver que dado $(a,b) \in D$, existe un único $c \in C$ tal que $f(c) = (a,b)$ (la existencia de c nos da la sobreyectividad de f y la unicidad nos da la inyectividad de f). Tenemos que probar entonces que dado $(a,b) \in D$ existe un único $c \in C$ tal que

$$\begin{cases} c \equiv a \pmod{m} \\ c \equiv b \pmod{n} \end{cases}$$

Como $mcd(m,n) = 1$, por el Teorema Chino del resto sabemos que el sistema tiene solución c_0, todas las soluciones son $c \equiv c_0 \ (mod mn)$. Por lo tanto, existe un único $c \in \{0,\dots,mn-1\}$ que verifica el sistema. Resta ver que efectivamente este $c \in C$: como $mcd(a,m) = 1$, $mcd(b,n) = 1$ y $c \equiv a \ (mod m)$, $c \equiv b \ (mod n)$, tenemos que

$$mcd(c,m) = 1 \text{ y } mcd(c,n) = 1$$

y por lo tanto $c \in C$. 😊

Corolario 2.5.1

Sea $n \in \mathbb{Z}^+$

1. Si n tiene descomposición factorial $n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$ (con los p_i primos distintos y $e_i > 0$), entonces:

$$\varphi(n) = \left(p_1^{e_1} - p_1^{e_1-1}\right)\left(p_2^{e_2} - p_2^{e_2-1}\right)\dots\left(p_k^{e_k} - p_k^{e_k-1}\right)$$

2. $\varphi(n) = n \prod_{p \text{ primo},\ p|n} \left(1 - \frac{1}{p}\right)$

Demostración: 1. Como los p_i son primos distintos, tenemos que los $p_i^{e_i}$ son coprimos 2 a 2, y por lo visto en el teorema anterior, reiteradas veces obtenemos que

$$\varphi(n) = \varphi(p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}) = \varphi(p_1^{e_1})\varphi(p_2^{e_2})\dots\varphi(p_k^{e_k})$$

y utilizando la formula 2.5 obtenemos lo deseado.

2. Como cada $(p_i^{e_i} - p_i^{e_i-1}) = p_i^{e_i}\left(1 - \frac{1}{p_i}\right)$ sustituyendo en la formula recién obtenida nos queda que

$$\begin{aligned} \varphi(n) &= p_1^{e_1}\left(1 - \frac{1}{p_1}\right) p_2^{e_2}\left(1 - \frac{1}{p_2}\right)\dots p_k^{e_k}\left(1 - \frac{1}{p_k}\right) \\ &= p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_k}\right) \\ &= n \prod_{p \text{ primo},\ p|n} \left(1 - \frac{1}{p}\right) \end{aligned}$$

😊

Teorema 2.5.2 Teorema de Euler

Sean $n, a \in \mathbb{Z}$ tales que $mcd(a,n) = 1$, entonces

$$a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

Demostración: Sea $B = \{b \in \{1, \ldots, n\} : mcd(b, n) = 1\}$; claramente $\#B = \varphi(n)$. Observar que si $b \in B$ en particular $mcd(b, n) = 1$, y como $mcd(a, n) = 1$ tenemos que tambien $mcd(ab, n) = 1$. Por lo tanto (tomando el resto de dividir ab entre n), existe un unico $b' \in B$ tal que $ab \equiv b' \ (mod\ n)$. Ademas, dados dos elementos distintos de B, b_1 y b_2, al multiplicarlos por a obtenemos enteros no congruentes modulo n, ya que si $ab_1 \equiv ab_2 \ (mod\ n)$, al ser $mcd(a, n) = 1$ podemos cancelar a y obtendriamos $b_1 \equiv b_2 \ (mod\ n)$, lo cual es absurdo ya que en B no hay dos elementos congruentes modulo n. Por lo tanto, si multiplicamos por a a todos los elementos de B, y luego tomamos los restos de dividir entre n, volvemos a obtener todos los elementos de B (permutados).
Entonces

$$\prod_{b \in B} ab \equiv \prod_{b' \in B} b' \ (mod\ n) \Rightarrow \prod_{b \in B} ab \equiv \prod_{b \in B} b \ (mod\ n)$$

En la izquierda, el factor a aparece $\#B = \varphi(n)$ veces, por lo que obtenemos

$$a^{\varphi(n)} \prod_{b \in B} b \equiv \prod_{b \in B} b \ (mod\ n)$$

y como cada $b \in B$ es coprimo con n, no lo podemos cancelar de la congruencia y obtenemos

$$a^{\varphi(n)} \equiv 1 \ (mod\ n)$$

😄

Corolario 2.5.2 Teorema de Fermat

Si p es primo y $a \in \mathbb{Z}$ tal que $p \nmid a$, entonces

$$a^{p-1} \equiv 1 \ (mod\ p)$$

Corolario 2.5.3

Sean a, n dos enteros coprimos

- Si $m \in \mathbb{Z}$ y $m = \varphi(n)q + r$ entonces $a^m \equiv a^r \ (mod\ n)$.
- Si $m \equiv k \ (mod\ \varphi(n))$ entonces $a^m \equiv a^k \ (mod\ n)$.

Demostración:

1. Si $m = \varphi(n)q + r$ entonces

$$a^m = a^{\varphi(n)q+r} = \left(a^{\varphi(n)}\right)^q a^r \equiv 1^q a^r \ (mod\ n) \equiv a^r \ (mod\ n)$$

2. Es claro a partir de lo anterior.

😄

Capítulo 3

Teoría de Grupos

3.1. Definición y propiedades

Definición 3.1.1

Un grupo es un conjunto G con una operación binaria $* : G \times G \to G$ tal que

- (asociativa) $x * (y * z) = (x * y) * z \ \forall x, y, z \in G$.
- (neutro) existe un elemento $e \in G$ tal que $e * x = x$ y $x * e = x \ \forall x \in G$.
- (inverso) para todo elemento $g \in G$, existe $g' \in G$ tal que $g * g' = e$ y $g' * g = e$.

En general escribimos al grupo como $(G, *)$ o $(G, *, e)$. Si la operación y neutro son claros simplemente notamos G.

Proposición 3.1.1

Sea $(G, *)$ un grupo y $g, h \in G$. Entonces:

1. El neutro de G es único.
2. $\forall g \in G$, el inverso de g es único (y lo escribimos g^{-1}; si la operación es una suma, generalmente lo llamamos opuesto y lo escribimos $-g$).
3. Si e es el neutro de G, entonces $e^{-1} = e$.
4. El inverso de g^{-1} es g.
5. $(gh)^{-1} = h^{-1}g^{-1}$.
6. Propiedad cancelativa a derecha: si $g, x, h \in G$ y $gx = hx$, entonces $g = h$.
7. Propiedad cancelativa a izquierda: si $g, x, h \in G$, y $xg = xh$, entonces $g = h$.
8. Soluciones de ecuaciones a derecha: si $g, h \in G$, entonces existe un único $x \in G$ tal que $gx = h$.
9. Soluciones de ecuaciones a izquierda: si $g, h \in G$, entonces existe un único $x \in G$ tal que $xg = h$.
10. (un inverso a izquierda es el inverso) Si $g' * g = e$ entonces $g' = g^{-1}$.
11. (un inverso a derecha es el inverso) Si $g * g' = e$ entonces $g' = g^{-1}$.

3.2. Grupos de permutacion

Definición 3.2.1

Un grupo de permutaciones es un conjunto de funciones que reordenan los elementos de un conjunto finito y que, al componerlas, siguen siendo permutaciones del mismo conjunto. El grupo de permutaciones de un conjunto finito de n elementos se denota como S_n, es decir, para cada $n \in \mathbb{Z}^+$ llamamos

$$S_n = \{f : \{1, 2, \ldots, n\} \to \{1, 2, \ldots, n\} : f \text{ es una función biyectiva}\}$$

Y ademas, $|S_n| = n!$

Ejemplo 3.2.1

Si $n = 2$, en S_2 tenemos dos funciones, Id (la función identidad) y la función f tal que $f(1) = 2$ y $f(2) = 1$.

Proposición 3.2.1

$(S_n, \circ, Id)$ es un grupo.

Utilizaremos la siguiente notación: a una función en S_n la escribiremos como una matriz, cuya primera fila consta de los números del 1 al n en orden, y en su segunda fila escribiremos $f(1), f(2), \ldots, f(n)$.

Ejemplo 3.2.2

$S_2 = \left\{ Id = \begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix}, \tau = \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix} \right\}$.

Observar en este caso que $\tau \circ \tau = Id$.

Ejemplo 3.2.3

$S_3 = \{Id = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \tau_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \tau_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \tau_3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$

$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \sigma_2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\}$

En este caso por ejemplo, $\tau_1 \circ \tau_2 = \sigma_1$ y $\tau_2 \circ \tau_1 = \sigma_2$ y por lo tanto S_3 no es abeliano. En general, si $n \geq 3$ S_n no es abeliano.

3.3. Tablas de Cayley

Para grupos de orden finito puede resultar conveniente escribir la tabla de multiplicación. A esta tabla se la conoce como Tabla de Cayley del grupo, y se construye de la siguiente manera: se colocan los elementos de G arriba de la tabla, y en el mismo orden también a la izquierda de la tabla; luego en la entrada correspondiente a la fila del elemento g y a la columna del elemento h colocamos $g * h$.

Ejemplo 3.3.1

La tabla de Cayley de S_2 es

$\circ$	Id	τ
Id	Id	τ
τ	τ	Id

Ejemplo 3.3.2

Algunas de las entradas de la Tabla de Cayley de S_3 son

$\circ$	Id	τ_1	τ_2	τ_3	σ_1	σ_2
Id	Id	τ_1	τ_2	τ_3	σ_1	σ_2
τ_1	τ_1	Id	σ_1			
τ_2	τ_2		Id			
τ_3	τ_3			Id		
σ_1	σ_1				σ_1	Id
σ_2	σ_2				Id	σ_1

Proposición 3.3.1

En la tabla de Cayley de un grupo, cada elemento de G aparece exactamente una vez en cada fila y columna. Es decir, que cada columna y cada fila de la tabla es una premutacion de los elementos de G.

Demostración: El elemento h aparece en la fila correspondiente a g y en la columna correspondiente a x, si y solo si $gx = h$. Ya vimos que dados g y h en G existe un único $x \in G$ tal que $gx = h$. Por lo tanto, en la fila de g el elemento h aparece una sola vez (en la columna x). De forma análoga probamos que cada elemento aparece una sola vez en cada columna. 😊

3.4. El grupo de enteros módulo n

Definición 3.4.1: Clase de congruencia

Una clase $\overline{z}$ es un conjunto de números enteros que comparten el mismo residuo cuando se dividen por un número entero (módulo).

$$\overline{z} = \{x \in \mathbb{Z} |\ x \equiv z\ (mod\ n)\}$$

Definición 3.4.2

Llamaremos $\mathbb{Z}_n$ al conjunto de clases de modulo n. Por ejemplo $\mathbb{Z}_2 = \{\overline{0}, \overline{1}\}$ y $\mathbb{Z}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$. Es claro entonces que $\mathbb{Z}_n$ tiene n elementos; es decir $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$.

Corolario 3.4.1

Queremos definir en $\mathbb{Z}_n$ una operación que le de estructura de grupo. Quisiéramos definir una operación que llamaremos suma y la escribiremos como $+$, de forma mas natural $\overline{a} + \overline{b} = \overline{a+b}$.

Ejemplo 3.4.1

En $\mathbb{Z}_5$ tendríamos que $\overline{3} + \overline{4} = \overline{3+4} = \overline{7} = \overline{2}$.

Proposición 3.4.1

Sea $n \in \mathbb{Z}$, entonces $(\mathbb{Z}_N, +)$ es un grupo abeliano.

Demostración: Veamos que la operación antes definida es asociativa: sean $a, b, c \in \mathbb{Z}$, entonces $(\overline{a} + \overline{b}) + \overline{c} \overset{\text{def}}{=} \overline{(a+b)} + \overline{c} \overset{\text{def}}{=} \overline{(a+b)+c}$. Ahora, como la suma de enteros es asociativa, tenemos que $\overline{(a+b)+c} = \overline{a+(b+c)} \overset{\text{def}}{=} \overline{a} + \overline{b+c} \overset{\text{def}}{=} \overline{a} + (\overline{b} + \overline{c})$. Claramente $\overline{0}$ es neutro de esta operación 😄

Proposición 3.4.2

Dados dos grupos $(G, *, e_G)$, $(K, *, e_K)$ si consideramos el conjunto $G \times K = \{(g,k) : g \in G, k \in K\}$ con la operación coordenada a coordenada: $(g,k)(g',k') = (g * g', k * k')$, entonces obtenemos un nuevo grupo (llamado el producto directo de G y K).

3.5. El grupo de los invertibles módulo n

Corolario 3.5.1

De manera análoga a la suma de clases en $\mathbb{Z}_n$, podemos definir el producto de clases:

$$\overline{a} \times \overline{b} = \overline{ab}$$

Definición 3.5.1

Llamamos $U(n)$ al conjunto de todas las clases de z modulo n que sean coprimos con n. Formalmente lo definimos como

$$U(n) = \{\overline{a} : mcd(a, n) = 1\}$$

Ejemplo 3.5.1

Por ejemplo $U(4) = \{\overline{1}, \overline{3}\}$, $U(5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$ y $U(8) = \{\overline{1}, \overline{3}, \overline{5}, \overline{7}\}$.

Corolario 3.5.2

Observar que $|U(n)| = \varphi(n)$.

Proposición 3.5.1

$(U(n), \times, \overline{1})$ es un grupo abeliano con $\varphi(n)$ elementos.

3.6. Grupos Dihedrales

Definición 3.6.1: Grupos dihedrales

Estos grupos describen las simetrías de figuras geométricas regulares, como polígonos y poliedros. El grupo dihedrico de orden n, denotado como D_n, consiste en todas las transformaciones rígidas (geométricas) que preservan las propiedades del objeto original. Estas transformaciones pueden ser rotaciones y reflexiones. La cantidad de elementos en el grupo dihedrico D_n es $2n$, donde n es el número de lados del polígono o caras del poliedro.

Ejemplo 3.6.1

Tomando $n = 3$, consideremos en el plano, un triangulo equilátero T. Sea $D_3 = \{f : \mathbb{R}^2 \to \mathbb{R}^2 : f$ es un movimiento del plano y $f(T) = T\}$. Entonces en D_3 tenemos al movimiento identidad, id; también las simetrías axiales s_1, s_2, s_3 con ejes en las mediatrices de los lados de T, y ademas tenemos las rotaciones antihorarias r_1 y r_2 con centro el centro del triangulo y ángulos 120 y 240 grados respectivamente.
Entonces:

$$D_3 = \{id, r_1, r_2, s_1, s_2, s_3\}$$

Es claro que si dos movimientos del plano preservan el triangulo, entonces su composición también.

Proposición 3.6.1

$(D_3, \circ, id)$ es un grupo de orden 6. Este grupo se llama grupo dihedral.

Demostración: Ya vimos que la composición de dos elementos de D_3 es nuevamente un elemento de D_3. La función id es el neutro de la composición así que resta ver que todo elemento de D_3 tiene inverso:

- Claramente $(id)^{-1} = id$.
- Para todo $i = 1, 2, 3$, tenemos que $s_i \circ s_i = id$ y por lo tanto cada simetría es inversa de si misma.
- Tenemos que $r_1 \circ r_2 = id$ y por lo tanto $(r_1)^{-1} = r_2$ y $(r_2)^{-1} = r_1$.

😄

Corolario 3.6.1

Observar que $s_1 \circ r_1 = s_2$ y $r_1 \circ s_1 = s_3$, por lo tanto D_3 no es abeliano.

Proposición 3.6.2

Por simplicidad notaremos $s = s_1$ y $r = r_1$. Tenemos las siguientes propiedades:

1. $D_3 = \{id, s, sr, sr^2, r, r^2\}$.
2. $r^3 = id$.
3. $s^2 = id$.
4. $rs = sr^2$.
5. Las relaciones anteriores (y la asociatividad) son suficientes para obtener todas las multiplicaciones en D_3.

Ejemplo 3.6.2

Para $n = 4$, se considera un cuadrado C en el plano y $D_4 = \{f : \mathbb{R}^2 \to \mathbb{R}^2 : f$ es un movimiento del plano y $f(C) = C\}$.
En D_4 tenemos el movimiento identidad id, cuatro simetrías axiales s_1, s_2, s_3, s_4 y tres rotaciones antihorarias r_1, r_2, r_3 con centro en el centro del cuadrado y ángulos $90, 180$ y 270 grados. Así que tenemos

$$D_4 = \{id, r_1, r_2, r_3, s_1, s_2, s_3, s_4\}$$

Y en este caso tenemos que $s_2 = s_1 \circ r_1^3$, $s_3 = s_1 \circ r_1^2$, $s_4 = s_1 \circ r_1$, $r_2 = r_1^2$ y $r_3 = r_1^3$.

Proposición 3.6.3

De forma analoga a lo hecho con D_3, se prueba que $(D_4, \circ, id)$ es un grupo no abeliano (con 8 elementos). En este caso, si llamamos $s = s_1$ y $r = r_1$ tenemos que

1. $D_4 = \{id, r, r^2, r^3, s, sr, sr^2, sr^3\}$.
2. $r^4 = id$.
3. $s^2 = id$.
4. $rs = sr^3$.
5. Las relaciones anteriores (y la asociatividad) son suficientes para obtener todas las multiplicaciones en D_4.

Proposición 3.6.4

$(D_n, \circ, id)$ es un grupo no abeliano y $|D_n| = 2n$. Estos grupos se llaman grupos dihedrales.
En este caso general, si llamamos $s = s_1$ y $r = r_1$ es la rotación antihoraria con centro en el centro del polígono y angulo $\frac{360}{n}$ grados, tenemos que

1. $D_n = \{id, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$.
2. $r^n = id$.
3. $s^2 = id$.
4. $rs = sr^{n-1}$.
5. Las relaciones anteriores (y la asociatividad) son suficientes para obtener todas las multiplicaciones en D_n.

3.7. Subgrupos y grupos cíclicos

Definición 3.7.1

Dado un grupo $(G, *, e)$, un subconjunto $H \subset G$ es un subgrupo de G si cumple:

1. (Cerrado con la operación) para todo $h, h' \in H,\ h * h' \in H$.
2. (Neutro) $e \in H$.
3. (Cerrado por inversos) si $h \in H$, entonces $h^{-1} \in H$.

Escribiremos $H < G$ cuando H es un subgrupo de G.
Claramente un subgrupo es en particular un grupo con la misma operación de G.

Definición 3.7.2

Si $(G, *, e)$ es un grupo definimos las potencias de g como $g^0 = e$ y si $n \in \mathbb{Z}^+$ entonces

$$g^n = \underbrace{g * g * \cdots * g}_{\text{n veces}}$$

$$g^{-n} = \underbrace{g^{-1} * g^{-1} * \ldots g^{-1}}_{\text{n veces}}$$

Proposición 3.7.1

Para todo $g \in G$ y $m, n \in \mathbb{Z}$, se cumple:

1. $g^n * g^m = g^{n+m}$.
2. $g^{-n} = (g^n)^{-1}$.
3. $(g^n)^m = g^{mn}$.

Definición 3.7.3

Si $(G, *, e)$ es un grupo y $g \in G$, al conjunto de todas las potencias de g lo escribiremos $\langle g \rangle$; es decir

$$\langle g \rangle = \{g^n : n \in \mathbb{Z}\}$$

Como $g^0 = e$, tenemos que $e \in \langle g \rangle$; ademas, por las dos primeras propiedades de la proposición anterior, tenemos que $\langle g \rangle$ es cerrado con la operación y cerrado por inversos y por lo tanto $\langle g \rangle$ es un subgrupo de G, al que llamamos subgrupo generado por g. En el caso en que para G, exista un elemento $g \in G$ tal que $\langle g \rangle = G$ decimos que G es un grupo cíclico generado por g (o decimos que g es generador de G).

Definición 3.7.4

Sea $(G, *, e)$ un grupo y $g \in G$. Definimos el orden del elemento g y lo escribiremos $o(g)$, de la siguiente manera:

- Si $g^n \neq e\ \forall n \in \mathbb{Z}^+$, decimos que $o(g) = \infty$.
- En caso contrario, definimos $o(g) = min\{n \in \mathbb{Z}^+ : g^n = e\}$.

Proposición 3.7.2

Si $(G, *, e)$ es un grupo y $g \in G$ entonces:

1. Si $n \in \mathbb{Z}^+$, tenemos que
$$o(g) = n \Leftrightarrow \begin{cases} g^n = e \\ \text{si } g^m = e \Rightarrow n|m \end{cases}$$
2. Si $n \in \mathbb{Z}^+$ entonces $o(g) = n$ si y solo si $\begin{cases} g^n = e \\ g^d \neq e \ \forall \ d|n, \ d \neq n, \ d > 0 \end{cases}$.
3. Si $n \in \mathbb{Z}^+$ entonces $o(g) = n$ si y solo si $\begin{cases} g^n = e \\ g^{\frac{n}{p}} \neq e \ \forall \ p|n, \ p \neq n, \ p \text{ primo} \end{cases}$.
4. Se tiene que $g^m = e \Leftrightarrow o(g)|m$.
5. Si $o(g)$ es finito, entonces $g^m = g^k$ si y solo si $m \equiv k \pmod{o(g)}$.
6. Si $o(g) = \infty$ y $m \neq k$ entonces $g^m \neq g^k$.
7. Si $o(g)$ es finito y $k \in \mathbb{Z}$ entonces $o(g^k) = \frac{o(g)}{mcd(k, o(g))}$.
8. Si $o(g)$ es finito y $k \in \mathbb{Z}$, entonces $o(g) = o(g^k)$ si y solo si $mcd(k, o(g)) = 1$.

Demostración: 1. Veamos primero el directo: si $n = o(g)$, por definición tenemos que $g^n = e$. Ademas, si $g^m = e$, dividiendo m entre n tenemos que $m = qn + r$ con $0 \leq r < n$. Tenemos que $e = g^m = g^{nq+r} = (g^n)^q g^r = e^q g^r = g^r$. Por lo tanto $g^r = e$ y como n es la menor potencia positiva de g con la que se obtiene e, y $0 \leq r < n$ concluimos que debe ser $r = 0$ y por lo tanto $n|m$.
Para el reciproco es evidente que si $n \in \mathbb{Z}^+$, $g^n = e$ y si cada vez que $g^m = e$ se tiene que $n|m$, entonces n es la menor potencia positiva de g con la cual se llega a e y por lo tanto $n = o(g)$.

2. Para el directo, si $n = o(g)$, por la definición sabemos que $g^n = e$. Ahora, si $g^d = e$ con $d|n, \ d \neq n$, por la primera parte sabemos que $n|d$, lo que implica que $n = d$ lo cual contradice la hipótesis sobre d. Concluimos que no existe tal d.
Para el reciproco, supongamos que $m = o(g) \neq n$, que por definición de orden cumple $m < n$. Sabemos que $g^m = e$ y por la parte 1, $m|n$, que contradice la hipótesis. Por lo tanto $n = o(g)$.

3. El directo es similar a la demostración anterior ya que $\frac{n}{p}|n$.
El reciproco también es similar al anterior, supongamos que $m = o(g) \neq n$, de vuelta $m < n$. Por la parte 1, vemos que $m|n$ y como $m < n$ existe un primo p tal que $p|n$ y $m|\frac{n}{p}$. Como $g^m = e$, entonces $g^{\frac{n}{p}} = e$ contradiciendo la hipótesis. Concluimos que $o(g) = n$.

4. Se puede deducir de la primer parte de la proposición.

5. Tenemos que $g^m = g^k$ si y solo si $g^m(g^k)^{-1} = e$; si y solo si, $g^{m-k} = e$. Y por la primer parte, esto sucede si y solo si $o(g)|(m-k)$; es decir, si y solo si $m \equiv k \pmod{o(g)}$.

6. Supongamos que $m > k$; si tuviéramos que $g^m = g^k$, tendríamos que $g^{m-k} = e$ con $m - k > 0$ y por lo tanto tendríamos que $o(g)$ es finito.

7. Llamemos $n = o(g)$, y $d = mcd(n, k)$. Entonces tenemos que $n = dn'$, $k = dk'$ siendo n' y k' enteros coprimos. Entonces queremos probar que $o(g^k) = n'$. Usando la primer parte, debemos probar dos cosas: que $(g^k)^{n'} = e$ y que si $(g^k)^m = e$ entonces $n'|m$. Veamos lo primero: $(g^k)^{n'} = (g^{dk'})^{n'} = g^{dn'k'} = g^{nk'} = (g^n)^{k'} = e^{k'} = e$.
Para lo segundo: si $(g^k)^m = e$ entonces $g^{km} = e$ y como $n = o(g)$, por la primer parte tenemos que $n|(km)$. Cancelando d obtenemos que $n'|(k'm)$, y como $mcd(n', k') = 1$, por el Lema de Euclides concluimos que $n'|m$.

8. Es claro por la parte anterior.

😄

Proposición 3.7.3

Si $(G, *, e)$ es un grupo y $g \in G$ entonces

$$|\langle g \rangle| = o(g)$$

Demostración: Si $o(g) = \infty$, por la parte 4 de la proposición, si $m \neq k$ tenemos que $g^m \neq g^k$ y por lo tanto en $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$ no hay elementos repetidos, y entonces $|\langle g \rangle| = \#\{g^k : k \in \mathbb{Z}\} = \infty = o(g)$.
Ahora si $o(g) = n$ es finito, por la parte 3 de la proposición anterior tenemos que $g^m = g^k$ si y solo si $k \equiv m \pmod{n}$ y por lo tanto $\langle g \rangle = \{g^k : k \in \mathbb{Z}\} = \{g^0 = e, g, g^2, \ldots, g^{n-1}\}$ y entonces $|\langle g \rangle| = \#\{g^0 = e, g, g^2, \ldots, g^{n-1}\} = n = o(g)$. 😄

Corolario 3.7.1

sea G un grupo de orden finito, entonces:

1. G es cíclico si y solo si existe $g \in G$ tal que $o(g) = |G|$.
2. Si $G = \langle g \rangle$, entonces $G = \langle g^k \rangle$ si y solo si $mcd(k, |G|) = 1$.
3. Si $G = \langle g \rangle$ entonces G tiene $\varphi(|G|)$ generadores distintos.

Demostración:

1. G es es cíclico si y solo si existe $g \in G$ tal que $\langle g \rangle = G$. Como $|G|$ es finito, esto sucede si y solo si existe $g \in G$ tal que $|\langle g \rangle| = |G|$. Y como $|\langle g \rangle| = o(g)$ queda demostrada la primera parte.
2. Tenemos que $G = \langle g^k \rangle$ si y solo si $|G| = o(g^k)$. Como $|G| = o(g)$, tenemos que $G = \langle g^k \rangle$ si y solo si $o(g^k) = o(g)$ y por la parte 8 de la proposición anterior, tenemos que $o(g^k) = o(g)$ si y solo si $mcd(k, o(g)) = 1$ y como $o(g) = |G|$ se concluye lo deseado.
3. Al ser $G = \langle g \rangle$ y G finito, tenemos que $G = \{e = g^0, g, g^2, \ldots, g^{|G|-1}\} = \{g^k : k \in \{0, \ldots, |G| - 1\}\}$.
Junto con lo visto en la parte anterior concluimos que $\{h \in G : \langle h \rangle = G\} = \{g^k : k \in \{0, \ldots, |G| - 1\}$ y $mcd(k, |G|) = 1\}$ y este conjunto tiene cardinal $\varphi(|G|)$.

😄

Proposición 3.7.4

Sea G un grupo cíclico, entonces todo subgrupo de G también es cíclico.

3.8. Teorema de Lagrange

Teorema 3.8.1 Teorema de Lagrange

Si G es un grupo finito y $H < G$, entonces $|H|$ divide a $|G|$.

Demostración: La idea de la demostración es la siguiente: definiremos en G una relación de equivalencia de forma tal que si C es una clase de equivalencia, entonces $\#C = |H|$. Entonces, como G es finito, la cantidad de clases de equivalencia también lo es; sean $C_1, C_2, \ldots, C_k$ las clases de equivalencia distintas. Sabemos que el conjunto de clases de equivalencia (de cualquier relación de equivalencia) es una partición de G; es decir que $G = C_1 \cup C_2 \cup \cdots \cup C_k$ y esta unión es disjunta. Por lo tanto tendremos que $|G| = \#C_1 + \#C_2 + \cdots + \#C_k = \underbrace{|H| + |H| + \cdots + |H|}_{k \text{ veces}} = k|H|$ y por lo tanto obtendremos que $|H|$ divide a $|G|$.

Resta entonces definir la relación de equivalencia en G que cumpla con lo deseado: para $g, g' \in G$ definimos $g \sim g'$ si existe $h \in H$ tal que $g = hg'$; o equivalentemente, $g \sim g'$ si $g(g')^{-1} \in H$. Veamos primero que esto define una relación de equivalencia:

- (reflexiva) Para todo $g \in G$, tenemos que $g \sim g$ pues $g = eg$ y $e \in H$ (pues H es subgrupo de G).
- (simétrica) Sean $g, g' \in G$ tales que $g \sim g'$. Entonces $g(g')^{-1} \in H$. Al ser H un subgrupo, es cerrado por inversos y por lo tanto $(g(g')^{-1})^{-1} \in H$. Por lo tanto $g'g^{-1} \in H$ y entonces $g' \sim g$.
- (transitiva) Si $g \sim g'$ y $g' \sim g''$ entonces existen $h, h' \in H$ tales que $g = hg'$ y $g' = h'g''$. Por lo tanto tenemos que $g = hg' = h(h'g'') = (hh')g''$. Al ser H un subgrupo (en particular cerrado con la operación) tenemos que $hh' \in H$ y entonces $g \sim g''$.

Resta ver entonces que una clase de equivalencia tiene tantos elementos como H. Observar que si $g' \in G$ entonces la clase de equivalencia de g' es $C = \{g \in G : g \sim g'\} = \{g \in G : \exists h \in H : g = hg'\}$. Por lo tanto $C = \{hg' : h \in H\}$. Ademas, al multiplicar a todos los elementos de H por g', no hay repeticiones; es decir que si $h_1 \neq h_2$ entonces $h_1g' \neq h_2g'$ (por la propiedad cancelativa). Por lo tanto $\#C = |H|$. 😊

Corolario 3.8.1

Si $(G, *, e)$ es un grupo de orden finito y $g \in g$ tenemos que

1. $o(g) \mid |G|$.
2. $g^{|G|} = e$.
3. Si $|G|$ es primo, entonces G es cíclico.
4. $G = \langle g \rangle$ si y solo si $g^d \neq e$ para todo $d \mid |G|$, $d \neq |G|$.
5. $G = \langle g \rangle$ si y solo si $g^{\frac{|G|}{p}} \neq e$ para todo $p \mid |G|$, p primo, $p \neq |G|$.

Demostración: Consideramos $H = \langle g \rangle$; ya vimos que H es un subgrupo de G y que $|H| = o(g)$. Entonces, por el Teorema de Lagrange tenemos que $o(g) = |H|$ divide a $|G|$ y hemos probado la primer parte.
Ademas, como $|G|$ es un múltiplo de $o(g)$, se deduce que $g^{|G|} = e$.
Para la tercer parte, como $|G| > 2$ entonces existe un $g \in G$ tal que $g \neq e$. Por el Teorema de Lagrange debemos tener que $|\langle g \rangle|$ divide a $|G|$. Como $|\langle g \rangle| > 1$ y $|G|$ es primo tenemos que $|\langle g \rangle| = |G|$ y entonces $\langle g \rangle = G$.
Por ultimo, las partes 4 y 5 son consecuencias de las partes 2 y 3 de la proposición 3.7. 😊

3.9. Homomorfismos

Definición 3.9.1

Sean $(G,*)$ y $(K,*)$ dos grupos. Una función $f : G \to K$ es un homomorfismo o morfismo de grupos si para todo $g, g' \in G,\ f(g * g') = f(g) * f(g')$.

Proposición 3.9.1

Sean $(G,*,e_G)$ y $(K,\star,e_K)$ dos grupos, $f : G \to K$ un homomorfismo y $g \in G$. Entonces:

1. $f(e_G) = e_K$.
2. $f(g^{-1}) = f(g)^{-1}$.
3. $f(g^n) = f(g)^n$ para todo $n \in \mathbb{Z}$.
4. Si $g \in G$ es un elemento de orden finito, entonces $o(f(g))$ también es finito y ademas divide a $o(g)$.

Definición 3.9.2

Sean $(G,*,e_G)$ y $(K,\star,e_K)$ grupos y $f : G \to K$ un homomorfismo. Definimos:

- El núcleo de f, $Ker(f) = \{g \in G : f(g) = e_K\}$.
- La imagen de f, $Im(f) = \{k \in K : \exists g \in G : f(g) = k\} = \{f(g) : g \in G\}$.

Proposición 3.9.2

Sean $(G,*,e_G)$ y $(K,\star,e_K)$ dos grupos y $f : G \to K$ un homomorfismo, entonces:

1. $Ker(f) < G$.
2. $Im(f) < K$.
3. f es inyectiva si y solo si $Ker(f) = \{e_G\}$.
4. f es sobreyectiva si y solo si $Im(f) = K$.

Teorema 3.9.1 Teorema de órdenes

Sean G y K dos grupos y $f : G \to K$ un homomorfismo, entonces

$$|G| = |Ker(f)| \times |Im(f)|$$

Demostración: Para cada $y \in Im(f)$, sea

$$f^{-1}(y) = \{g \in G : f(g) = y\} \subset G$$

es decir, $f^{-1}(y)$ es el conjunto de preimagenes de y. Observar que

$$G = \bigcup_{y \in Im(f)} f^{-1}(y)$$

y la unión es disjunta; esto es porque:

- Claramente la unión de las preimagenes es un subconjunto de G. A su vez, cada $g \in G$, esta en $f^{-1}(f(g))$, así que G esta incluido en la unión de todas las preimagenes.

- Los conjuntos son disjuntos: si $g \in f^{-1}(y) \cap f^{-1}(y') \Rightarrow f(g) = y$ y $f(g) = y'$, al ser f función, esto puede pasar solo si $y = y'$.

Si probamos que para todo $y \in Im(f)$, $\#(f^{-1}(y)) = |Ker(f)|$ entonces tendremos que:

$$|G| = \#\left(\bigcup_{y \in Im(f)} f^{-1}(y)\right) = \sum_{y \in Im(f)} \#\left(f^{-1}(y)\right) = \sum_{y \in Im(f)} |Ker(f)| = |Ker(f)| \times |Im(f)|$$

Probaremos esto ultimo verificando que si $y \in Im(f)$ y fijamos que $g \in f^{-1}(y)$, entonces

$$f^{-1}(y) = \{gx : x \in Ker(f)\}$$

Observemos que $\#\{gx : x \in Ker(f)\} = |Ker(f)|$ puesto que para cada $x \in Ker(f)$ tenemos un elemento gx en este conjunto, y no hay repeticiones pues si $x \neq x'$, por la cancelativa se tiene que $gx \neq gx'$.
Probaremos entonces que si $y \in Im(f)$ y fijamos que $g \in f^{-1}(y) = \{gx : x \in Ker(f)\}$.

- Veamos primero que $\{gx : x \in Ker(f)\} \subset f^{-1}(y)$: si $x \in Ker(f)$ entonces

  $$f(gx) = f(g)f(x) = f(g)e_K = f(g) = y \Rightarrow gx \in f^{-1}(y)$$

  (en la primer igualdad usamos que f es homomorfismo y en la segunda que $x \in Ker(f)$).

- Veamos que ahora que $f^{-1}(y) \subset \{gx : x \in Ker(f)\}$: sea $g' \in f^{-1}(y)$, queremos ver que existe $x \in Ker(f)$ tal que $g' = gx$. Ahora $g' = gx \Leftrightarrow x = g^{-1}g'$, así que basta con ver $g^{-1}g' \in Ker(f)$. Veamos:

  $$f(g^{-1}g') = f(g^{-1})f(g') = f(g)^{-1}f(g') = y^{-1}y = e_K \Rightarrow g^{-1}g' \in Ker(f)$$

  (en la primer igualdad usamos que f es homomorfismo y en la segunda, la propiedad de homomorfismo para el inverso).

😄

Proposición 3.9.3

Sean G un grupo cíclico finito con generador g y K un grupo finito. Sea $k \in K$, la función $f : G \to K$ dada por

$$f(g^n) = k^n,\ n \in \mathbb{Z}$$

esta bien definida y es un homomorfismo si y solo si $o(k)|o(g)$.

Demostración: El directo de la proposición es consecuencia de la parte 4 de la proposición 3.9.
Para el reciproco tenemos que verificar dos cosas, primero que f esta bien definida y luego que es un homomorfismo. Para ver que esta bien definida tenemos que ver que si $g^n = g^m$ entonces $k^n = k^m$. Para eso recordamos que como $g^n = g^m$ entonces $n \equiv m\ (mod\ o(g))$, o sea que $o(g)|n - m$, pero $o(k)|o(g)$ entonces $o(k)|n - m$ y por lo tanto $k^n = k^m$. Solo queda verificar que f es un homomorfismo. 😄

Lenma 3.9.1

Sea G un grupo cíclico finito con generador g. Si K es otro grupo finito, entonces todos los morfismos

$$f : G \to K$$

quedan determinados por $f(g) \in K$ tal que $o(f(g))|o(g)$.

Corolario 3.9.1

Sean G y K grupos finitos:

1. Si $f : G \to K$ es un homomorfismo, entonces $|Im(f)|$ divide a $mcd(|G|, |K|)$.

2. Si $|G|$ y $|K|$ son coprimos, entonces el único homomorfismo $f : G \to K$ es el trivial.

Definición 3.9.3

Dados dos grupos $(G, *, e_G)$ y $(K, \star, e_K)$, una función $f : G \to K$ es un isomorfismo si es un homomorifsmo biyectivo. Decimos que G y K son isomorfos si existe un isomorfismo $f : G \to K$.

Corolario 3.9.2

Tenemos que

1. Un homomorifsmo $f : G \to K$ es un isomorfismo si y solo si $Ker(f) = \{e_G\}$ e $Im(f) = K$.
2. Si $f : G \to K$ es un isomorfismo, entonces la función $f^{-1} : K \to G$ también es un isomorfismo.
3. Si G y K son grupos isomorfos, entonces $|G| = |K|$.
4. Si G y K son grupos isomorfos, entonces G es abeliano si y solo si K es abeliano.
5. Si $f : G \to K$ es un isomorfismo y $g \in G$ entonces $o(g) = o(f(g))$.

Capítulo 4

Raíces Primitivas

4.1. Raíces Primitivas