Notas de Matemática Discreta II

Mariana Pereira, Claudio Qureshi, Gustavo Rama.*
Facultad de Ingeniería
Universidad de la República
Uruguay

*Corregidas por Marcelo Lanzilotta 2016

Índice general

Capítulo 1

Divisibilidad

1.1. Introducción

Escribiremos:

- $\mathbb{Z}$ para el conjunto de números enteros,

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

- $\mathbb{Z}^+$ para el conjunto de enteros positivos,

$$\mathbb{Z}^+ = \{z \in \mathbb{Z} : z > 0\} = \{1,\, 2,\, 3\, \dots\},$$

- $\mathbb{N}$ para el conjunto de números naturales,

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

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 $a = bq + r$.*

Antes de demostrar el teorema, hagamos algunas observaciones y definiciones:

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. Tal como observamos, vamos a suponer $a \geq 0$ 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, al ser $a \geq 0$ tomando $x = 0$, tenemos que $a \in S$ y por lo tanto $\emptyset \neq S \subset \mathbb{N}$. Como todo conjunto de naturales no vacío 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 sólo resta probar que $r < b$. Supongamos

que por el contrario, $r \geq b$; 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 $bq_1 + r_1 = bq_2 + r_2$ y por lo tanto

$$r_2 = b(q_1 - q_2) + r_1 \tag{1.1.1}$$

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 en (1.1.1) tenemos que $r_1 = r_2$.

□

Como aplicación del teorema anterior tenemos la siguiente proposición que nos dice como escribir un número en una base cualquiera.

Proposición 1.1.2. *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 $x \in \mathbb{N}$. Si $x = 0$ es claro porque $x = b^0 \times 0$.

Si $x > 0$, 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

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

con $a_0 = r$ y $a_{i+1} = a_i'$ para $i = 0, 1, \ldots, n$, demostrando así la proposición. □

En el teorema anterior los enteros son únicos y denotamos la descomposición de x en base b como $x = (a_n a_{n-1} \ldots a_1 a_0)_b$.

Ejemplos 1.1.3. 1. *Veamos como escribir $n = 233$ en base 4.*

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

2. *Ahora veamos $n = 8037$ y $b = 7$:*

$$\begin{aligned} 8037 &= 7 \times 1148 + 1 \\ &= 7 \times (7 \times 164 + 0) + 1 \\ &= 7 \times (7 \times (7 \times 23 + 3) + 0) + 1 \\ &= 7 \times (7 \times (7 \times (7 \times 3 + 2) + 3) + 0) + 1 \\ &= 7^4 \times 3 + 7^3 \times 2 + 7^2 \times 3 + 7^1 \times 0 + 7^0 \times 1 \\ &= (32301)_7 \end{aligned}$$

3. *Si queremos hallar la descomposición de n en base 2, podemos utilizar la descomposición en base 4:*

$$\begin{aligned} 233 &= 4^3 \times 3 + 4^2 \times 2 + 4^1 \times 2 + 4^0 \times 1 \\ &= 2^6 \times (2+1) + 2^4 \times 2 + 2^2 \times 2 + 2^0 \times 1 \\ &= 2^7 + 2^6 + 2^5 + 2^3 + 2^0 \\ &= (11101001)_2 \end{aligned}$$

4. *Por otro lado si tenemos la descomposición de un número en base 2, podemos hallar su descomposición en base 2^k de manera fácil. Lo podemos ver con el siguiente ejemplo para 2^2,*

$$\begin{aligned} 447 &= 2^8 + 2^7 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 \\ &= (2^9 \times 0 + 2^8) + (2^7 + 2^6 \times 0) + (2^5 + 2^4) + (2^3 + 2^2) + (2^1 + 2^0) \\ &= 2^8(2 \times 0 + 1) + 2^6(2 + 0) + 2^4(2 + 1) + 2^2(2 + 1) + (2 + 1) \\ &= 4^4 \times 1 + 4^3 \times 2 + 4^2 \times 3 + 4^1 \times 3 + 4^0 \times 3 \\ &= (12333)_4. \end{aligned}$$

Para 2^k en general solo tenemos que agrupar de a k sumandos de la descomposición en base 2.

Por convención, cuando trabajamos con bases que son más grandes que 10 se utilizan las letras del alfabeto para designar los dígitos mayores que 9. Por ejemplo, si la base es $b = 16$ los dígitos posibles son $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, A, B, C, D, E, F y si $x = 3962 = 16^2 \times 15 + 16^1 \times 7 + 16^0 \times 10 = (\text{F7A})_{16}$.

Veamos otra aplicación del teorema de división entera. Supongamos que una asamblea de 16 personas tiene que votar una moción. Los miembros de la asamblea prefieren mantener su voto secreto. Modelemos matemáticamente una manera de que cada persona vote por Si, por No, o Abstención, asegurando que todos los votos sean mantenidos en secreto. Sea A_1 el presidente de la asamblea y los otros 15 miembros $A_2, A_3, \ldots, A_{16}$. El presidente en una hoja en blanco escribe un número grande, digamos 7923, y se lo pasa a A_2. Luego A_2 suma 17 por Si, 1 por No y 0 por Abstención. A_2 escribe la suma en una nueva hoja y se la pasa a A_3. Luego A_3 tiene una hoja con el número 7940 (si A_2 voto Si), 7924 (si A_2 voto No) o 7923 (si A_2 se Abstuvo). Como A_3 no conoce el número original, no puede saber qué voto A_2. El proceso continúa con A_3 sumando 17 por Si, 1 por No o 0 por Abstención y pasándoselo a A_4. Continúan hasta que A_{16} le entrega un número a A_1, que le suma su voto. Digamos que la suma final es 8050. El presidente, que conoce el primer número 7923, se lo substrae a 8050 y obtiene 127. Luego utilizando el Algoritmo de División divide 127 entre 17:

$$127 = 7 \times 17 + 8.$$

El presidente anuncia que 7 personas votaron por Si, 8 personas votaron por No y hubo una Abstención (ya que $7 + 8$ es uno menos que 16, una persona se tuvo que Abstener).

¿Por qué contamos un voto por Si como 17 en este ejemplo? Es uno más que la cantidad de votantes. Si usamos 16 para un voto por Si, no podríamos diferenciar entre 16 votos por No, y un solo Si más 15 Abstenciones ya que tendríamos un total de 16 en ambos casos.

Definición 1.1.4. 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 $m \nmid n$.

Veamos algunas observaciones, ejemplos y propiedades de divisibilidad en los enteros, cuyas demostraciones quedan como ejercicio.

Propiedades 1.1.5.

1. *Tenemos que m divide a n si y sólo si, el resto de dividir n entre m es cero.*
2. $\pm 1 \mid a$, $\forall a \in \mathbb{Z}$. *Además si un entero x cumple que $x \mid a$, $\forall a \in \mathbb{Z}$, entonces $x = \pm 1$.*
3. $b \mid 0$, $\forall b \in \mathbb{Z}$. *Además, 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. *Si $d \mid a$ y $d \mid b$, entonces $d \mid (ax + by)$ para todo $x, y \in \mathbb{Z}$.*
11. *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 $\mathrm{Div}(a)$ al conjunto de divisores de a y $\mathrm{Div}_+(a)$ al conjunto de divisores positivos de a. Es decir $\mathrm{Div}(a) = \{x \in \mathbb{Z} : x \mid a\}$ y $\mathrm{Div}_+(a) = \{x \in \mathbb{Z}^+ : x \mid a\}$.

Por ejemplo, $\mathrm{Div}(3) = \{1, -1, 3, -3\}$, $\mathrm{Div}_+(3) = \{1, 3\}$, $\mathrm{Div}_+(1) = \{1\}$, $\mathrm{Div}(0) = \mathbb{Z}$.

Definición 1.2.2. Decimos que un entero positivo $p \in \mathbb{Z}^+$ es *primo* si

$$\#(\mathrm{Div}_+(p)) = 2.$$

Por ejemplo, 1 no es primo, -3 no es primo, 4 no es primo y 7 es primo.

Observación 1.2.3. *Observar que si $a \neq 0$ y $x \mid a$ entonces como $|x| \leq |a|$, $\mathrm{Div}(a) \subset \{\pm 1, \pm 2, \cdots, \pm a\}$, y por lo tanto $\mathrm{Div}(a)$ 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 $\mathrm{Div}(a) \cap \mathrm{Div}(b)$.*

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 1.2.4. Sean $a, b \in \mathbb{Z}$. Definimos el *máximo común divisor de a y b*, que escribiremos $\mathrm{mcd}(a, b)$ (o simplemente (a, b)), de la siguiente manera:

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

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

- En caso contrario definimos $\mathrm{mcd}(0, 0) = 0$.

Ejemplos 1.2.5. *Tenemos las siguientes propiedades y ejemplos (que quedan como ejercicio)*

1. $\mathrm{mcd}(1, a) = 1$ *para todo $a \in \mathbb{Z}$.*

2. $\mcd(0,b) = |b|$ *para todo* $b \in \mathbb{Z}$.

3. $\mcd(a,b) = \mcd(|a|,|b|)$ *para todo* $a, b \in \mathbb{Z}$.

4. $\mcd(60,77) = \text{máx}(\text{Div}(60) \cap \{\pm 1, \pm 7, \pm 11, \pm 77\}) = \text{máx}\{\pm 1\} = 1$.

5. $\mcd(60,96) =$
   $= \text{máx}(\{\pm 1, \pm 2, \pm 4, \pm 3, \pm 6, \pm 12, \pm 5, \pm 10, \pm 20, \pm 15, \pm 30, \pm 60\} \cap \text{Div}(96))$
   $= \text{máx}\{1, 2, 4, 3, 6, 12\} = 12$

Cuando $\mcd(a,b) = 1$ decimos que a y b son *coprimos* o *primos entre sí*. Como vimos en los ejemplos, 60 y 77 son coprimos.

Ya en el último ejemplo queda evidente, que no es eficiente hallar todos los divisores de a y b para hallar el $\mcd(a,b)$. Necesitamos entonces, algún método mejor para hallar el máximo común divisor, que no sea utilizar la definición.

La siguiente propiedad, si bien es sencilla de probar, es clave para desarrollar dicho método.

Proposición 1.2.6. *Dados* $a, b \in \mathbb{Z}$ *con* $a, b \neq 0$ *entonces:*

1. $\mcd(a,b) = \mcd(b, a - bx)$ *para todo* $x \in \mathbb{Z}$.

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) de los ejemplos anteriores, basta con probarlo para a y b positivos. Llamemos $d = \mcd(a,b)$ y $d' = \mcd(b, a-bx)$. Como $d \mid a$ y $d \mid b$, por lo visto en las propiedades 1.1.5, tenemos que d divide a cualquier combinación lineal entera de a y b, en particular, $d \mid a - bx$. Por lo tanto $d \in \text{Div}(b) \cap \text{Div}(a - bx)$, y entonces $d \leq \text{máx}(\text{Div}(b) \cap \text{Div}(a - bx)) = d'$.

Por otro lado, $d' \mid b$ y $d' \mid a-bx$; utilizando el mismo razonamiento tenemos que d' divide a $(a-bx)+x(b) = a$. Así que $d' \in \text{Div}(a) \cap \text{Div}(b)$ y tenemos que $d' \leq \text{máx}\,\text{Div}(a) \cap \text{Div}(b) = d$. □

Veamos cómo utilizar ésto último, en un ejemplo.

Ejemplo 1.2.7. *Queremos hallar el máximo común divisor de 96 y 60. Si escribimos*

$$96 = 60q + r = 60 \times 1 + 36$$

entonces tenemos que $\mcd(96,60) = \mcd(60,36)$ *y de esta forma hemos disminuido el tamaño de los números. Ahora hacemos lo mismo para 60 y 36:*

$$60 = 36 \times 1 + 24$$

y por lo tanto

$$\mcd(96,60) = \mcd(60,36) = \mcd(36,24).$$

Ahora, seguimos con 36 y 24 , hallamos el resto de dividir 36 entre 24:

$$36 = 24 \times 1 + 12$$

y por lo tanto

$$\mcd(96,60) = \mcd(60,36) = \mcd(36,24) = \mcd(24,12).$$

Si bien ya sabemos calcular este último, hacemos un paso más para ver en qué momento el algoritmo se detiene. Continuamos entonces con 24 y 12:

$$24 = 12 \times 2 + 0$$

y por lo tanto

$$\mathrm{mcd}(96, 60) = \mathrm{mcd}(60, 36) = \mathrm{mcd}(36, 24) = \mathrm{mcd}(24, 12) = \mathrm{mcd}(12, 0).$$

Ahora bien, como para todo entero r se tiene que $\mathrm{mcd}(r, 0) = |r|$, en el último paso no hay nada para calcular. Así que tenemos

$$\mathrm{mcd}(96, 60) = \mathrm{mcd}(60, 36) = \mathrm{mcd}(36, 24) = \mathrm{mcd}(24, 12) = \mathrm{mcd}(12, 0) = 12.$$

Este algoritmo que vimos en el ejemplo, tiene la ventaja de que NO necesita hallar los divisores de a y b para hallar el $\mathrm{mcd}(a, b)$. El algoritmo es conocido como el **Algoritmo de Euclides.** A continuación lo describimos en general.

Dados $a, b \in \mathbb{Z}$ con $a \geq b > 0$. Utilizaremos la siguiente notación: al resto de dividir a entre b lo escribiremos $\mathrm{resto}(a, b)$.

- Fijamos $r_0 = b$.
- Sea $r_1 = \mathrm{resto}(a, b)$; por lo tanto tenemos que $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1)$ y que $0 \leq r_1 < b$.
- Si $r_1 = 0$ entonces $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(b, 0) = b$; y si no, sea $r_2 = \mathrm{resto}(b, r_1)$. Por lo tanto $0 \leq r_2 < r_1 < b$ y $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2)$.
- Si $r_2 = 0$, entonces $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, r_1) = \mathrm{mcd}(r_1, r_2) = \mathrm{mcd}(r_1, 0) = r_1$; y si no, sea $r_3 = \mathrm{resto}(r_1, r_2)$.

Se sigue de esta forma, definiendo en el paso $i + 1$, $r_{i+1} = \mathrm{resto}(r_{i-1}, r_i)$. En particular tenemos que $0 \leq r_{i+1} < r_i$ y que $\mathrm{mcd}(r_{i-1}, r_i) = \mathrm{mcd}(r_i, r_{i+1})$.

Ahora, de esta forma vamos construyendo enteros $r_0, r_1, r_2, \cdots, r_i, r_{i+1}, \cdots$ ... que cumplen que $0 \leq \cdots < r_{i+1} < r_i < \cdots < r_1 < r_0 = b$, y por lo tanto, existe $n \in \mathbb{Z}^+$ tal que $r_n = 0$. Como en cada caso tenemos que el mcd se preserva, obtenemos:

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

Es decir, $\mathrm{mcd}(a, b) = r_{n-1}$.

Un pseudocódigo del Algoritmo de Euclides es el siguiente:

Algoritmo 1 Algoritmo de Euclides

Entrada: Dos números naturales a y b.
Salida: Máximo común divisor g de a y b.

```
si a < b entonces
    aux ← b
    b ← a
    a ← aux
fin si
mientras b ≠ 0 hacer
    r ← resto(a, b)
    a ← b
    b ← r
fin mientras
g ← a
devolver g.
```

A continuación veremos una propiedad fundamental del máximo común divisor, y sus consecuencias. Daremos una demostración, que si bien no es constructiva, es muy sencilla. Más adelante con ejemplos veremos cómo hallar los x, y del teorema.

Teorema 1.2.8 (Igualdad de Bézout)**.** *Sean $a, b \in \mathbb{Z}$, con $a, b \neq 0$, entonces*

1. $\mcd(a, b) = \min\{s > 0 : s = ax + by, \text{ para algún } x, y \in \mathbb{Z}\}$.
2. *En particular, existen $x, y \in \mathbb{Z}$ tal que $\mcd(a, b) = ax + by$.*

Antes de demostrar el teorema vale la pena hacer algunos comentarios y aclaraciones:

- El enunciado del teorema, dice que de todas las combinaciones lineales de a y b con coeficientes enteros, que dan un resultado positivo, el $\mcd(a, b)$ es la menor.
- La segunda parte del teorema es lo que se conoce como **Igualdad de Bézout** y los enteros x, y se llaman **coeficientes de Bézout.**
- Ya vimos que $12 = \mcd(96, 60)$, por lo tanto el teorema nos garantiza que existen $x, y \in \mathbb{Z}$ tales que $12 = 96x + 60y$. Más adelante veremos un algoritmo para hallar los coeficientes de Bézout. En este caso, se puede ver fácilmente que $12 = 96(2) + 60(-3)$. La próxima pregunta que nos podemos hacer es sobre la unicidad de estos coeficientes. Observamos que $96(2 + 60) + 60(-3 - 96) = 96(2) + 96(60) + 60(-3) - 60(96) = 96(2) + 60(-3) = 12$. Y de la misma forma, para cualquier $k \in \mathbb{Z}$ tenemos que $96(2 + 60k) + 60(-3 - 96k) = 12$. O sea, que no sólo no tenemos unicidad en los coeficientes, si no que existen infinitos enteros x, y tales que $12 = 96x + 60y$. También nos podríamos preguntar si hay otros coeficientes, además de $x = 2 + 60k$ e $y = -3 + 96k$. Por ahora dejamos esta pregunta en suspenso, pero volveremos a ella en el siguiente capítulo.

Ahora sí, procedemos a la demostración del teorema.

Demostración. Llamemos $S = \{s > 0 : s = ax + by, \text{ para algún } x, y \in \mathbb{Z}\}$. Por definición, tenemos que $S \subset \mathbb{Z}^+$ y además $\emptyset \neq S$ ya que tomando $x = a$ e $y = b$, tenemos que $s = ax + by = a^2 + b^2 > 0$ así que $a^2 + b^2 \in S$. Entonces por el principio del 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 que $s_0 = ax_0 + by_0$. Llamemos $d = \mathrm{mcd}(a, b)$. Como $d \mid a$ y $d \mid b$, tenemos $d \mid ax_0 + by_0 = s_0$. Por lo tanto $d \leq s_0$.

Probemos ahora que s_0 divide a a y b. Por el teorema de divisón 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 que r debe ser igual a 0. Resulta entonces que $a = qs_0$ y por lo tanto $s_0 \mid a$. De igual modo se muestra que $s_0 \mid b$. Hemos obtenido que s_0 es un divisor común de a y b, luego $s_0 \leq d$. □

Veamos algunas consecuencias importantes de este teorema; sus demostraciones quedan como ejercicio.

Corolario 1.2.9. *Sean $a, b \in \mathbb{Z}$, no nulos.*

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

El siguiente corolario nos resultará muy útil; es conocido como el **Lema de Euclides.**

Lema 1.2.10. *Sean $a, b, c \in \mathbb{Z}$ con $\mathrm{mcd}(a, b) = 1$. Si $a \mid bc$ entonces $a \mid c$.*

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

Como consecuencia obtenemos una propiedad fundamental de los números primos:

Corolario 1.2.11. *Sea p un entero primo y $b, c \in \mathbb{Z}$. Si $p \mid bc$ entonces $p \mid b$ o $p \mid c$.*

Demostración. Si $p \nmid b$, entonces (al ser p primo) tenemos que $\mathrm{mcd}(p, b) = 1$, y por el Lema de Euclides concluimos que $p \mid c$. □

Del corolario anterior se puede obtener una definición alternativa de primo.

Observación 1.2.12. Sea $p \in \mathbb{N}$ que cumple que si $p \mid bc$ entonces $p \mid b$ o $p \mid c$, 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 $p \mid p = bc$, se tiene que $p \mid b$ o $p \mid c$. Además $b \mid p$ y $c \mid p$. Concluimos que $p = b$ o $p = c$, pero $b, c < p$. Por lo tanto p tiene que ser primo. □

La propiedad que surge del último corolario se puede generalizar a varios factores. La demostración la dejamos como ejercicio:

Corolario 1.2.13. *Sea p un entero primo, y $a_1, \ldots, a_n$ enteros, tales que $p \mid a_1 a_2 \cdots a_n$. Entonces $p \mid a_i$ para algún $i \in \{1, \cdots, n\}$.*

También, como consecuencia del Lema de Euclides obtenemos una importante relación entre el máximo común divisor y el mínimo común múltiplo de dos enteros.

Definición 1.2.14. Dados $a, b \in \mathbb{Z}$ no nulos, definimos el *mínimo común múltiplo* de a y b (y lo llamaremos $\mathrm{mcm}(a, b)$) como

$$\mathrm{mcm}(a, b) = \mathrm{mín}\{x \in \mathbb{Z}^+ : a \mid x \text{ y } b \mid x\}.$$

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

Observemos que en el caso en que a y b no son nulos, la definición tiene sentido, ya que el conjunto al cual le tomamos el mínimo no es vacío pues $0 < |ab|$ y $a \mid |ab|$, $b \mid |ab|$.

Al igual que para el máximo común divisor, nos interesa tener un algoritmo para hallar el mínimo común múltiplo de dos enteros sin tener que conocer sus divisores o múltiplos. La siguiente propiedad, nos dice que para hallar el mínimo común múltiplo de dos enteros, basta con hallar su máximo común divisor:

Proposición 1.2.15. *Dados $a, b \in \mathbb{Z}$ no nulos, se cumple que*

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

Demostración. Llamemos $m = \operatorname{mcm}(a,b)$ y sean a^* y b^* los cofactores de a y b. Claramente $\dfrac{|ab|}{\operatorname{mcd}(a,b)} > 0$ y $\dfrac{|ab|}{\operatorname{mcd}(a,b)} = |ab^*| = |a^*b|$ es múltiplo de a y b; así que $m \leq \dfrac{|ab|}{\operatorname{mcd}(a,b)}$.

Por otro lado, como $a \mid m$, existe $k \in \mathbb{Z}$ tal que

$$m = ak = \operatorname{mcd}(a,b)a^*k. \tag{1.2.1}$$

Como $b \mid m$ y $b = \operatorname{mcd}(a,b)b^*$ tenemos que $\operatorname{mcd}(a,b)b^* \mid \operatorname{mcd}(a,b)a^*k$. Como $\operatorname{mcd}(a,b) \neq 0$, por la cancelativa tenemos que entonces $b^* \mid a^*k$. Ahora como $\operatorname{mcd}(a^*,b^*) = 1$, por el Lema de Euclides (lema 1.2.10), tenemos que $b^* \mid k$. Por lo tanto, existe $k' \in \mathbb{Z}$ tal que $k = b^*k'$ y sustituyendo en (1.2.1) obtenemos que $m = ab^*k'$ y por lo tanto $\dfrac{|ab|}{\operatorname{mcd}(a,b)} = |ab^*| \leq m$. □

Observar que entonces tenemos que $\operatorname{mcm}(a,b) = \dfrac{|ab|}{\operatorname{mcd}(a,b)} = |a^*b^* \operatorname{mcd}(a,b)|$.

Ejemplo 1.2.16. *Ya habíamos visto que* $\operatorname{mcd}(96,60) = 12$*; así que* $\operatorname{mcm}(96,60) = \dfrac{96 \times 60}{12} = 96 \times 5 = 480$.

Antes de finalizar con esta sección, hacemos un par de comentarios:

- De forma análoga a lo hecho para dos enteros, se puede definir el máximo común divisor de cualquier cantidad de enteros: dados $a_1, a_2, \cdots, a_n \in \mathbb{Z}$, con $n > 2$, no todos nulos, definimos

$$\operatorname{mcd}(a_1, \cdots, a_n) = \text{máx}\{x \in \mathbb{Z} : x \mid a_i, \forall\, i = 1, \cdots, n\}$$

  .

- Es fácil probar que $\operatorname{mcd}(a_1, a_2, \cdots, a_n) = \operatorname{mcd}(\operatorname{mcd}(a_1, a_2, \cdots, a_{n-1}), a_n)$ (ejercicio).

- En consecuencia, es posible probar por inducción una igualdad de Bézout generalizada (ejercicio): existen enteros $x_1, x_2, \cdots, x_n$ tales que

$$a_1x_1 + a_2x_2 + \cdots a_nx_n = \operatorname{mcd}(a_1, a_2, \cdots, a_n).$$

Veamos un ejemplo de esto último.

Ejemplo 1.2.17. *Sean* $a = 140$, $b = 60$ *y* $c = 55$. *Por lo visto antes* $\operatorname{mcd}(a,b,c) = \operatorname{mcd}(140,60,55) = \operatorname{mcd}(\operatorname{mcd}(140,60),55) = \operatorname{mcd}(20,55) = 5$. *Utilizando las igualdades de Bezout para* $20 = \operatorname{mcd}(140,60)$ *y para* $5 = \operatorname{mcd}(20,50)$,

$$\begin{aligned} 20 &= 140 \times 1 + 60 \times (-2) \\ 5 &= 20 \times 3 + 55 \times (-1) \\ &= (140 \times 1 + 60 \times (-2)) \times 3 + 55 \times (-1) \\ &= 140 \times 3 + 60 \times (-6) + 55 \times (-1) \end{aligned}$$

1.3. Pruebas de Irracionalidad

Como consecuencia del Lema de Euclides podemos probar que $\sqrt{2}$ no es racional; a continuación vemos una demostración que utiliza las herramientas recién vistas.

Proposición 1.3.1. *$\sqrt{2}$ no es racional.*

Demostración. Supongamos por absurdo, que $\sqrt{2}$ es racional; es decir, que existen $a, b \in \mathbb{Z}$ tales que $\sqrt{2} = \frac{a}{b}$. Cancelando el $\mathrm{mcd}(a, b)$ si es necesario, podemos escribir entonces $\sqrt{2} = \frac{m}{n}$ con $m, n \in \mathbb{Z}^+$ y $\mathrm{mcd}(m, n) = 1$.

Ahora, $2 = \frac{m^2}{n^2}$ y por lo tanto $2n^2 = m^2$. En consecuencia $2 \mid m^2$ y por el corolario del Lema de Euclides tenemos que $2 \mid m$. Sea $m' \in \mathbb{Z}$ tal que $m = 2m'$.

Ahora volviendo a la igualdad $2n^2 = m^2$, tenemos que $2n^2 = (2m')^2 = 4(m')^2$ así que $n^2 = 2(m')^2$. Por lo tanto $2 \mid n^2$ y nuevamente por el corolario del Lema de Euclides, tenemos que $2 \mid n$.

Por lo tanto 2 es un divisor común de m y n lo que contradice que $\mathrm{mcd}(m, n) = 1$.

□

Claramente, no hay nada de especial en el 2 en la prueba anterior. Sólo utilizamos que 2 es primo. Tenemos entonces la siguiente generalización:

Proposición 1.3.2. *Si p es primo entonces $\sqrt{p}$ no es racional.*

1.4. Algoritmo de Euclides Extendido

Veamos ahora un método para hallar coeficientes de Bézout; es decir $x, y \in \mathbb{Z}$ tales que $\mathrm{mcd}(a, b) = ax + by$. Veámoslo con un ejemplo.

Ejemplo 1.4.1. *Apliquemos el Algoritmo de Euclides para hallar $\mathrm{mcd}(132, 28)$:*

$$132 = 4 \times 28 + 20 \tag{1.4.1}$$

$$28 = 1 \times 20 + 8 \tag{1.4.2}$$

$$20 = 2 \times 8 + 4 \tag{1.4.3}$$

$$8 = 2 \times 4 + 0$$

Por lo tanto, $\mathrm{mcd}(132, 28) = 4$. Ahora, de la ecuación (1.4.3) tenemos que

$$4 = 20 - 2 \times 8. \tag{1.4.4}$$

Despejando 8 de la ecuación (1.4.2) y sustituyendo en (1.4.4) obtenemos:

$$4 = 20 - 2 \times 8 = 20 - 2(28 - 1 \times 20) = 20(3) + 28(-2). \tag{1.4.5}$$

donde en el último paso sacamos factores comunes 20 y 28. Ahora, despejando 20 de la ecuación (1.4.1) y sustituyendo en (1.4.5) obtenemos:

$$4 = 20(3) + 28(-2) = (132 - 4 \times 28)(3) + 28(-2) = 132(3) + 28(-14),$$

donde nuevamente, en el último paso sacamos factores comunes 132 y 28.

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

Este método de despejar los restos obtenidos en un paso del Algoritmo de Euclides y sustituirlos en las ecuaciones, se llama **Algoritmo de Euclides Extendido.** Daremos otra forma de hacer lo mismo pero que puede resultar más ordenado (y programable).

Escribimos los datos de cada paso del Algoritmo de Euclides en forma de vector.

- El dato inicial del algortimo es el vector $B_0 = \binom{132}{28}$.
- En el primer paso, a partir de $132 = 4 \times 28 + 20$, cambiamos los datos del algoritmo a $B_1 = \binom{28}{20}$. 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 $B_2 = \binom{20}{8}$. Observar que:

$$B_2 = \begin{pmatrix} 20 \\ 8 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 28 \\ 20 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} \begin{pmatrix} 132 \\ 28 \end{pmatrix}.$$

- En el segundo paso, a partir de $20 = 2 \times 8 + 4$, cambiamos los datos del algoritmo a $B_3 = \binom{8}{4}$. Observar 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, realizando el producto

$$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & -4 \end{pmatrix} = \begin{pmatrix} -1 & 5 \\ 3 & -14 \end{pmatrix}$$

obtenemos que

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

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

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

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 tenemos los nuevos datos

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

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 en 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

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

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

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

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

$$B_{n-1} = \begin{pmatrix} r_{n-2} \\ \mathrm{mcd}(a,b) \end{pmatrix} = M B_0 = M \begin{pmatrix} a \\ b \end{pmatrix}; \tag{1.4.6}$$

por lo tanto, si $M = \begin{pmatrix} z & w \\ x & y \end{pmatrix}$, la última fila de la ecuación (1.4.6) nos dice que $\mathrm{mcd}(a,b) = xa + yb$; es decir, la segunda fila de M son coeficientes de Bézout para a y b.

Una buena forma de ir guardando todos los datos del algoritmo, es armando una tabla con columnas: B_i, M_i y el producto $M_i \cdots M_1$. Haremos un último ejemplo usando esta tabla.

Ejemplo 1.4.2. *Calculemos* $\mathrm{mcd}(456, 123)$*:*

1. *Comenzamos armando la tabla:*

i	B_i	M_i	$M_i \cdots M_1$
0	$\begin{pmatrix} 456 \\ 123 \end{pmatrix}$		
1	$\vdots$	$\vdots$	$\vdots$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

2. *Luego, de* $456 = 3(123) + 87$ *completamos la fila para* $i = 1$ *de la tabla:*

i	B_i	M_i	$M_i \cdots M_1$
0	$\begin{pmatrix} 456 \\ 123 \end{pmatrix}$		
1	$\begin{pmatrix} 123 \\ 87 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

3. *Luego con* $123 = 1(87) + 36$, *completamos la fila para* $i = 2$ *con* B_2, M_2 *y* M_2M_1*:*

i	B_i	M_i	$M_i \cdots M_1$
0	$\begin{pmatrix} 456 \\ 123 \end{pmatrix}$		
1	$\begin{pmatrix} 123 \\ 87 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}$
2	$\begin{pmatrix} 87 \\ 36 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$
$\vdots$	$\vdots$	$\vdots$	$\vdots$

4. *Y seguimos completando la tabla:*

i	B_i	M_i	$M_i \cdots M_1$
0	$\begin{pmatrix} 456 \\ 123 \end{pmatrix}$		
1	$\begin{pmatrix} 123 \\ 87 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -3 \end{pmatrix}$
2	$\begin{pmatrix} 87 \\ 36 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -1 \end{pmatrix}$	$\begin{pmatrix} 1 & -3 \\ -1 & 4 \end{pmatrix}$
3	$\begin{pmatrix} 36 \\ 15 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$	$\begin{pmatrix} -1 & 4 \\ 3 & -11 \end{pmatrix}$
4	$\begin{pmatrix} 15 \\ 6 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$	$\begin{pmatrix} 3 & -11 \\ -7 & 26 \end{pmatrix}$
5	$\begin{pmatrix} 6 \\ 3 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$	$\begin{pmatrix} -7 & 26 \\ 17 & -63 \end{pmatrix}$
6	$\begin{pmatrix} 3 \\ 0 \end{pmatrix}$	$\begin{pmatrix} 0 & 1 \\ 1 & -2 \end{pmatrix}$	$\begin{pmatrix} 17 & -63 \\ * & * \end{pmatrix}$

Por lo tanto, obtenemos que $\mathrm{mcd}(456, 123) = 3$ *y que* $3 = 456(17) + 123(-63)$.

Cualquiera de los métodos aquí explicados es conocido como el **Algoritmo de Euclides Extendido**. Damos un pseudocódigo del mismo a continuación, denotando $\mathrm{cociente}(a, b)$ como el cociente de dividir a entre b.

Algoritmo 2 Algoritmo de Euclides extendido

Entrada: Dos naturales $a \leq b$.
Salida: Máximo común divisor g de a y b y x, y tales que $ax + by = g$.

$M \leftarrow \left(\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right)$.
mientras $b \neq 0$ **hacer**
  $q \leftarrow \text{cociente}(a, b)$
  $r \leftarrow \text{resto}(a, b)$
  $M \leftarrow \left(\begin{smallmatrix} 0 & 1 \\ 1 & -q \end{smallmatrix}\right) \times M$.
  $a \leftarrow b$
  $b \leftarrow r$
fin mientras
$g \leftarrow a$
$x \leftarrow M_{11}$
$y \leftarrow M_{12}$
devolver g, x, y.

1.5. Ecuaciones diofánticas lineales

En esta sección utilizaremos los métodos antes descriptos para resolver un tipo de problemas modelados por ecuaciones diofánticas lineales. Comencemos con un ejemplo para ilustrar los resultados que queremos probar.

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 cuántas formas podemos hacerlo?*

Si llamamos x a la cantidad de ladrillos que compramos, e y a la cantidad de baldozas, tenemos que $x, y \in \mathbb{N}$ y la condición de gastar los 333 pesos se traduce a

$$12x + 21y = 333. \tag{1.5.1}$$

Algunas observaciones:

- *La primera es que como tanto 12 y 21 son múltiplos de 3, el dinero que gastemos tendrá qe ser múltiplo de 3. Es decir, si en vez de 333 pesos quisiéramos gastar exactamente 100 pesos, no podríamos hacerlo.*
- *La segunda observación es que, como $3 = \text{mcd}(12, 21)$, por la igualdad de Bézout (por ejemplo con el Algoritmo de Euclides Extendido) podemos hallar $x', y' \in \mathbb{Z}$ tales que*

$$12x' + 21y' = 3.$$

- *Por ejemplo $x' = 2$ e $y' = -1$ cumplen la última ecuación:*

$$12(2) + 21(-1) = 3.$$

- *Si multiplicamos la última igualdad por 111, obtenemos que*

$$12(222) + 21(-111) = 333;$$

es decir, que $x = 222$ e $y = -111$ verifican la ecuación (1.5.1); pero estos valores de x e y no nos resuelven el problema original ya que buscábamos $x, y \geq 0$. Nos interesa entonces hallar TODOS los pares de enteros (x, y) que son solución de (1.5.1) para luego entre ellos, buscar los que no sean negativos.

- *Observar que*
$$12(222-21k)+21(-111+12k)=333$$
para todo $k\in\mathbb{Z}$; por lo tanto, para todo $k\in\mathbb{Z}$, el par $(x=222-21k,\ y=-111+12k)$ verifica la ecuación (1.5.1).

- *Lo fundamental en la última observación es que $12(-21k)=-21(12k)$. Pero también $12(-7k)=-21(4k)$; y por lo tanto,*
$$12(222-7k)+21(-111+4k)=333.$$
Así que para cada $k\in\mathbb{Z}$, el par $(x=222-7k,\ y=-111+4k)$ verifica la ecuación (1.5.1). *De esta forma obtuvimos nuevas soluciones que no teníamos en la observación anterior.*

Lo que probaremos en este capítulo, es que estas últimas son TODAS las soluciones enteras de la ecuación (1.5.1).

Asumamos ésto por el momento. Es decir, que el conjunto de soluciones enteras a
$$12x+21y=333$$
es $\{(x,y)=(222-7k,\ -111+4k):\ k\in\mathbb{Z}\}$.

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 $(x=26,y=1)$, $(x=19,y=5)$ $(x=12,y=9)$, $(x=5,y=13)$. Es decir se pueden comprar 26 ladrillos y una baldoza, o 19 ladrillos y 5 baldozas, o 12 ladrillos y 9 baldozas, o 5 ladrillos y 13 baldozas.

Ahora sí, enunciaremos el teorema que resume las propiedades vistas en el ejemplo anterior; definiendo antes la noción de ecuación diofántica.

Definición 1.5.2. 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* de la ecuación 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 1.5.3. *Sean a,b y c enteros con $(a,b)\neq(0,0)$. Entonces la ecuación diofántica*
$$ax+by=c$$

1. *Tiene solución si y sólo si $\mathrm{mcd}(a,b)|c$.*
2. *Además, si tiene una solución, tiene infinitas. Es más, si (x_0,y_0) es una solución, entonces el conjunto de soluciones es*
$$S=\left\{\left(x_0+\frac{b}{\mathrm{mcd}(a,b)}k,\ y_0-\frac{a}{\mathrm{mcd}(a,b)}k\right):\ k\in\mathbb{Z}\right\}=\{(x_0+b^*k,\ y_0-a^*k):\ k\in\mathbb{Z}\}.$$

Demostración. Por simplicidad, llamemos $d=\mathrm{mcd}(a,b)$. 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 $d \mid a$ y $d \mid b$, entonces $d \mid ax_0 + by_0 = c$.

   Supongamos ahora que $d \mid c$ y veamos que la ecuación tiene solución: como $d \mid c$, existe $e \in \mathbb{Z}$ tal que $c = de$. Por la igualdad de Bézout (Teorema 1.2.8), existen $x', y' \in \mathbb{Z}$ tales que $ax' + by' = d$. Multiplicando por e obtenemos 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

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

   es solución de la ecuación. Para esto simplemente sustituímos:

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

   donde la última 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 $b^* = b/d \neq 0$).

   Sea entonces (x_1, y_1) una solución, tenemos pues que

$$\begin{aligned} ax_1 + by_1 &= c \text{ y} \\ ax_0 + by_0 &= c. \end{aligned}$$

   Por lo tanto $ax_1 + by_1 = ax_0 + by_0$ y entonces $a(x_1 - x_0) = b(y_0 - y_1)$. Al ser $d \neq 0$, podemos dividir entre d y obtenemos

$$a^*(x_1 - x_0) = b^*(y_0 - y_1). \tag{1.5.2}$$

   Tenemos en particular que $b^* \mid a^*(x_1 - x_0)$ y como $\mathrm{mcd}(a^*, b^*) = 1$, por el Lema de Euclides tenemos que $b^* \mid (x_1 - x_0)$. 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 (1.5.2) 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 $y_1 = y_0 - a^*k$.

□

1.6. El Problema de los Sellos

Si vamos a la oficina del correo a enviar una carta y vemos que solo hay sellos de valores de 3 y 5 pesos, ¿qué valores de envío son posibles?, ¿qué valores no son posibles con esos dos sellos? Estas preguntas son parte de un problema más general llamado **El Problema de los Sellos:** Si a y b son enteros positivos, ¿qué enteros positivos pueden ser expresados como $ax + by$ con x, y no negativos?

Para comenzar, notamos que basta considerar solo los casos donde a y b son primos entre si. Por ejemplo, si son ambos pares, entonces no podemos obtener números impares como combinación lineal de ellos y el problema es menos interesante.

A los números que se pueden expresar como $ax + by$ con x, y no negativos los llamamos números *factibles*. Por ejemplo, a, b, y ab son siempre factibles ya que

$$a = 1 \times a + 0 \times b,\ b = 0 \times a + 1 \times b,\ \text{y}\ ab = b \times a + 0 \times b = 0 \times a + a \times b.$$

Es claro también que los múltiplos de a o b también son factibles.

Vamos a probar que $ab - a - b$ no es factible y que además es el último que no lo es. La primer parte de esto queda como ejercicio en el repartido de práctico.

Proposición 1.6.1. *Sean $a > 1$, $b > 1$ enteros, primos entre sí. 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 $\mathrm{mcd}(a, b) = 1$. Si $n \geq ab - a - b + 1$, entonces existen enteros no negativos x, y tales que*

$$ax + by = n.$$

Demostración. Por el Teorema 1.5.3, como $\mathrm{mcd}(a, b) = 1$, 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

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

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 $y_1 \leq a - 1$,

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

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

Volviendo al ejemplo de los sellos: si tenemos tres o más sellos, no se conocen fórmulas como en el caso de dos sellos. Se pueden utilizar técnicas de *backtracking* para decidir si un número es factible o no en el caso general.

1.7. Teorema Fundamental de la Aritmética

En esta sección veremos el Teorema Fundamental de la Aritmética y sus principales consecuencias, el cual dice que todo entero $n > 1$ es producto de primos y que a menos del orden, la forma de escribirlo como producto de primos es única. Existen varias demostraciones de este teorema, pero en general las diferencias son mínimas y la mayoría se basa en las ideas originales de Euclides (300 A.C).

Teorema 1.7.1 (Teorema Fundamental de la Aritmética)**.** *Sea $n \in \mathbb{N}$, $n > 1$; entonces:*

1. *Existen primos $p_1, \cdots, p_k$ (no necesariamente distintos) con $k \geq 1$, tales que $n = p_1 \cdots p_k$.*

2. *Hay unicidad en la factorización. Es decir, k (la cantidad de factores primos) es único y la lista de primos (contando repeticiones), $p_1, \cdots, p_k$ 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 probémoslo 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 $p_1, \cdots, p_k$ y $p'_1 \cdots p'_r$ tales que $a = p_1 \cdots p_k$ y $b = p'_1 \cdots p'_r$. Al ser $n = ab$ tenemos que $n = p_1 \cdots p_k p'_1 \cdots p'_r$ 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 $p_1, \cdots, p_k$, $q_1, \cdots, q_r$ tales $n_0 = p_1 \cdots p_k$, $n_0 = q_1 \cdots q_r$ con $\{p_1, \cdots, p_k\} \neq \{q_1, \cdots, q_r\}$ (y como claramente n_0 no puede ser primo, tenemos que $k, r \geq 2$.)

   Tenemos entonces que $p_1 \cdots p_k = q_1 \cdots q_r$ y por lo tanto $p_1 \mid q_1 \cdots q_r$. Al ser p_1 primo, por el corolario 1.2.13 existe $j \in \{1, \cdots, r\}$ tal que $p_1 \mid q_j$; 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 $p_1 \cdots p_k = p_1 q_2 \cdots q_r$ y cancelando p_1 obtenemos $p_2 \cdots p_k = q_2 \cdots q_r$. Pero al ser $\{p_2, \cdots, p_k\} \neq \{q_2, \cdots, q_r\}$, tenemos que $m = p_2 \cdots p_k = q_2 \cdots q_r$ es un entero > 1 que se escribe de dos formas distintas como producto de primos, y esto es absurdo ya que $m = n_0/p_1 < n_0$ y n_0 era el menor entero mayor que uno que se podía escribir de dos formas distintas como producto de primos. □

Antes de comentar sobre los algoritmos de factorización, veamos una importante consecuencia del último teorema debido a Euclides.

Corolario 1.7.2. *Existen infinitos primos.*

Demostración. Supongamos por absurdo que existe una cantidad finita de primos y sea $\{p_1, \cdots, p_k\}$ el conjunto de todos los primos. Consideremos el entero $n = p_1 p_2 \cdots p_k + 1$. 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 $\{p_1, \cdots, p_k\}$ tenemos que $p_i \mid n$ para algún $i \in \{1, \cdots, k\}$. Tenemos entonces que $p_i \mid p_1 p_2 \cdots p_k + 1$, pero como $p_i \mid p_1 p_2 \cdots p_k$, tenemos que $p_i \mid 1$ lo cual es absurdo al ser $p_i > 1$. □

Observación 1.7.3. *Hacemos algunos comentarios sobre el último resultado:*

- *Si bien existen infinitos primos, no existen fórmulas para hallar infinitos primos (y mucho menos, todos los primos). Existen métodos muy antiguos para hallar todos los primos menores que un entero dado n. Por ejemplo, la* Criba de Eratóstenes, *del 200 A.C. Dejamos a cargo del lector buscar la información sobre este método.*

- *Es un tema de investigación permanente hallar un primo mayor al último que se conoce. Los* números de Mersenne, *son los números $M_n = 2^n - 1$, con $n \in \mathbb{N}$. Es fácil probar que si n es compuesto, entonces M_n es también lo es. Si n es primo, M_n puede ser primo o compuesto. Existen tests de primalidad (como*

el Test de Lucas) para verificar si un número es primo que son eficientes (realizables en tiempo real) para los números de Mersenne. Hay un programa de búsqueda de primos de Mersenne, llamado GIMPS (Great Internet Mersenne Prime Search) que funciona utilizando una pequeña porción de la memoria de las computadoras que tienen instalado el programa y están conectadas a internet, y que aplica el test de primalidad al próximo número de Mersenne que no se sabe si es primo o compuesto. De esta forma, en 2008 se probó que para $n = 30402457$, M_n es primo (con casi 13 millones de cifras). En enero de 2013 con el mismo programa se probó que para $n = 5788516$, M_n también es primo (con más de 17 millones de cifras) y es hasta el momento el mayor primo conocido (y el 48avo primo de Mesenne). La página para bajar el programa GIMPS y con toda la información de la búsqueda es: http://www.mersenne.org.

Observación 1.7.4. *Si en la descomposición de un entero positivo a, tomamos primos distintos, entonces éstos pueden aparecer con exponentes. Por lo tanto, todo entero $a > 1$ se escribe (de forma única, a menos del orden) como $a = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, con p_i primos distintos y $e_i \in \mathbb{Z}^+$.*

Por ejemplo, $280 = 2^3 \cdot 5 \cdot 7 = 2^3 \cdot 5^1 \cdot 7^1$; así que los primos involucrados en la descomposición factorial son 2, 5 y 7, con exponentes 3, 1 y 1 respectivamente.

Puede resultar conveniente escribir $a = 2^{a_1} 3^{a_3} 5^{a_5} \cdots$ con la convención de que $a_i \geq 0$ y sólo una cantidad finita de ellos no nulos (únicamente los exponentes de los primos que efectivamente dividen a n son no nulos).

Por ejemplo, con esta notación, en el caso 280, $a_2 = 3$, $a_3 = 0$, $a_5 = a_7 = 1$ y el resto todos cero.

Proposición 1.7.5. *Sean a, b enteros positivos con descomposición en factores primos*

$$a = 2^{a_2} 3^{a_3} 5^{a_5} \cdots \quad y \quad b = 2^{b_2} 3^{b_3} 5^{b_5} \cdots,$$

entonces:

1. *$a \mid b$ si y sólo si $a_p \leq b_p$ para todo p.*
2. *$\mathrm{mcd}(a, b) = 2^{d_2} 3^{d_3} 5^{d_5} \cdots$ siendo $d_p = \mín\{a_p, b_p\}$ para todo primo p.*
3. *$\mathrm{mcm}(a, b) = 2^{m_2} 3^{m_3} 5^{m_5} \cdots$ siendo $m_p = \máx\{a_p, b_p\}$ para todo primo p.*

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

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

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

Recíprocamente, si $a_p \leq b_p$, entonces tomando $c = 2^{b_2 - a_2} 3^{b_3 - a_3} 5^{b_5 - a_5} \cdots$ tenemos que $c \in \mathbb{Z}^+$ y $ac = b$. Por lo tanto $a \mid b$.

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

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

y

$$\mathrm{Div}_+(b) = \{c = 2^{c_2} 3^{c_3} 5^{c_5} \cdots \text{ con } 0 \leq c_p \leq b_p, \forall p\}.$$

Por lo tanto, los divisores comunes (positivos) de a y b son

$$\begin{aligned} \mathrm{Div}_+(a) \cap \mathrm{Div}_+(b) &= \{c = 2^{c_2} 3^{c_3} 5^{c_5} \cdots \text{ con } 0 \leq c_p \leq a_p, \text{ y } c_p \leq b_p, \forall p\} = \\ &= \{c = 2^{c_2} 3^{c_3} 5^{c_5} \cdots \text{ con } 0 \leq c_p \leq \mín\{a_p, b_p\}, \forall p\}. \end{aligned}$$

El máximo de este conjunto es claramente $c = 2^{d_2} 3^{d_3} 5^{d_5} \cdots$ siendo $d_p = \mín\{a_p, b_p\}$ 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 $\mathrm{mcm}(a,b) = \dfrac{ab}{\mathrm{mcd}(a,b)}$.

□

Tenemos entonces los siguietes corolarios:

Corolario 1.7.6. *Sea $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, con p_i primos distintos y $e_i \in \mathbb{Z}^+$. Entonces:*

1. $\mathrm{Div}_+(n) = \{p_1^{c_1}\, p_2^{c_2} \cdots p_k^{c_k} : c_i \in \mathbb{N} \text{ y } c_i \leq e_i, \forall\, i = 1, \cdots, k\}$.
2. *La cantidad de divisores positivos de n es*

$$\#\,\mathrm{Div}_+(n) = (e_1+1)(e_2+1)\cdots(e_k+1).$$

3. *El entero n es un cuadrado perfecto (es decir, existe $m \in \mathbb{Z}$ tal que $n = m^2$) si y sólo si $2 \mid e_i\ \forall i = 1, \cdots, k$.*
4. *Existe $m \in \mathbb{Z}^+$ y $k \in \mathbb{Z}^+$ tales que $n = m^k$ si y sólo si, todos los e_i son múltiplos de k.*

Demostración. 1. Se deduce claramente de la primer parte de la proposición anterior.

2. Por lo visto en la parte anterior,
$\#Div_+(n) = \#\{p_1^{c_1}\, p_2^{c_2} \cdots p_k^{c_k} : c_i \in \mathbb{N} \text{ y } c_i \leq e_i, \forall\, i = 1, \cdots, k\} =$
$= \#\{(c_1, c_2, \cdots, c_k) : c_i \in \mathbb{N} \text{ y } c_i \leq e_i, \forall\, i = 1, \cdots, k\} =$
$= \#\{\{0, 1, \cdots, e_1\} \times \{0, 1, \cdots, e_2\} \times \cdots \times \{0, 1, \cdots, e_k\}\} = (e_1+1)(e_2+1)\cdots(e_k+1).$

3. Si e_i es par para todo i, tomando $c_i = e_i/2$ y $m = p_1^{c_1}\, p_2^{c_2} \cdots p_k^{c_k}$, claramente $m \in \mathbb{Z}$ y $m^2 = n$.
Recíprocamente, si existe un entero (positivo) m tal que $m^2 = n$, como en particular $m \mid n$, por la primer parte, existen $c_1, \cdots, c_k \in \mathbb{N}$ (con $c_i \leq e_i$) tales que $m = p_1^{c_1}\, p_2^{c_2} \cdots p_k^{c_k}$ (observar que la primer parte nos dice en particular, que en la descomposición factorial de m, los únicos primos que pueden aparecer son los de n). Ahora
$$p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k} = n = m^2 = p_1^{2c_1}\, p_2^{2c_2} \cdots p_k^{2c_k}$$
y por la unicidad de la descomposición, debe ser $e_i = 2c_i$ para todo $i = 1, \cdots, k$.

4. Es análogo a la parte anterior.

□

Dejamos planteados los siguientes ejercicios:

1. Investigar qué enteros positivos poseen exactamente 3 divisores positivos.
2. Investigar qué enteros positivos poseen una cantidad impar de divisores positivos.
3. Probar que para todo entero positivo n, existen únicos enteros positivos r, s, con s libre de cuadrados (esto quiere decir, que $z^2 \nmid s$ para todo entero $z > 1$) y tales que $n = r^2 s$.

1.8. Comentarios sobre los algoritmos de factorización.

Ya sabemos que todo entero se puede escribir de forma única como producto de primos, pero ¿cómo hallamos estos factores primos? Veamos algunas ideas sencillas (pero no muy eficientes) con ejemplos:

Ejemplo 1.8.1. *Si queremos hallar la descomposición factorial de* 588*:.*

1. *Utilizando el algoritmo de divisón entera, nos fijamos si* $2 \mid 588$*. Efectivamente* $588 = 2 \times 294$*. Así que* 2 *es un factor primo de* 588*.*
2. *Ahora comenzamos de nuevo con el cociente* 294 *y nos fijamos si* $2 \mid 294$*. Efectivamente* $294 = 2 \times 147$*. Así que* 2 *es un factor primo de* 294 *y por lo tanto* 2^2 *es factor de* 588*.*
3. *Ahora volvemos a empezar con* 147*. Vemos que* $2 \nmid 147$*, y entonces nos fijamos si* $3 \mid 147$*. Efectivamente,* $147 = 3 \times 49$ *y por lo tanto* 3 *es un factor primo de* 147 *y tenemos que* $588 = 2^2 \times 3 \times 49$*.*
4. *Ahora deberíamos comenzar de nuevo con* 49*. Pero como ya vimos que* $2 \nmid 147$ *ya sabemos que* $2 \nmid 49$*. Así que comenzamos probando si* $3 \mid 49$*. Claramente* $3 \nmid 49$ *y luego pasamos a probar si* $4 \mid 49$*,* $5 \mid 49$*,* $6 \mid 49$ *hasta llegar hasta que* $49 = 7^2$ *y así obtenemos que*

$$588 = 2^2 \times 3 \times 7^2.$$

Observar que en el último paso, como ya sabíamos que $2 \nmid 49$, también sabemos que cualquier múltiplo de 2 no divide a 49. Y de la misma forma, al saber que $3 \nmid 49$, no es necesario probar si los múltiplos de 3 dividen a 49. Es decir, en realidad basta probar con divisores primos; pero para ésto se necesita tener una lista de primos (menores que 49), o al menos efectuar multiplicaciones para eliminar todos los múltiplos de 2 y de 3 de la lista de divisores a probar (este método de eliminar todos los múltiplos de 2 y luego los múltiplos de 3, etc, es en el fondo lo que se hace para obtener la Criba de Eratóstenes).

Veamos otro ejemplo con las simplificaciones recién mencionadas.

Ejemplo 1.8.2. *Hallemos la descomposición factorial de* $n = 836077$*.*

1. *Tenemos que* $2 \nmid n$*,* $3 \nmid n$*,* $5 \nmid n$*,* $7 \nmid n$*, y* $836077 = 11 \times 76007$*.*
2. *Tenemos que* $11 \nmid 76007$*,* $13 \nmid 76007$ *y* $76007 = 17 \times 4471$*.*
3. *Ahora* $4471 = 17 \times 263$*.*
4. *Ahora buscamos divisores de 263:* $17 \nmid 263$*; pero además* $263 = 17 \times 15 + 8$ *y por lo tanto* $17 \times 16 > 263$ *y en particular* $17^2 > 263$ *(es decir* $17 > \sqrt{263}$*).*
5. *Por lo observado anteriormente* $263 \neq ab$ *con* a *o* b *mayores que* 17 *(pues si* $a > 17$*,* $b < 263/17 < 17$ *y ya sabemos que 263 no tiene factores menores que 17). Concluimos entonces que* 263 *es primo y luego* $836077 = 11 \times 17^2 \times 263$ *es la descomposición factorial de* 836077*.*

Como observamos anteriormente, para buscar divisores (mayores que 1) de un entero n, basta con buscar divisores $a \leq \sqrt{n}$. Por lo tanto se necesitan a lo sumo (la parte entera de) $\sqrt{n}$ divisiones para encontrar un factor de n. En el caso en que n sea primo, necesitaríamos exactamente (la parte entera de) $\sqrt{n}$ para comprobar con este método que n es primo. Por ejemplo, para chequear que 7919 es primo necesitaríamos efectuar 88 divisiones (si bien esto sería probando todos los posibles divisores, y no únicamente los divisores primos, asumamos que el descartar divisores compuestos lleva el mismo trabajo que no sacarlos de la lista de divisores posibles).

Ejemplo 1.8.3. *En el libro de Coutinho [2] se muestra con un ejemplo lo poco eficiente que puede ser este método: supongamos que estamos buscando los divisores de un entero n que tiene 101 cifras. Por lo tanto $n > 10^{100}$. En el peor de los casos (que n sea primo) debemos realizar $\sqrt{n}$ divisiones; por lo tanto debemos realizar más de 10^{50} divisiones. Supongamos que nuestra computadora puede realizar 10 mil millones (10^{10}) de divisiones por segundo.*

Entonces para realizar las divisiones necesarias, necesitaríamos más de

$$\frac{10^{50}}{10^{10}} \text{ segs } = 10^{40} \text{ segs } > 10^{36} \text{ horas } > 10^{34} \text{ días } > 10^{31} \text{ años .}$$

Esto supera ampliamente la vida del universo que es aproximadamente 20mil millones de años, es decir, 2×10^{10} años.

La cantidad de **bits** necesaria para almacenar un número n en la computadora, es la cantidad de dígitos de n escrito en base 2. Por ejemplo el número 123456789 escrito en base 2 es $111010110111100110100010101$ y por lo tanto requiere 27 bits. Observar que $\log_2 123456789 = 26{,}879431$. En general si escibimos $n = a_k 2^k + \cdots a_1 2 + a_0$ con $a_i \in \{0, 1\}$ y $a_k = 1$, tenemos que la cantidad de bits de n es

$$k + 1 = \left(\log_2 2^k\right) + 1 \leq \left(\log_2 \left(2^k + \cdots + a_1 2 + a_0\right)\right) + 1 = (\log_2 n) + 1.$$

Además, como $n < 2^{k+1}$ tenemos que $\log_2 n < k + 1$.

Así que tenemos que $\log_2 n < k + 1 \leq \log_2 n + 1$. Si llamamos b_n a la cantidad de bits necesarios para n, tenemos que para n lo suficientemente grande $b_n \simeq (\log_2 n) + 1$.

Por lo tanto, la cantidad de operaciones necesarias para factorizar n, en el peor de los casos es

$$\sqrt{n} = \sqrt{2^{\log_2 n}} = 2^{\frac{1}{2}\log_2 n} = 2^{\frac{1}{2}(b_n - 1)}.$$

Por lo tanto la cantidad de operaciones depende exponencialmente en la cantidad de bits, y por eso decimos que el algoritmo es de **tiempo exponencial**.

Es un tema de constante investigación buscar mejores algoritmos de factorización. Hasta hoy, el mejor algoritmo para factorizar enteros de más de 100 dígitos es el llamado *Criba General del Cuerpo de Números* (General Number Field Sieve), debido a John Pollard en 1996. Este algoritmo es de tiempo **subexponencial**, del orden de

$$e^{c(\ln(n))^{1/3}(\ln\ln(n))^{2/3}} = e^{c'(b_n - 1)^{1/3}(\ln(b_n - 1))^{2/3}}$$

para factorizar un entero n (donde c y c' son constantes conocidas). Si bien con los temas del curso no nos da para cubrir este algortimo, recomendamos al interesado estudiar previamente teoría de Anillos para poder comprenderlo.

Con el desarrollo de la computación cuántica, han surgido nuevos algoritmos para computadoras cuánticas. El Algoritmo de Peter Shor, de 1994, en un computadora cuántica correría en tiempo **polinomial**, del orden de $\ln(n)^3 = c.(b_n - 1)^3$. En 2001, utilizando una implementación de resonancia magnética nuclear de una computadora cuántica de 7 qubits, se pudo comprobar este algoritmo factorizando $15 = 3 \times 5$. Si se lograra obtener una computadora cuántica de suficientes qubits, con este algoritmo se podrían quebrar los sistemas de encriptado más utilizados, como por ejemplo el RSA.

Capítulo 2

Congruencias

2.1. Introducción

Cuando clasificamos un número como par o impar, estamos usando el concepto de congruencia. En el algoritmo de división, un número par es un número que tiene un resto 0 cuando es dividido por 2 y un número impar es uno que tiene resto 1 cuando es dividido por 2. Aunque nadie diría que 14 y 96 son el mismo número, comparten la propiedad de que tienen el mismo resto al ser divididos por 2. De manera similar, cuando uno mira un reloj que marca las $10{:}00$ y sabe que en 5 horas marcara las $3{:}00$, no esta diciendo que $10 + 5 = 3$. Lo que en realidad está haciendo, tal vez sin darse cuenta, es $10 + 5 = 15$ y dividir por 12, lo cual tiene resto es 3. Las congruencias generalizan estos conceptos para todos los enteros, decimos que dos números son congruentes para el número n si tienen el mismo resto al dividir por n. Volviendo al ejemplo del reloj, 3 y 15 son congruentes para el número 12 porque tienen resto 3 al dividir por 12.

2.2. Definiciones y primeras propiedades.

Definición 2.2.1. 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 $n \mid a - b$. En caso contrario escribiremos

$$a \not\equiv b \pmod{n}.$$

Ejemplos 2.2.2. *Veamos los primeros ejemplos.*

1. *Si* $n = 1$, *tenemos que* $a \equiv b \pmod{n}$ *si y sólo si* $1 \mid a - b$. *Por lo tanto,* $a \equiv b \pmod{1}$ *para todo* $a, b \in \mathbb{Z}$.
2. *Si* $n = 0$, *tenemos que* $a \equiv b \pmod{n}$ *si y sólo si* $0 \mid a - b$; *es decir, si y sólo si* $a = b$.
3. *Si* $n = 2$, *tenemos que* $a \equiv 0 \pmod{2}$ *si y sólo si* $2 \mid a - 0$; *es decir, si y sólo si* a *es par. Por otro lado,* $a \equiv 1 \pmod{2}$ *si y sólo si* $2 \mid a - 1$; *es decir, si y sólo si* a *es impar.*
4. $a \equiv 0 \pmod{n}$ *si y sólo si* $n \mid a$.
5. $5 \equiv 11 \pmod{6}$, $5 \equiv 17 \pmod{6}$ *y* $5 \equiv -1 \pmod{6}$.

Las siguientes propiedades son inmediatas de la definición y de las propiedades de divisibilidad, las demostraciones quedan a cargo del lector.

Proposición 2.2.3. *1. La congruencia módulo n es una relación de equivalencia.*

2. $a \equiv b \pmod{n}$ *si y sólo 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 $r \in \{0, 1, \cdots, n-1\}$ tal que $a \equiv r \pmod{n}$ (r es el resto de dividir a entre n).*

Ahora nos preguntamos si vale la propiedad cancelativa para congruencias. Veamos algunos ejemplos:

1. 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 bien, ¿por qué podemos cancelar el 2?

   La congruencia $6 \equiv 16 \pmod{5}$ es cierta pues $5 \mid (16-6)$; factorizando el 2, tenemos que $5 \mid 2(8-3)$. Como 5 y 2 son coprimos, por el Lema de Euclides, obtenemos que entonces $5 \mid (8-3)$ y por lo tanto $3 \equiv 8 \pmod{5}$. Aquí utilizamos que $\mcd(5,2) = 1$; veamos que ésto es absolutamente necesario para poder cancelar y obtener una congruencia con el mismo módulo.

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 $5 \mid (10-5) = 5(2-1)$ no implica que $5 \mid (2-1)$.

3. Veamos otro caso en que el factor común no es coprimo con el módulo: tenemos que $6 \equiv 16 \pmod{10}$, es decir $2 \times 3 \equiv 2 \times 8 \pmod{10}$. Claramente no podemos cancelar el 2 pues $3 \not\equiv 8 \pmod{10}$. Pero observemos que $3 \equiv 8 \pmod{5}$!! ¿qué pasó aquí? Bueno, tenemos que $6 \equiv 16 \pmod{10}$ dado que $10 \mid (16-6)$; ésto es $2 \times 5 \mid 2(8-3)$; es decir que existe $e \in \mathbb{Z}$ tal que $2(8-3) = 2 \times 5\, e$. Ahora por la cancelativa del producto en $\mathbb{Z}$, tenemos entonces que $8 - 3 = 5e$ y por lo tanto $5 \mid (8-3)$ y entonces $3 \equiv 8 \pmod{5}$.

4. En el ejemplo anterior, el factor en común 2, era un divisor del módulo. Veamos que esto no es necesario para cancelar y obtener una congruencia con un módulo distinto: por ejemplo $12 \equiv 42 \pmod{10}$, es decir $6 \times 2 \equiv 6 \times 7 \pmod{10}$ y si bien $2 \not\equiv 7 \pmod{10}$, lo que sí vale es que $2 \equiv 7 \pmod{5}$. Si quisiéramos deducir esta congruencia a partir de la primera, podríamos proceder en dos pasos.

   Primero, como $12 \equiv 42 \pmod{10}$, tenemos que $2 \times 6 \equiv 2 \times 21 \pmod{10}$ y de forma análoga a lo hecho en el ejemplo anterior obtenemos que $6 \equiv 21 \pmod{5}$. Ahora tenemos que $3 \times 2 \equiv 3 \times 7 \pmod{5}$, y como $\mcd(3,5) = 1$, procediendo de forma análoga a lo hecho en el ejemplo (1), obtenemos que $2 \equiv 7 \pmod{5}$.

Resumimos en la próxima proposición lo observado en estos ejemplos (y la demostración es totalmente análoga a lo hecho en los ejemplos).

Proposición 2.2.4. *[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 $c \mid n$ y $ca \equiv cb \pmod{n}$ entonces $a \equiv b \left(\mod \frac{n}{c}\right)$.*

3. *Si $ca \equiv cb \pmod{n}$ entonces $a \equiv b \left(\mod \frac{n}{\mcd(c,n)}\right)$.*

Demostración. 1. Tenemos que $ca \equiv cb \pmod{n}$, es decir $n \mid (ca - cb)$. Entonces $n \mid c(a-b)$ y como $\mcd(c,n) = 1$ por el Lema de Euclides obtenemos que $n \mid (a-b)$ y por lo tanto $a \equiv b \pmod{n}$.

2. Si $c \mid n$, existe un $k \in \mathbb{Z}$ tal que $n = ck$. Si además $ca \equiv cb \pmod{n}$ entonces $ck = n \mid c(a-b)$. 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 $k \mid (a-b)$ y entonces $a \equiv b \pmod{k}$, es decir $a \equiv b \left(\mod \frac{n}{c}\right)$.

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 $dc^*a \equiv dc^*b \pmod{dn^*}$, 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 $a \equiv b \left(\mod \frac{n}{\mcd(c,n)}\right)$.

□

Observar que separamos el enunciado en 3 partes simplemente para simplificar la demostración, pero el tercer enunciado abarca los 3 anteriores. Es decir, que podemos enunciar la propiedad cancelativa simplemente como

$$\text{si } c \neq 0 \text{ y } ca \equiv cb \pmod{n} \quad \text{entonces} \quad a \equiv b \left(\mod \frac{n}{\mcd(c,n)}\right).$$

2.3. Algunas aplicaciones

Veamos algunas aplicaciones interesantes de utilizar congruencias. Para ésto necesitaremos las siguientes propiedades que están como ejericicio en el repartido de práctico de congruencias:

Proposición 2.3.1. *Sean $a, b, c, n, m \in \mathbb{Z}$.*

1. $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n} \Rightarrow a + c \equiv b + d \pmod{n}$ *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* $n \in \mathbb{N} \Rightarrow a^n \equiv b^n \pmod{m}$.

2.3.1. Criterios de divisibilidad

Veamos algunos criterios de divisibilidad conocidos por todos:

Proposición 2.3.2. *Si los dígitos de a son $a = a_k \cdots a_1 a_0$. Entonces $3 \mid a$ si y sólo si $3 \mid a_0 + a_1 + \cdots + a_k$.*

Demostración. Tenemos que $a = a_k 10^k + \cdots a_1 10 + a_0$. Tenemos que $3 \mid a$ si y sólo si $a \equiv 0 \pmod{3}$; es decir, si y sólo 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 última 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 $i = 0, \cdots, k$ 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 divide a a, si y sólo si 3 divide a la suma de sus dígitos. □

Observar que en la última proposición, lo único que utilizamos (además de las propiedades de congruencia) es que $10 \equiv 1 \pmod{3}$. Como también $10 \equiv 1 \pmod{9}$, de forma análoga se prueba el siguiente criterio de divisibilidad entre 9:

Proposición 2.3.3. *Si los dígitos de a son $a = a_k \cdots a_1 a_0$. Entonces $9 \mid a$ si y sólo si $9 \mid a_0 + a_1 + \cdots + a_k$.*

2.3.2. Dígitos verificadores

Veamos una aplicación de las congruencias muy utilizada como lo son los dígitos verificadores (en la cédula de identidad, en códigos ISBN de libros, etc). Veremos con detalle el caso del código ISBN de los libros y dejaremos planteado en el práctico el caso del dígito verificador de la cédula de identidad.

El International Standard Book Number (conocido como el número ISBN) es una cadena de diez símbolos que identifica a los libros. Los primeros nueve símbolos son dígitos, y el último es el *símbolo verificador*.

Es entonces una cadena $x_1x_2\dots x_9-x_{10}$ donde cada $x_1, x_2, \cdots, x_9$ 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. Sea

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

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

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

Ejemplo 2.3.4. *Si los primeros 9 símbolos de un ISBN son* 038798403, *entonces* $r \equiv 1(0)+2(3)+3(8)+4(7)+5(9)+6(8)+7(4)+8(0)+9(3) \pmod{11} \equiv 6+24+28+45+48+28+27 \equiv 6+2+6+1+4+6+5 \pmod{11} \equiv 8 \pmod{11}$.

Así que el dígito verificador de este código es 8, *y por lo tanto el libro tiene el código ISBN* $038798403-8$. *Teniendo el código ISBN, existen varios motores de búsqueda para conseguir la información del libro.*

Ahora bien, ¿para qué sirve el dígito verificador?. Es de esperar que si uno comete ciertos errores al copiar un ISBN, entonces la relación $x_{10} \equiv \sum_{i=1}^{9} i \cdot x_i \pmod{11}$ ya no se cumpla.

Por ejemplo, si en un motor de búsqueda (por ejemplo http://www.isbn-check.de/) buscamos el libro con número $038798503-8$, obtendremos un mensaje del estilo "el número ingresado no es código ISBN", o "la secuencia ingresada falló el test del dígito verificador"(además, en muchas páginas nos dicen cuáles son los posibles errores cometidos). Este mensaje significa que para los primeros 9 símbolos ingresados, el último símbolo debería haber sido distinto al ingresado.

Veamos ésto: $c = 1(0)+2(3)+3(8)+4(7)+5(9)+6(8)+7(5)+8(0)+9(3) = 6+24+28+45+48+35+27 \equiv 6+2+6+1+4+2+5 \equiv 4 \pmod{11}$. Efectivamente, el último símbolo debería haber sido un 4 y no un 8. Lo que mostramos con este ejemplo sucede en general: si copiamos mal únicamente un dígito de los primeros 9, entonces el dígito verificador no verifica la congruencia que tiene que verificar. Dicho de otra forma, si tenemos dos códigos ISBN tales que en los primeros 9 símbolos sólo tienen uno distinto, entonces sus dígitos verificadores son distintos. Diremos entonces que el dígito verificador *detecta el error de copiar mal uno de los primero 9 símbolos*. Probemos esta propiedad:

Proposición 2.3.5. *Sean* $x_1x_2\dots x_9-x_{10}$ *y* $y_1y_2\dots y_9-y_{10}$ *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

$$\sum_{i=1}^{9} i \cdot x_i \equiv \sum_{i=1}^{9} i \cdot y_i \pmod{11}.$$

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 $\mathrm{mcd}(k, 11) = 1$, 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.

□

Dejamos como ejercicio en el práctico investigar si el dígito verificador detecta el error de intercambiar dos de los primeros 9 símbolos. Desde hace un par de años, para evitar que se agoten los códigos ISBN, se está utilizando un nuevo código ISBN con 13 símbolos. Dejamos a cargo del lector interesado, que busque información sobre este código y los errores que detecta.

2.4. Ecuaciones con congruencias

En esta sección veremos cuándo una ecuación lineal (en una variable) con congruencias módulo n tiene soluciones, y en caso que las tenga, queremos saber cuántas soluciones tiene. Veamos primero con algunos ejemplos las distintas situaciones que podemos tener, y luego demostraremos el teorema en general.

Ejemplos 2.4.1. *En todos estos ejemplos nos interesa hallar todos los $x \in \mathbb{Z}$ que verifican la ecuación planteada:*

1. *Veamos si existen $x \in \mathbb{Z}$ tales que $4x \equiv 3 \pmod{6}$. Primero observemos que si $x \equiv x' \pmod{6}$, $4x \equiv 4x' \pmod{6}$ y entonces x es solución si y sólo si x' es solución. Por lo tanto, basta con buscar soluciones en el conjunto $\{0, 1, \cdots, 5\}$. Observando que $4 \times 0 = 0, 4 \times 1 = 4$, $4 \times 2 = 8 \equiv 2 \pmod{6}$, $4 \times 3 = 12 \equiv 0 \pmod{6}$, $4 \times 4 = 16 \equiv 4 \pmod{6}$, $4 \times 5 = 20 \equiv 2 \pmod{6}$, vemos que* **no existe** *$x \in \{0, 1, \cdots, 5\}$ tal que $4x \equiv 3 \pmod{6}$, por lo que la* **ecuación no tiene solución.**

   ¿Cuál es el motivo de que no tenga solución? Existe $x \in \mathbb{Z}$ tal que $4x \equiv 3 \pmod{6}$ si y sólo si existe $x \in \mathbb{Z}$ tal que $6 \mid (4x - 3)$; si y sólo si, existen $x, y \in \mathbb{Z}$ tal que $4x - 3 = 6y$. Es decir que la ecuación tiene solución si y sólo si, existen $x, y \in \mathbb{Z}$ tales que $4x - 6y = 3$. El problema entonces es equivalente a resolver una ecuación diofántica, y como $\mathrm{mcd}(4, 6) = 2 \nmid 3$, por el Teorema de Ecuaciones Diofánticas 1.5.3, sabemos que esta diofántica no tiene solución.

2. *Veamos si existen $x \in \mathbb{Z}$ tales que $4x \equiv 2 \pmod{6}$. Por lo calculado en el ejemplo anterior, vemos que $x = 2$ y $x = 5$ cumplen la ecuación, y por lo tanto cualquier entero congruente con ellos módulo 6 también cumple la ecuación. Es decir que las soluciones son $x = 2 + 6k$ y $x = 5 + 6k$ con $k \in \mathbb{Z}$. O dicho de forma más económica, las soluciones de la ecuación son $x \equiv 2 \pmod{6}$ y $x \equiv 5 \pmod{6}$. Es decir que tenemos* **exactamente 2 soluciones distintas** *(no congruentes)* **módulo 6.**

   Observar que si lo resolvíamos con ecuaciones diofánticas, obtenemos la ecuación $4x - 6y = 2$, y como $\mathrm{mcd}(4, 6) = 2 \mid 2$, tenemos que la ecuación diofántica tiene (infinitas) soluciones. Por ejemplo $(x_0, y_0) = (2, 1)$ es una solución. El Teorema de Ecuaciones Diofánticas nos dice además que todas las soluciones de la ecuación son $(x, y) = \left(2 + \frac{6}{2}k, 1 + \frac{4}{2}k\right) = (2 + 3k, 1 + 2k)$ con $k \in \mathbb{Z}$. Como para obtener nuevas soluciones debemos sumar múliplos de 3, **en un intervalo de largo 6 tendremos dos soluciones**, *una congruente a 2 y otra congruente a 2+3= 5 módulo 6.*

3. *Por último veamos si la ecuación $5x \equiv 4 \pmod{6}$ tiene solución; nuevamente, probando con los enteros en $\{0, 1, \cdots, 5\}$, vemos que el único que verifica la ecuación es $x = 2$ y por lo tanto, las soluciones de la ecuación son los x tales que $x \equiv 2 \pmod{6}$. En este caso la* **ecuación tiene un única solución módulo 6.**

Vimos entonces que una ecuación de la forma $ax \equiv b \pmod{n}$, puede no tener solución. Cuando tiene solución, tiene infinitas, pero puede haber una única o varias soluciones módulo n. Veamos ahora el teorema en general, que resume los observado en los ejemplos.

Teorema 2.4.2. *Dados $a, b, n \in \mathbb{Z}$ y sea $d = \mathrm{mcd}(a, n)$. Entonces la ecuación*

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

tiene solución si y sólo si $d \mid b$. Además, si $d \mid b$ existen exactamente d soluciones distintas módulo n.

Demostración. Como observamos antes, tenemos que $ax \equiv b \pmod{n}$ si y sólo si $n \mid (ax - b)$, 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 sólo si existen $x, y \in \mathbb{Z}$ tales que $ax - ny = b$. Por el Teorema de Ecuaciones Diofánticas, sabemos que ésto sucede si y sólo si $d \mid b$.

Ahora, en el caso que $d \mid b$, 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 $\left\{(x, y) = \left(x_0 + \frac{n}{d}k,\, y_0 + \frac{a}{d}k\right) ;\, k \in \mathbb{Z}\right\}$. 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 $x_0, x_1 = x_0 + \frac{n}{d}, x_2 = x_0 + 2\frac{n}{d}, \cdots, x_{d-1} = x_0 + (d-1)\frac{n}{d}$ son d soluciones que no son congruentes entre ellas módulo n. Esto es porque si $i \neq j$, $0 \neq |x_i - x_j| = \left|x_0 + i\frac{n}{d} - x_0 - j\frac{n}{d}\right| = |(i-j)\frac{n}{d}| \leq (d-1)\frac{n}{d} < n$; por lo tanto $n \nmid x_i - x_j$ y entonces $x_i \not\equiv x_j \pmod{n}$. Veamos ahora que cualquier otra solución es congruente (módulo n) a una de éstas.

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 $x = x_0 + \frac{n}{d}k = x_0 + \frac{n}{d}(dq + i) = x_0 + i\frac{n}{d} + qn = x_i + qn \equiv x_i \pmod{n}$. □

Terminamos esta sección haciendo algunos comentarios sobre invertibilidad módulo n.

Definición 2.4.3. Decimos que un entero a es **invertible** módulo n, si existe otro entero x tal que $ax \equiv 1 \pmod{n}$. Al entero x se le llama **inverso** de a módulo n.

Ejemplos 2.4.4.

1. *Veamos si 4 es invertible módulo 6. Tenemos que ver si existe $x \in \mathbb{Z}$ tal que $4x \equiv 1 \pmod{6}$. Es decir, tenemos que resolver una ecuación con congruencias. Ahora, como $\mathrm{mcd}(4, 6) = 2 \nmid 1$, por el teorema recién visto, la ecuación $4x \equiv 1 \pmod{6}$ no tiene solución. Por lo tanto, 4 no es invertible módulo 6.*

2. *Veamos ahora si 4 es invertible módulo 17. Tenemos que ver si existe $x \in \mathbb{Z}$ tal que $4x \equiv 1 \pmod{17}$. Por el teorema recién visto, como $\mathrm{mcd}(4, 17) = 1 \mid 1$, tenemos que la ecuación tiene solución y que además hay una única solución módulo 17.*

   Para hallar el inverso de 4 módulo 17, tenemos que resolver la ecuación $4x \equiv 1 \pmod{17}$, lo que equivale a resolver la ecuación diofántica $4x - 17y = 1$. Ahora, como ya sabemos que hay un único x módulo 17, basta con encontrar una solución de la diofántica (por ejemplo utilizando el Algoritmo de Euclides). Por ejemplo $(x, y) = (-4, 1)$ es solución y por lo tanto el inverso de 4 módulo 17 es $x \equiv -4 \pmod{17}$, es decir $x \equiv 13 \pmod{17}$.

Claramente, la condición de que a sea invertible módulo n es equivalente a que la ecuación $ax \equiv 1 \pmod{n}$ tenga solución. Por lo tanto tenemos el siguiente corolario del Teorema 2.4.2:

Corolario 2.4.5. *Un entero a es invertible módulo n si y sólo si $\mathrm{mcd}(a, n) = 1$. Además, si a es invertible, el inverso de a módulo n es único módulo n.*

2.5. Teorema Chino del resto

Hace más de 1700 años, el matemático chino Sun Tzu planteó el problema de encontrar un número cuyo resto al dividirlo entre 3 sea 2, el resto al dividirlo entre 5 sea 3 y el resto al dividirlo entre 7 sea 2. En términos de congruencias, buscaba un entero x tal que

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7. \end{cases}$$

Comencemos investigando si existen $x \in \mathbb{Z}$ que cumplan las primeras 2 congruencias, es decir, buscamos resolver

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5. \end{cases} \tag{2.5.1}$$

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

$$x = 2 + 3s, \tag{2.5.2}$$

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

$$x = 3 + 5t. \tag{2.5.3}$$

Por lo tanto, debemos encontrar $x \in \mathbb{Z}$ que verifique estas dos últimas condiciones. Es decir, que existe $x \in \mathbb{Z}$ que verifica las congruencias si y sólo si (igualando las ecuaciones (2.5.2) y (2.5.3))

$$\exists\, s, t \in \mathbb{Z} : \quad 2 + 3s = 3 + 5t$$

si y sólo si

$$\exists\, s, t \in \mathbb{Z} : \quad 3s - 5t = 1. \tag{2.5.4}$$

Nuevamente el problema original terminó siendo equivalente a resolver una ecuación diofántica. En este caso, como $\mathrm{mcd}(3, 5) = 1$, por el Teorema de Ecuaciones Diofánticas, la ecuación tiene solución. Una particular es $(s_0, t_0) = (2, 1)$, por lo que todas las soluciones son $(s, t) = (2 + 5k, 1 + 3k) : k \in \mathbb{Z}$. Ahora sustituyendo el s de estas soluciones en (2.5.2), obtenemos que $x = 2 + 3s = 2 + 3(2 + 5k) = 2 + 6 + 15k = 8 + 15k$, $k \in \mathbb{Z}$.

Hemos obtenido entonces que las soluciones del sistema (2.5.1) son $x = 8+15k, k \in \mathbb{Z}$. Es decir, las soluciones son $x \equiv 8 \pmod{15}$.

Así que obtuvimos **una única solución módulo 15**.

Observar que en particular obtuvimos

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \end{cases} \Leftrightarrow x \equiv 8 \pmod{15}. \tag{2.5.5}$$

Ahora bien, si queremos resolver el sistema original con tres congruencias

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases} \tag{2.5.6}$$

por lo recién observado, ésto equivale a resolver

$$\begin{cases} x \equiv 8 \pmod{15} \\ x \equiv 2 \pmod 7 \end{cases}$$

Prosiguiendo de forma análoga a lo hecho antes, tendremos $x = 8 + 15k = 2 + 7h$, y obtenemos la ecuación diofántica $15k - 7h = -6$. Nuevamente, esta diofántica tiene solución pues $\mathrm{mcd}(15, 7) = 1$ y tenemos que sus soluciones son $(k, h) = (-6 + 7r, -12 + 15r) : r \in \mathbb{Z}$. Y sustituyendo obtenemos que

$$x = 8 + 15k = 8 + 15(-6 + 7r) = 8 - 90 + 105r = -82 + 105r \equiv 23 \pmod{105}.$$

Hemos probado que el sistema (2.5.6) tiene solución, y **tiene única solución módulo 105**, $x \equiv 23 \pmod{105}$. Observar que tanto en la existencia de una solución, como en su unicidad módulo 105, fue fundamental que $\mathrm{mcd}(3, 5) = 1$ y que $\mathrm{mcd}(15, 7) = 1$; es decir, que los enteros $3, 5$ y 7 son coprimos dos a dos.

Enunciamos ahora el teorema que generaliza lo observado en el ejemplo: el Teorema Chino del Resto.

Teorema 2.5.1 (Teorema Chino del Resto)**.** *Sean* $m_1, m_2, \cdots, m_k$ **enteros coprimos dos a dos** *y* $a_1, a_2, \cdots, a_k \in \mathbb{Z}$*. Entonces el sistema*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{2.5.7}$$

tiene solución, y hay una única solución módulo $m_1 m_2 \cdots m_k$*. Es decir, si* x_0 *es solución, entonces todas las soluciones son* $x \equiv x_0 \pmod{m_1 m_2 \cdots m_k}$.

Demostración. Haremos la demostración por inducción en k (la cantidad de ecuaciones), siendo el paso $k = 2$ totalmente análogo a lo que hicimos en el ejemplo. Consideremos entonces dos enteros m_1, m_2 coprimos, $a_1, a_2 \in \mathbb{Z}$ y el sistema

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2}. \end{cases} \tag{2.5.8}$$

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

$$x = a_1 + m_1 s, \tag{2.5.9}$$

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

$$x = a_2 + m_2 t. \tag{2.5.10}$$

Por lo tanto, debemos encontrar $x \in \mathbb{Z}$ que verifique estas dos últimas condiciones. Es decir, que existe $x \in \mathbb{Z}$ que verifica las congruencias si y sólo si (igualando las ecuaciones (2.5.9) y (2.5.10))

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

Es decir, si y sólo si

$$\exists\, s, t \in \mathbb{Z} : \quad m_1 s - m_2 t = a_2 - a_1. \tag{2.5.11}$$

Como $\mathrm{mcd}(m_1, m_2) = 1$, por el Teorema de Ecuaciones Diofánticas, la ecuación diofántica (2.5.11) tiene solución. Además, 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 en (2.5.9), 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 (2.5.8) tiene solución x_0 y todas las soluciones son $x \equiv x_0 \pmod{m_1 m_2}$.

Así que obtuvimos **una única solución módulo** m_1m_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

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_{k-1} \pmod{m_{k-1}} \end{cases} \tag{2.5.12}$$

tiene solución x_1 y que además cualquier solución cumple $x \equiv x_1 \pmod{m_1m_2\cdots m_{k-1}}$; por lo tanto, este sistema con $k-1$ ecuaciones es equivalente a la ecuación $x \equiv x_1 \pmod{m_1m_2\cdots m_{k-1}}$.

Entonces el sistema con k ecuaciones

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_{k-1} \pmod{m_{k-1}} \\ x \equiv a_k \pmod{m_k} \end{cases} \tag{2.5.13}$$

es equivalente al sistema

$$\begin{cases} x \equiv x_1 \pmod{m_1m_2\cdots m_{k-1}} \\ x \equiv a_k \pmod{m_k}. \end{cases} \tag{2.5.14}$$

Como los enteros $m_1, m_2, \cdots, m_k$ son coprimos 2 a 2, tenemos que $\mcd(m_1m_2\cdots m_{k-1}, m_k) = 1$. Por lo tanto tenemos un sistema con 2 ecuaciones que involucran módulos coprimos. Por lo ya probado para $k = 2$, tenemos entonces que el sistema (2.5.14) tiene solución $x_0 \in \mathbb{Z}$ y además que toda solución cumple $x \equiv x_0 \pmod{(m_1m_2\cdots m_{k-1}) \cdot m_k}$.

Por lo tanto el sistema (2.5.13) tiene solución x_0, y las soluciones son $x \equiv x_0 \pmod{m_1m_2\cdots m_{k-1}m_k}$; es decir, la solución es única módulo $m_1m_2\cdots m_k$.

□

Observaciones 2.5.2. *Hagamos algunas observaciones sobre el teorema recién visto:*

1. *En algunos casos, cuando uno de los módulos es pequeño, no es necesario recurrir a las ecuaciones diofánticas para encontrar las soluciones. Por ejemplo, supongamos queremos resolver el sistema:*

$$\begin{cases} x \equiv 3 \pmod{17} \\ x \equiv 2 \pmod{4}. \end{cases}$$

Por el Teorema Chino del Resto, sabemos que existe una solución x_0, pero además que las soluciones son $x \equiv x_0 \pmod{17 \times 4}$. Por lo tanto nos basta con encontrar una solución para tenerlas todas y además en cualquier intervalo de largo 17×4 vamos a tener una solución. La primer congruencia (aquí tomamos la congruencia que involucre al módulo más grande) nos dice que $x = 3 + 17k$ con $k \in \mathbb{Z}$. Pero por lo recién observado, en el conjunto $A = \{3,\ 3+17,\ 3+17\times 2, 3+17\times 3\}$ debe haber una solución (observar que el siguiente candidato $3 + 17 \times 4 \equiv 3 \pmod{17 \times 4}$, etc., por lo que los demás enteros de la forma $x = 3+17k$ serán congruentes módulo 17×4 a uno de los enteros del conjunto A). Así que para encontrar una solución del sistema, basta con verificar cuál de los 4 enteros de A cumple con la segunda congruencia. Tenemos que $3 \not\equiv 2 \pmod 4$, $3 + 17 = 20 \not\equiv 2 \pmod 4$, $3 + 17 \times 2 = 37 \not\equiv 2 \pmod 4$ y finalmente $3 + 17 \times 3 = 54 \equiv 2 \pmod 4$, por lo que $x_0 = 54$ es solución del sistema y tenemos que las soluciones son $x \equiv 54 \pmod{17 \times 4}$. Este método es eficiente porque el cardinal de A, el conjunto de candidatos, es pequeño pues uno de los dos módulos de las ecuaciones con congruencias es pequeño.

2. *Si tenemos un sistema de la forma*

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases}$$

con $\mcd(m_1, m_2) = 1$, *claramente* $x_0 = a$ *es solución, y por lo visto en el Teorema Chino del Resto, todas las soluciones del sistema son* $x \equiv a \pmod{m_1 m_2}$. *Es decir que tenemos*

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases} \Leftrightarrow x \equiv a \pmod{m_1 m_2}.$$

Esta equivalencia se podría haber probado sin usar el Teorema:

- *Por definición de congruencia tenemos que*

$$\left.\begin{array}{l} x \equiv a \pmod{m_1} \Leftrightarrow m_1 \mid (a-x) \\ x \equiv a \pmod{m_2} \Leftrightarrow m_2 \mid (a-x) \end{array}\right\} \underset{\mcd(m_1,m_2)=1}{\Longrightarrow} m_1 m_2 \mid (a-x) \Rightarrow x \equiv a \pmod{m_1 m_2}.$$

- *Para el recíproco no se necesita el hecho de que* m_1 *y* m_2 *sean coprimos pues (por la transitividad de la divisibilidad) si* $m_1 m_2 \mid (a-x)$ *tenemos que* $m_1 \mid (a-x)$ *y* $m_2 \mid (a-x)$.

3. *Vale la pena aclarar que el directo es* **falso** *si* $\mcd(m_1, m_2) \neq 1$. *Por ejemplo*

$$\begin{cases} x \equiv 1 \pmod{4} \\ x \equiv 1 \pmod{6} \end{cases}$$

no implica *que* $x \equiv 1 \pmod{24}$. *Por ejemplo,* $x = 13$ *cumple ambas congruencias del sistema, pero* $13 \not\equiv 1 \pmod{24}$. *Lo que sí vale es que* $13 \equiv 1 \pmod{12}$, *y en general lo que vale es que* $x \equiv 1 \pmod{12}$. *Esto es porque el hecho que* $4 \mid (x-1)$ *y* $6 \mid (x-1)$ **no implica** *que* $24 \mid (x-1)$, *pero sí implica que* $\mcm(4, 6) \mid (x-1)$*; es decir, implica que* $12 \mid (x-1)$.

4. *De forma análoga a lo hecho recién, tenemos entonces que si* m_1 *y* m_2 *son dos enteros cualesquiera y* $a \in \mathbb{Z}$ *entonces*

$$\begin{cases} x \equiv a \pmod{m_1} \\ x \equiv a \pmod{m_2} \end{cases} \Leftrightarrow x \equiv a \pmod{\mcm(m_1, m_2)}.$$

5. *Veamos una técnica útil para resolver algunos sistemas de ecuaciones de congruencias. Sea el sistema*

$$\begin{cases} x \equiv 4 \pmod{7} \\ x \equiv 2 \pmod{13} \\ x \equiv 15 \pmod{17} \end{cases}.$$

Si consideramos el cambio de variable lineal $x' = x - 15$ *el sistema queda*

$$\begin{cases} x' \equiv 4 - 15 \pmod{7} \\ x' \equiv 2 - 15 \pmod{13} \\ x' \equiv 15 - 15 \pmod{17} \end{cases} \Longleftrightarrow \begin{cases} x' \equiv 3 \pmod{7} \\ x' \equiv 0 \pmod{13} \\ x' \equiv 0 \pmod{17} \end{cases} \Longleftrightarrow \begin{cases} x' \equiv 3 \pmod{7} \\ x' \equiv 0 \pmod{13 \times 17} \end{cases}.$$

El sistema tiene solución $x' = 3 \times 13 \times 17 \times ((13 \times 17)^{-1} \pmod{7})$. *Fácilmente se puede calcular* $(13 \times 17)^{-1} \equiv (4)^{-1} \pmod{7} \equiv 2 \pmod{7}$. *Por lo tanto* $x' \equiv 1326 \pmod{7 \times 13 \times 17}$, *y deshaciendo el cambio de variable obtenemos* $x \equiv 1326 + 15 \pmod{7 \times 13 \times 17} \equiv 1342 \pmod{7 \times 13 \times 17}$.

Nos queda ver qué sucede con sistemas de congruencias cuando los módulos no son coprimos. Veamos con ejemplos las distintas situaciones que podemos encontrar:

Ejemplo 2.5.3. *Si queremos resolver el sistema*

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 6 \end{cases}$$

1. *Podemos proceder de la misma manera que en el primer ejemplo de la sección y resolverlo usando ecuaciones diofánticas: la primer ecuación equivale a* $x = 3 + 4s$, $t \in \mathbb{Z}$, *y la segunda congruencia equivale a* $x = 0 + 6t$, $t \in \mathbb{Z}$. *Por lo tanto, igualando tenemos que ver si existen* $s, t \in \mathbb{Z}$ *tales que* $3 + 4s = 6t$, *lo que equivale a resolver la ecuación diofántica* $4s - 6t = -3$. *En este caso, como* $\mathrm{mcd}(4, 6) = 2$ *y* $2 \nmid (-3)$, *por el Teorema de Ecuaciones Diofánticas concluimos que esta ecuación no tiene solución, y por lo tanto el sistema original no tiene solución.*

2. *Otra forma de darnos cuenta que no tiene solución es la siguiente: por lo visto en las observaciones anteriores, como* $6 = 2 \times 3$ *y* $\mathrm{mcd}(2, 3) = 1$, *tenemos que:*

$$x \equiv 0 \pmod 6 \Leftrightarrow \begin{cases} x \equiv 0 \pmod 2 \\ x \equiv 0 \pmod 3), \end{cases}$$

y por lo tanto el sistema original es equivalente al sistema

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 0 \pmod 2 \\ x \equiv 0 \pmod 3). \end{cases}$$

Ahora, la primera congruencia nos dice que $4 \mid (x - 3)$ *y por lo tanto implica que* $2 \mid (x - 3)$. *Es decir que si* $x \equiv 3 \pmod 4$, *entonces* $x \equiv 3 \pmod 2$ *y entonces* $x \equiv 1 \pmod 2$. *Esta congruencia es incompatible con la segunda congruencia del sistema (*$x \equiv 0 \pmod 2$*) ya que el resto de dividir* x *entre* 2 *es único; no puede ser 1 y 2. Concluimos entonces que el sistema original no tiene solución.*

Ejemplo 2.5.4. *Si queremos resolver el sistema*

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 5 \pmod 6 \end{cases}$$

1. *Nuevamente podemos proceder usando ecuaciones diofánticas: la primer ecuación equivale a* $x = 3 + 4s$, $s \in \mathbb{Z}$, *y la segunda congruencia equivale a* $x = 5 + 6t$, $t \in \mathbb{Z}$. *Por lo tanto, igualando tenemos que ver si existen* $s, t \in \mathbb{Z}$ *tales que* $3 + 4s = 5 + 6t$, *lo que equivale a resolver la ecuación diofántica* $4s - 6t = 2$. *En este caso, como* $\mathrm{mcd}(4, 6) = 2$ *y* $2 \mid 2$, *por el Teorema de Ecuaciones Diofánticas tenemos que esta ecuación tiene solución. Una solución es* $(s_0, t_0) = (2, 1)$, *y todas las soluciones son* $(s, t) = \left(2 + \frac{6}{2}k, 1 + \frac{4}{2}k\right) = (2 + 3k, 1 + 2k)$ *con* $k \in \mathbb{Z}$. *Ahora, sustituyendo las soluciones para* s *en* $x = 3 + 4s$ *obtenemos que* $x = 3 + 4(2 + 3k) = 11 + 12k$. *Es decir que las soluciones del sistema son* $x \equiv 11 \pmod{12}$. *Observar que el* 12 *se obtuvo de* $4 \times \frac{6}{2} = \frac{4 \times 6}{\mathrm{mcd}(4,6)} = \mathrm{mcm}(4, 6)$.

2. *Hagámoslo de la otra forma obteniendo un sistema equivalente: en este caso como*

$$x \equiv 5 \pmod 6 \Leftrightarrow \begin{cases} x \equiv 5 \pmod 2 \equiv 1 \pmod 2 \\ x \equiv 5 \pmod 3 \equiv 2 \pmod 3), \end{cases}$$

tenemos que el sistema original es equivalente al sistema

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3. \end{cases}$$

Como $x \equiv 3 \pmod 4 \Rightarrow x \equiv 3 \pmod 2 \Rightarrow x \equiv 1 \pmod 2$, *tenemos que si un entero* x *cumple la primer congruencia del sistema* (2), *automáticamente verifica la segunda congruencia de ese sistema. Por lo tanto, la segunda ecuación es redundante y obtenemos que el sistema es equivalente a*

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 3. \end{cases}$$

Ahora como $\mcd(4,3) = 1$ *por el Teorema Chino del Resto sabemos que este sistema tiene solución, y que si* x_0 *es solución, todas las soluciones son* $x \equiv x_0 \pmod{4 \times 3}$. *Claramente* $x_0 = 11$ *es solución y por lo tanto todas las soluciones de este sistema (y del original) son* $x \equiv 11 \pmod{12}$.

Veamos un último ejemplo utilizando el método de encontrar un sistema equivalente.

Ejemplo 2.5.5. *Consideremos el sistema*

$$\begin{cases} x \equiv 5 \pmod 6 \\ x \equiv 26 \pmod{45} \\ x \equiv 11 \pmod{100}. \end{cases}$$

Utilizando que

$$\begin{aligned} x \equiv 5 \pmod 6 &\Leftrightarrow \begin{cases} x \equiv 5 \pmod 2 \equiv 1 \pmod 2 \\ x \equiv 5 \pmod 3 \equiv 2 \pmod 3, \end{cases} \\ x \equiv 26 \pmod{45} &\Leftrightarrow \begin{cases} x \equiv 26 \pmod 9 \equiv 8 \pmod 9 \\ x \equiv 26 \pmod 5 \equiv 1 \pmod 5, \end{cases} \\ x \equiv 11 \pmod{100} &\Leftrightarrow \begin{cases} x \equiv 11 \pmod{25} \\ x \equiv 11 \pmod 4 \equiv 3 \pmod 4, \end{cases} \end{aligned}$$

tenemos que el sistema original es equivalente al sistema

$$\begin{cases} x \equiv 1 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 8 \pmod 9 \\ x \equiv 1 \pmod 5 \\ x \equiv 11 \pmod{25} \\ x \equiv 3 \pmod 4. \end{cases}$$

Ahora como $x \equiv 3 \pmod 4 \Rightarrow x \equiv 3 \pmod 2 \Rightarrow x \equiv 1 \pmod 2$ *la última ecuación del sistema implica la primera, y por lo tanto no necesitamos incluir la primera. Como* $x \equiv 8 \pmod 9 \Rightarrow x \equiv 8 \pmod 3 \Rightarrow x \equiv 2 \pmod 3$, *la tercer ecuación implica la segunda, y por lo tanto no necesitamos la segunda ecuación. Y finalmente como* $x \equiv 11 \pmod{25} \Rightarrow x \equiv 11 \pmod 5 \Rightarrow x \equiv 1 \pmod 5$, *tampoco necesitamos la cuarta ecuación. Así que el sistema original es equivalente al sistema*

$$\begin{cases} x \equiv 8 \pmod 9 \\ x \equiv 11 \pmod{25} \\ x \equiv 3 \pmod 4. \end{cases}$$

y como los enteros $9, 25, 4$ son coprimos 2 a 2, este sistema tiene solución x_0 y todas las soluciones son $x \equiv x_0 \pmod{9 \times 25 \times 4}$ (dejamos como ejercicio verificar que las soluciones son $x \equiv 611 \pmod{900}$.)

Observación 2.5.6. *Generalizando lo visto en los ejemplos tenemos que si $m_1, \cdots, m_k$* **no son coprimos 2 a 2** *entonces el sistema*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

puede o no tener solución. En caso de que tenga una solución x_0, todas las soluciones son

$$x \equiv x_0 \pmod{\operatorname{mcm}(m_1, m_2, \cdots, m_k)}.$$

Dejamos el siguiente ejercicio al lector.

Ejercicio 2.5.7. *Dar una condición necesaria y suficiente para que el sistema*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \quad \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

tenga solución.

2.6. Exponenciación y Teoremas de Fermat y Euler

En esta sección buscamos técnicas que nos ayuden a calcular potencias módulo n. Es decir, dados $a, n \in \mathbb{Z}$ y $k \in \mathbb{N}$ queremos encontrar $r \in \{0, 1, \cdots, n-1\}$ tal que $a^k \equiv r \pmod{n}$. Por ejemplo, si buscamos $r \in \{0, 1, \cdots, 9\}$ tal que $3^{103} \equiv r \pmod{10}$, empezamos a calcular potencias de 3: $3^2 = 9 \equiv (-1) \pmod{10}$ por lo que $3^4 \equiv 1 \pmod{10}$. Así que $3^{103} = (3^4)^{25}3^3 \equiv 1^{25}3^3 \pmod{10} \equiv 27 \pmod{10} \equiv 7 \pmod{10}$ así que $r = 7$.

Entonces, en general, para hallar $r \in \{0, 1, \cdots, n-1\}$ tal que $a^k \equiv r \pmod{n}$ resultaría muy útil si podemos encontrar un exponente b tal que $a^b \equiv 1 \pmod{n}$. Observar que si tal $b > 1$ existe, en particular tendríamos que $a(a^{b-1}) \equiv 1 \pmod{n}$ así que a es invertible módulo n. Es decir, tal exponente b, sólo puede existir en los casos en que $\operatorname{mcd}(a, n) = 1$. En esta sección probaremos el Teorema de Euler, que nos dice que dado n, existe un exponente b que nos sirve para todos los a tales que $\operatorname{mcd}(a, n) = 1$. Por ejemplo, siguiendo con $n = 10$, tenemos que $7^2 = 49 \equiv (-1) \pmod{10}$ y entonces $7^4 \equiv 1 \pmod{10}$. También tenemos que $9^2 \equiv 1 \pmod{10}$, y si bien 4 no es la primera potencia de 9 con la cual llegamos al 1, también tenemos que $9^4 \equiv 1 \pmod{10}$. Acabamos de probar que para todo a con $\operatorname{mcd}(a, 10) = 1$, se cumple que $a^4 \equiv 1 \pmod{10}$. El exponente que nos va a servir para todo a coprimo con n es $\varphi(n)$, donde φ es la **función de Euler:**

Definición 2.6.1. La *función de Euler* es $\varphi : \mathbb{Z}^+ \to \mathbb{Z}^+$ dada por

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

Es decir que la función de Euler cuenta la cantidad de naturales coprimos con n y menores que n. Veamos algunos ejemplos:

Ejemplos 2.6.2. *1. Los naturales menores que 10 y coprimos con 10 son $\{1, 3, 7, 9\}$ por lo que $\varphi(10) = 4$.*

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

3. $\varphi\left(5^3\right) = \#\left\{a \in \{1, 2, \cdots, 125\} : \operatorname{mcd}(a, 5^3) = 1\right\} = \#\left\{a \in \{1, 2, \cdots, 125\} : \operatorname{mcd}(a, 5) = 1\right\}$. *Así que*

$$\varphi\left(5^3\right) = \#\{1, 2, \cdots, 125\} - \#\{a \in \{1, 2, \cdots, 125\} : \operatorname{mcd}(a, 5) \neq 1\}$$

y entonces

$$\varphi\left(5^3\right) = 125 - \#\{a \in \{1, 2, \cdots, 125\} : \operatorname{mcd}(a, 5) \neq 1\}. \tag{2.6.1}$$

Ahora, como 5 *es primo, tenemos que* $\operatorname{mcd}(a, 5) \neq 1 \Leftrightarrow 5 \mid a \Leftrightarrow a = 5k$ *para algún* $k \in \mathbb{Z}$. *Por lo tanto* $\{a \in \{1, \cdots, 125\} : \operatorname{mcd}(a, 5) \neq 1\} = \{a = 5k \text{ con } k \in \{1, 2, \cdots, 25\}\}$ *y el cardinal de este conjunto es* 25. *Por lo tanto, sustituyendo en* (2.6.1) *obtenemos que* $\varphi(125) = 125 - 25 = 100$.

4. *Siguiendo la idea del ejemplo de anterior, obtengamos una fórmula para* $\varphi\left(p^k\right)$ *cuando* p *es primo. Tenemos que*

$$\varphi\left(p^k\right) = \#\left\{a \in \{1, 2, \cdots, p^k\} : \operatorname{mcd}(a, p^k) = 1\right\} = \#\left\{a \in \{1, 2, \cdots, p^k\} : \operatorname{mcd}(a, p) = 1\right\}.$$

Así que

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

y por lo tanto

$$\varphi\left(p^k\right) = p^k - \#\left\{a \in \{1, 2, \cdots, p^k\} : \operatorname{mcd}(a, p) \neq 1\right\}. \tag{2.6.2}$$

Ahora, como p *es primo, tenemos que* $\operatorname{mcd}(a, p) \neq 1 \Leftrightarrow p \mid a \Leftrightarrow a = pk$ *para algún* $k \in \mathbb{Z}$. *Por lo tanto* $\left\{a \in \left\{1, \cdots, p^k\right\} : \operatorname{mcd}(a, p) \neq 1\right\} = \left\{a = pk \text{ con } k \in \left\{1, 2, \cdots, p^{k-1}\right\}\right\}$ *y el cardinal de este conjunto es* p^{k-1}. *Por lo tanto, sustituyendo en* (2.6.2) *obtenemos que*

$$\varphi\left(p^k\right) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right). \tag{2.6.3}$$

Veamos ahora la propiedad que nos permitirá obtener una fórmula de la función de Euler para cualquier entero:

Teorema 2.6.3. *Si* $\operatorname{mcd}(m, n) = 1$, $\varphi(mn) = \varphi(m)\varphi(n)$.

Demostración. Como la tesis es obvia si m o n es 1, demostrémoslo para $m, n > 1$. La idea de la demostración es la siguiente: daremos dos conjuntos C y D tales que $\#C = \varphi(mn)$ y $\#D = \varphi(m)\varphi(n)$, y luego construiremos una función biyectiva $f : C \to D$ lo cual terminaría probado que $\#C = \#D$; es decir que $\varphi(mn) = \varphi(m)(n)$.

Sea $C = \{c \in \{0, \cdots, mn-1\} : \operatorname{mcd}(c, mn) = 1\}$; claramente $\#C = \varphi(mn)$. Además, tenemos que

$$\operatorname{mcd}(c, mn) = 1 \Leftrightarrow \operatorname{mcd}(c, m) = 1 \text{ y } \operatorname{mcd}(c, n) = 1. \tag{2.6.4}$$

Así que $C = \{c \in \{0, \cdots, mn\} : \operatorname{mcd}(c, m) = 1 \text{ y } \operatorname{mcd}(c, n) = 1\}$.

Sean $A = \{a \in \{0, \cdots, m-1\} : \operatorname{mcd}(a, m) = 1\}$ y $B = \{b \in \{0, \cdots, n-1\} : \operatorname{mcd}(b, n) = 1\}$; tenemos que $\#A = \varphi(m)$, $\#B = \varphi(n)$ 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 $a \in \{0, \cdots, m-1\}$, $b \in \{0, \cdots, n-1\}$ 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 $c = nq' + b$ tememos (por la Proposición 1.2.6) que

$$\mathrm{mcd}(c, m) = \mathrm{mcd}(a, m) \text{ y } \mathrm{mcd}(c, n) = \mathrm{mcd}(b, n). \tag{2.6.5}$$

Por lo tanto si $\mathrm{mcd}(c, m) = 1$ y $\mathrm{mcd}(c, n) = 1$ tenemos que $\mathrm{mcd}(a, m) = 1$ y $\mathrm{mcd}(b, n) = 1$. Como además claramente $a \in \{0, \cdots, m-1\}$ y $b \in \{0, \cdots, n-1\}$ concluimos que $(a, b) \in D$.

Veamos ahora que la función f es biyectiva. Para ésto 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

$$\begin{cases} c \equiv a \pmod{m} \\ c \equiv b \pmod{n}. \end{cases} \tag{2.6.6}$$

Como $\mathrm{mcd}(m, n) = 1$, por el Teorema Chino del Resto sabemos que el sistema

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

tiene solución x_0 y que además, todas las soluciones son $x \equiv x_0 \pmod{mn}$. Por lo tanto, existe un único $c \in \{0, \cdots, mn-1\}$ que verifica (2.6.6). Resta ver que efectivamente este $c \in C$: como $\mathrm{mcd}(a, m) = 1$, $\mathrm{mcd}(b, n) = 1$ y $c \equiv a \pmod{m}$, $c \equiv b \pmod{n}$, por (2.6.5) tenemos que

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

y por lo tanto $c \in C$.

□

Corolario 2.6.4. *Sea $n \in \mathbb{Z}^+$*

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

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

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

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

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

y utilizando la fórmula (2.6.3) obtenemos lo deseado.

2. Como cada $(p_i^{e_i} - p_1^{e_i - 1}) = p_i^{e_i}\left(1 - \frac{1}{p_i}\right)$ sustituyendo en la fórmula recién obtenida nos queda que

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

□

Ahora sí veamos que el exponente $\varphi(n)$ es el que nos sirve para todas las bases coprimas con n:

Teorema 2.6.5 (Teorema de Euler)**.** *Sean $n, a \in \mathbb{Z}$ tales que $\mathrm{mcd}(a,n) = 1$, entonces*

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

Demostración. Sea $B = \{b \in \{1, \cdots, n\} : \mathrm{mcd}(b,n) = 1\}$; claramente $\#B = \varphi(n)$. Observar que si $b \in B$ en particular $\mathrm{mcd}(b,n) = 1$, y como $\mathrm{mcd}(a,n) = 1$ tenemos que también $\mathrm{mcd}(ab,n) = 1$. Por lo tanto, (tomando el resto de dividir ab entre n), existe un único $b' \in B$ tal que $ab \equiv b' \pmod{n}$. Además, dados dos elementos distintos de B, b_1 y b_2, al multiplicarlos por a obtenemos enteros no congruentes módulo n, ya que si $ab_1 \equiv ab_2 \pmod{n}$, al ser $\mathrm{mcd}(a,n) = 1$ podemos cancelar a y obtendríamos $b_1 \equiv b_2 \pmod{n}$, lo cual es absurdo ya que en B no hay dos elementos congruentes módulo 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,

$$\prod_{b\in B} ab \equiv \prod_{b'\in B} b' \pmod{n} \Rightarrow \prod_{b\in B} ab \equiv \prod_{b\in B} b \pmod{n}.$$

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

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

y como cada $b \in B$ es coprimo con n, lo podemos cancelar de la congruencia y obtenemos:

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

□

Ahora si p es primo, ya vimos que $\varphi(p) = p - 1$, así que obtenemos el siguiente corolario:

Corolario 2.6.6 (Teorema de Fermat)**.** *Si p es primo y $a \in \mathbb{Z}$ es tal que $p \nmid a$, entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Corolario 2.6.7. *Sean a, n dos enteros coprimos.*

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

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

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

2. Es claro a partir de lo anterior.

□

Observar que el recíproco del corolario anterior no vale. Sean $n = 10$ y $a = 9 \equiv -1 \pmod{n}$, con $\varphi(n) = 4$. Se cumple que $9^1 \equiv 9^3 \pmod{n}$, pero $1 \not\equiv 3 \pmod{4}$.

Ejemplos 2.6.8. *En estos ejemplos utilizaremos que $\varphi(100) = 100\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{5}\right) = 40$ y que $\mathrm{mcd}(3,100) = 1$ para usar el Teorema de Euler.*

1. *Si queremos calcular el resto de dividir* 3^{85} *entre* 100*, tenemos que encontrar* $r \in \{0, 1, \cdots, 99\}$ *tal que* $r \equiv 3^{85} \pmod{100}$*. Ahora como* $\varphi(100) = 40$ *y* $85 \equiv 5 \pmod{40}$ *tenemos que* $3^{85} \equiv 3^5 \pmod{100}$ *y por lo tanto* $r \equiv 3^5 \pmod{100}$*. Así que* $r \equiv 243 \pmod{100}$*, por lo que* $r = 43$*.*

2. *Si queremos calcular el resto de dividir* 3^{78} *entre* 100*, tenemos que encontrar* $r \in \{0, 1 \cdots, 99\}$ *tal que* $r \equiv 3^{78} \pmod{100}$*. Si multiplicamos por* 3^2 *a ambos lados obtenemos que* $3^2 r \equiv 3^{80} \pmod{100}$*. Como* $\mcd(3, 100) = 1$ *y* $\varphi(100) = 40$ *obtenemos que* $9r \equiv 1 \pmod{100}$*. Así que tenemos que hallar el inverso de* 9 *módulo* 100*. Para ésto tenemos que resolver la ecuación diofántica* $9r - 100y = 1$*, que claramente tiene solución* $(r_0, y_0) = (-11, -1)$ *por lo que* $r \equiv -11 \pmod{100}$*. Entonces* $r = 89$*.*

3. *Observar que en el ejemplo anterior podríamos haber empezado con* $78 \equiv 38 \pmod{40}$*, por lo que* $3^{78} \equiv 3^{38} \pmod{100}$*. Una opción era calcular* $3^{38} \pmod{100}$ *directamente (calculando las potencias de* 3 *y reduciendo módulo* 100 *en cada paso). Otro camino era empezar con* $78 \equiv -2 \pmod{40}$ *por lo que* $3^{78} \equiv 3^{-2} \pmod{100}$*. Si bien hasta este momento no habíamos mencionado las potencias negativas módulo* n *(lo haremos con más detalle cuando hablemos de grupos), cuando escribimos* $a^{-m} \pmod{n}$ *nos referimos al inverso de* a^m *módulo* n*. Es decir, que con este razonamiento, nuevamente llegamos a que* r *es el inverso de* 3^2 *módulo* 100*.*

Nos quedaría ver cómo calcular potencias grandes módulo n *cuando la base no es coprima con el módulo, lo que no nos permite usar el Teorema de Euler. Mostramos una técnica con un ejemplo: si queremos calcular el resto de dividir* $306^{127} \pmod{100}$*. Lo primero que observamos es que como* $306 \equiv 6 \pmod{100}$ *entonces* $306^{127} \equiv 6^{127} \pmod{100}$*.* **Siempre conviene reducir la base primero antes de seguir operando, para operar con números más chicos.**

Ahora bien, buscamos $r \in \{0, \cdots, 99\}$ *tal que* $r \equiv 6^{127} \pmod{100}$*. Aquí claramente no podemos utilizar el Teorema de Euler.*

Pero (por lo observado luego del Teorema Chino del Resto) tenemos que

$$r \equiv 6^{127} \pmod{100} \Leftrightarrow \begin{cases} r \equiv 6^{127} \pmod{25} \\ r \equiv 6^{127} \pmod{4}. \end{cases} \tag{2.6.7}$$

Ahora procedemos a simplicar cada una de estas congruencias: para la primera, ahora sí podemos utilizar el Teorema de Euler ya que $\mcd(6, 25) = 1$*. Como* $\varphi(25) = 25 - 5 = 20$ *obtenemos que* $6^{127} \equiv 6^7 \pmod{25}$*. Tenemos que* $6^2 = 36 \equiv 11 \pmod{25}$*, así que* $6^4 \equiv 11^2 \pmod{25}$ *y como* $121 \equiv 21 \pmod{25} \equiv (-4) \pmod{25}$ *tenemos que* $6^7 = 6^4 6^2 6 \equiv (-4)11(6) \pmod{25} \equiv -44(6) \pmod{25} \equiv 6(6) \pmod{25} \equiv 11 \pmod{25}$*. Por lo que la primer congruencia del sistema* (2.6.7) *la podemos escribir como* $r \equiv 11 \pmod{25}$*. Otro consejo, como hicimos recién:* **a medida que se opera siempre conviene reducir los resultados módulo** n **para operar con números más chicos.** *Ahora para la segunda congruencia no podemos utilizar el Teorema de Euler, pero:* $6^{127} = 6^2 6^{125} = (36)6^{125} \equiv 0 \pmod{4}$*. Así que buscamos* $r \in \{0, \cdots, 99\}$ *tal que*

$$\begin{cases} r \equiv 11 \pmod{25} \\ r \equiv 0 \pmod{4}. \end{cases}$$

Resolviendo este sistema obtenemos $r \equiv 36 \pmod{100}$ *por lo que* $r = 36$*.*

2.7. Método de exponenciación rápida

Supongamos ahora que queremos calcular

$$5^{49} \pmod{101}.$$

Como $5 < 101$ y $49 < \varphi(101) = 100$, no podemos aplicar lo estudiado en las secciones anteriores. Lo primero que podemos hacer para calcular dicha potencia es multiplicar 5 con 5 y reducir módulo 101, al resultado multiplicarlo por 5 y reducirlo, y hacer esto mismo 46 veces más. Este método tiene un costo de 48 multiplicaciones y reducciones módulo 101. En general, si queremos calcular

$$b^e \pmod{m}, \text{ con } 0 \leq b < m,\ 0 \leq e < \varphi(m),$$

utilizando el método anterior, tendrá un costo de $e - 1$ multiplicaciones y reducciones módulo b.

Podemos mejorar mucho el costo del método anterior. Veámoslo primero aplicado en el primer ejemplo que vimos. Si escribimos $49 = 2^5 + 2^4 + 2^0$, entonces

$$5^{49} \equiv 5^{2^5} 5^{2^4} 5^{2^0}.$$

Por lo que solo necesitamos calcular las potencias $5^{2^i} \pmod{101}$ para $i = 0, 1, \ldots, 5$. Observando que $5^{2^{i+1}} = \left(5^{2^i}\right)^2$, podemos generar la siguiente tabla

n	$5^{2^n} \pmod{101}$
0	5
1	25
2	$625 \equiv 19$
3	$361 \equiv -43$
4	$1849 \equiv 31$
5	$961 \equiv 52,$

y obtener que $5^{49} \equiv 52 \times 31 \times 5 \pmod{101} \equiv 81 \pmod{101}$. En total hicimos 7 productos y 5 reducciones. Este método es llamado el **método de exponenciación rápida**. Veamos cómo funciona en general. Si $e = 2^l + a_{l-1}2^{l-1} + \cdots + a_1 2 + a_0$, con $a_i \in \{0, 1\}$ entonces

$$b^e \equiv b^{2^l} \left(b^{2^{l-1}}\right)^{a_{l-1}} \cdots \left(b^{2^1}\right)^{a_1} \left(b^{2^0}\right)^{a_0} \pmod{m}.$$

De igual manera se puede generar la tabla, para poder computar el producto anterior,

n	$b^{2^n} \pmod{m}$
0	$b \pmod{m}$
1	$b^2 \pmod{m}$
2	$\left(b^2\right)^2 \pmod{m}$
$\vdots$	$\vdots$
l	$\left(b^{2^{l-1}}\right)^2 \pmod{m},$

El costo del método anterior en el peor caso sería de $l = \log_2(e)$ productos y l reducciones, decimos entonces que el método de exponenciación rápida es de orden lineal en la entrada.

Capítulo 3

Grupos

En esta sección generalizaremos algunas de las nociones vistas en la sección anterior, y hablaremos de grupos en general: conjuntos con una operación asociativa, con neutro e inverso para cada elemento. Formalicemos esta idea.

3.1. Definición, primeros ejemplos y propiedades.

Definición 3.1.1. Un *grupo* es un conjunto G con una operación binaria $* : G \times G \to G$ tal que

- (asociativa) $x * (y * z) = (x * y) * z$ para todo $x, y, z \in G$,
- (neutro) existe un elemento $e \in G$ tal que $e * x = x$ y $x * e = x$ para todo $x \in G$,
- (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 $(G, *, e)$. Cuando la operación y neutro son claros escribimos simplemente G.

Ejemplos 3.1.2.

1. $(\mathbb{Z}, +)$ *es un grupo (donde* $+$ *es la suma usual de enteros), con neutro* 0*, y donde el inverso de cada elemento* z *es* $-z$ *(el opuesto de* z*).*
2. $(\mathbb{Z}, \times)$ *no es un grupo. Si bien el producto de enteros es asociativo y tiene neutro* 1*, no todo elemento tiene inverso, por ejemplo, no existe* $z \in \mathbb{Z}$ *tal que* $0 \times z = 1$*; y tampoco existe tal que* $2 \times z = 1$*.*
3. *El conjunto* $G = \{-1, 1\}$ *con la multiplicación de enteros es un grupo.*
4. $(\mathbb{R}, +)$ *es un grupo.*
5. $(\mathbb{R}, \times)$ *no es un grupo (la multiplicación de reales es asociativa y tiene neutro* 1*, pero el elemento* 0 *no tiene inverso).*
6. *Si llamamos* $\mathbb{R}^* = \mathbb{R} - \{0\}$*, entonces* $(\mathbb{R}^*, \times)$ *es un grupo.*
7. $(M_{n\times n}(\mathbb{R}), +)$ *es un grupo.*
8. $(M_{n\times n}(\mathbb{R}), \times)$ ***NO** es un grupo. Si bien la multiplicación de matrices es asociativa y tiene neutro* I_n *(la matriz identidad), hay muchas matrices que no tienen inverso; por ejemplo,* $\nexists N \in M_{n\times n}$ *tal que* $0 \times N = I_n$*.*
9. *Quedémonos entonces con las matrices que tienen inverso: si llamamos* $GL_n(\mathbb{R}) = \{M \in M_{n\times n}(\mathbb{R}) : det(M) \neq 0\}$ *entonces* $(GL_n(\mathbb{R}), \times)$ *es un grupo.*

Un grupo puede tener una cantidad finita de elementos (como en el ejemplo (3)) o una cantidad infinita de elementos (como en los ejemplos (1), (4), (6), (7) y (9)). A la cantidad de elementos del grupo lo llamamos **orden de** G y lo escribimos $|G|$. La operación del grupo puede ser conmutativa (como en el ejemplo (1)) o no (como en el ejemplo (9)). En el caso en que la operación sea conmutativa decimos que el **grupo es abeliano**. Generalmente, cuando no genera confusión, se acostumbra escribir simplemente gh en vez de $g * h$.

Proposición 3.1.3. *Sea $(G, *)$ un grupo y $g, h \in G$. Entonces:*

1. *El neutro de G es único.*
2. *Para todo $g \in G$, 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 $g' = g^{-1}$.*

Demostración. 1. Supogamos que e y e' son neutros de G. Entonces $e * e' = e'$ (pues e es neutro). Pero también, como e' es neutro tenemos que $e * e' = e$ y por lo tanto $e = e * e' = e'$.

(8) Si $gx = h$, multiplicando ambos lados a la izquierda por g^{-1} obtenemos $g^{-1}(gx) = g^{-1}h$. Luego, por la propiedad asociativa tenemos que $(g^{-1}g)x = g^{-1}h$ y entonces $ex = g^{-1}h$ y por la propiedad del neutro finalmente obtenemos que $x = g^{-1}h$ y por lo tanto existe solución y es única.
Dejamos el resto de ejercicio.

□

A continuación veremos varias familias de ejemplos de grupos finitos.

3.2. Grupos de Permutaciones

Para cada $n \in \mathbb{Z}^+$ llamamos

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

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

Si componemos dos funciones biyectivas, el resultado vuelve a ser una función biyectiva. Sabemos que la composición de funciones es asociativa y además Id, la función identidad, es biyectiva y es neutro de la composición. Además, si f es biyectiva, entonces f tiene una función inversa f^{-1} que también es biyectiva. Tenemos entonces el siguiente resultado:

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 una segunda fila escribiremos $f(1)$, $f(2), \cdots, f(n)$.

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

Observar que en este caso $\tau \circ \tau = \mathrm{Id}$ y por lo tanto τ es inverso de sí mismo.

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

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

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.

La segunda fila de estas matrices es entonces (por ser las funciones biyectivas) una permutación de los números del 1 al n. Por lo tanto cada elemento de S_n se puede pensar como una permutación de $1, 2, \cdots, n$. Es por esto que a S_n se lo llama el **grupo de permutaciones** (de n elementos). En particular tenemos que $|S_n| = n!$

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 forma: se colocan los elementos de G arriba de la tabla, y en el mismo orden se los colocan 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 $g * h$.

Por ejemplo, la tabla de Cayley de S_2 es:

$\circ$	Id	τ
Id	Id	τ
τ	τ	Id

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	σ_2	Id			
τ_3	τ_3			Id		
σ_1	σ_1				σ_2	Id
σ_2	σ_2				Id	σ_1

.

Dejamos como ejercicio completar la tabla de S_3. Para esto recomendamos (además de calcular algunos productos más) utilizar la siguiente propiedad de las tablas de Cayley: son como un juego Sudoku.

Proposición 3.3.1. *En la tabla de Cayley de un grupo, cada elemento de G aparece exactamente una vez en cada fila y en cada columna. Es decir, que cada columna y cada fila de la tabla es una permutación 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 sólo 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 y aparece una sola vez (en la columna de x). De forma análoga se prueba que cada elemento aparece una sola vez en cada columna. □

Observar que un grupo finito G es abeliano si y sólo si su tabla es simétrica (en el sentido de matriz simétrica).

Dejamos planteado el ejercicio de hallar las tablas de Cayley de cualquier grupo con 2 elementos y de cualquier grupo con 3 elementos.

3.4. El grupo de enteros módulo n

La idea del siguiente grupo es ver que al sumar dos enteros entre 0 y $n-1$ y quedarnos con el resto de dividir la suma entre n, entonces con esta operación obtenemos un grupo. Si bien esta es la idea principal, usaremos las **clases de congruencia** para facilitarnos las cosas.

Recordamos que la congruencia módulo n es una relación de equivalencia. Por lo tanto para cada $z \in \mathbb{Z}$ tenemos la **clase de** z, que escribiremos como $[z]$, o $[z]_n$ o simplemente como $\bar{z}$:

$$\bar{z} = \{x \in \mathbb{Z} : x \equiv z \pmod{n}\}.$$

Tenemos entonces que (por la propiedad transitiva de la congruencia)

$$x \equiv z \pmod{n} \text{ si y sólo si } \bar{x} = \bar{z}.$$

Por lo tanto, si r es el resto de dividir z entre n tenemos que $\bar{z} = \bar{r}$.

Por ejemplo, si $n = 2$ tenemos que $\bar{0} = \{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\} = \{2k : k \in \mathbb{Z}\} = \bar{2} = \overline{-10}$. Y $\bar{1} = \{\cdots -5, -3, -1, 1, 3, 5, \cdots\} = \{2k+1 : k \in \mathbb{Z}\} = \bar{3} = \overline{-11}$.

Llamaremos $\mathbb{Z}_n$ al conjunto de clases de equivalencia módulo n. Por ejemplo $\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$ y $\mathbb{Z}_3 = \{\bar{0}, \bar{1}, \bar{2}\}$. Es claro que $\mathbb{Z}_n$ tiene n elementos (una clase por cada resto posible de dividir entre n); es decir $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \cdots, \overline{n-1}\}$.

Queremos definir en $\mathbb{Z}_n$ una operación que le dé estructura de grupo. Quisiéramos definir una operación (que llamaremos *suma* y la escribiremos como $+$) de la forma más natural:

$$\bar{a} + \bar{b} := \overline{a+b}.$$

Por ejemplo, en $\mathbb{Z}_5$ tendríamos que $\bar{3} + \bar{4} = \overline{3+4} = \bar{7} = \bar{2}$.

Esta forma de hacerlo podría tener un problema: al utilizar el entero 3 para describir al conjunto $\bar{3}$ estamos eligiendo un representante del conjunto. Tenemos que ver que si cambiamos los representantes de las clases, entonces el resultado de la operación no cambia. Por ejemplo, en $\mathbb{Z}_5$ tenemos que $A = \bar{3} = \bar{8}$ y $B = \bar{4} = \bar{9}$, al definir $A+B$ debe ser independiente de si utilizamos el 3 o el 8 (o cualquier otro elemento de A) para representar a A, y de si elegimos el 4 o el 9 para representar a B. Claramente en este caso como $\overline{8+9} = \overline{17} = \bar{2}$, el resultado efectivamente nos da igual.

Veamos que ésto pasa en general: para un n cualquiera, en $\mathbb{Z}_n$, si $A = \bar{a} = \overline{a'}$ y $B = \bar{b} = \overline{b'}$ entonces $\overline{a+b} = \overline{a'+b'}$. Esto es claro por la primer parte de la Proposición 2.3.1: Si $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n} \Rightarrow a + b \equiv a' + b' \pmod{n}$. Por lo tanto la definición de la suma de clases es independiente de los elementos que elegimos como representantes.

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 $\left(\bar{a} + \bar{b}\right) + \bar{c} \overset{\text{def}}{=} \overline{(a+b)} + \bar{c} \overset{\text{def}}{=} \overline{(a+b)+c}$. Ahora como la suma de enteros es asociativa, tenemos que $\overline{(a+b)+c} = \overline{a+(b+c)} \overset{\text{def}}{=} \bar{a} + \overline{b+c} \overset{\text{def}}{=} \bar{a} + \left(\bar{b} + \bar{c}\right)$. Claramente $\bar{0}$ es neutro de esta operación, y un elemento $\bar{a}$ tiene como opuesto a $\overline{-a} = \overline{n-a}$. Además como la suma de enteros es conmutativa, esta suma de clases también lo es. □

Veamos cómo nos queda la tabla para $\left(\mathbb{Z}_4, +, \bar{0}\right)$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

Proposición 3.4.2. *Dados dos grupos* $(G, \star, e_G)$, $(K, *, e_K)$ *si consideramos el conjunto* $G \times K = \{(g,k) : g \in G, k \in K\}$ *con la operación coordenada a coordenada:* $(g,k)(g',k') = (g \star g', k * k')$, *entonces obtenemos un nuevo grupo (llamado el* **producto directo** *de* G *y* K*).*

Demostración. Dejamos los detalles de ejercicio, pero claramente la nueva operación es asociativa pues las operaciones en cada coordenada lo son. Esta operación tiene neutro $e = (e_G, e_K)$ y el inverso está dado por $(g,k)^{-1} = (g^{-1}, k^{-1})$. □

Veamos entonces como queda la tabla de Cayley de $\mathbb{Z}_2 \times \mathbb{Z}_2$ (donde en cada coordenada usamos la suma de clases):

$(+,+)$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{0},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$
$(\overline{1},\overline{0})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$
$(\overline{0},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{0})$	$(\overline{1},\overline{0})$
$(\overline{1},\overline{1})$	$(\overline{1},\overline{1})$	$(\overline{0},\overline{1})$	$(\overline{1},\overline{0})$	$(\overline{0},\overline{0})$.

Obtenemos entonces otro grupo abeliano con 4 elementos, pero diferente a $\mathbb{Z}_4$. Por ejemplo, en $\mathbb{Z}_2 \times \mathbb{Z}_2$ todo elemento x cumple que $x + x = e$, mientras que esto no es cierto en $\mathbb{Z}_4$ (por ejemplo $\overline{1} + \overline{1} \neq \overline{0}$). Más adelante formalizaremos el concepto de "diferentes"(no isomorfos) y será un ejercicio ver que estos dos ejemplos son básicamente los únicos grupos con 4 elementos.

3.5. El grupo de los invertibles módulo n

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

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

Nuevamente resulta que esta definición es independendiente de la elección de los elementos en cada clase. Es decir, si $A = \overline{a} = \overline{a'}$ y $B = \overline{b} = \overline{b'}$ entonces $\overline{ab} = \overline{a'b'}$. Esto es claro por la primer parte de la Proposición 2.3.1: Si $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n} \Rightarrow ab \equiv a'b' \pmod{n}$. Este producto de clases es asociativo y claramente tiene neutro $\overline{1}$. Pero $\mathbb{Z}_n$ **no es un grupo** con este producto pues existen elementos que no tienen inversos: por ejemplo $\overline{0}$ no tiene inverso ya que $\overline{0}\overline{a} = \overline{0} \neq \overline{1}$ para todo $\overline{a} \in \mathbb{Z}_n$.

Pero puede haber más elementos que no tienen inversos: un elemento de $\overline{a} \in \mathbb{Z}_n$ tiene inverso con el producto, si y sólo si existe $\overline{x}$ tal que $\overline{a} \times \overline{x} = \overline{1}$; si y sólo si $\overline{ax} = \overline{1}$. Es decir que $\overline{a}$ tiene inverso, si y sólo si existe $x \in \mathbb{Z}$ tal que $ax \equiv 1 \pmod{n}$. Y ya vimos (en el Corolario 2.4.5) que ésto sucede si y sólo si $\mathrm{mcd}(a,n) = 1$. Quedémonos entonces con estos elementos; llamamos

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

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

Por todo lo observado antes, es claro que:

Proposición 3.5.1. $(U(n), \times, \overline{1})$ *es un grupo abeliano con* $\varphi(n)$ *elementos.*

Por ejemplo la tabla de Cayley de $U(8)$ es:

$\times$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

3.6. Grupos Dihedrales

En esta sección definiremos para cada $n \in \mathbb{N}$, $n \geq 3$, un subconjunto de los movimientos del plano, y veremos que con la composición de funciones, cada uno de estos subconjuntos es un grupo.

Comencemos con $n = 3$. Consideremos, en el plano, un triángulo equilátero T (el $n = 3$ es la cantidad de lados). Sea $D_3 = \{f : \mathbb{R}^2 \to \mathbb{R}^2 : f \text{ es un movimiento del plano y } f(T) = T\}$. Es decir, D_3 es el conjunto de movimientos del plano que dejan fijo el triángulo. Entonces en D_3 tenemos al movimiento identidad, id; también tenemos las simetrías axiales s_1, s_2 y s_3 con ejes las mediatrices de los lados de T, y además tenemos las rotaciones antihorarias r_1 y r_2 con centro el centro del triángulo y ángulos 120 y 240 grados respectivamente, ver Figura 3.1.

Entonces

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

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

Proposición 3.6.1. $(D_3, \circ, \mathrm{id})$ *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 $(\mathrm{id})^{-1} = \mathrm{id}$.
- Para todo $i = 1, 2, 3$, tenemos que $s_i \circ s_i = \mathrm{id}$ y por lo tanto cada simetría es inversa de sí misma.
- Tenemos que $r_1 \circ r_2 = \mathrm{id}$ y por lo tanto $(r_1)^{-1} = r_2$ y $(r_2)^{-1} = r_1$.

□

Observar que $s_1 \circ r_1 = s_2$ y $r_1 \circ s_1 = s_3$ y por lo tanto D_3 **no es abeliano.**
Tenemos también que $r_2 = r_1^2$ y $s_1 \circ r_1^2 = s_3 = r_1 \circ s_1$, por lo tanto

$$D_3 = \{\mathrm{id}, r_1, r_1^2, s_1, s_1 r_1, s_1 r_1^2\}.$$

Es decir que todo elemento de D_3 es de la forma $s_1^i r_1^j$ con $i \in \{0, 1\}$ y $j \in \{0, 1, 2\}$.

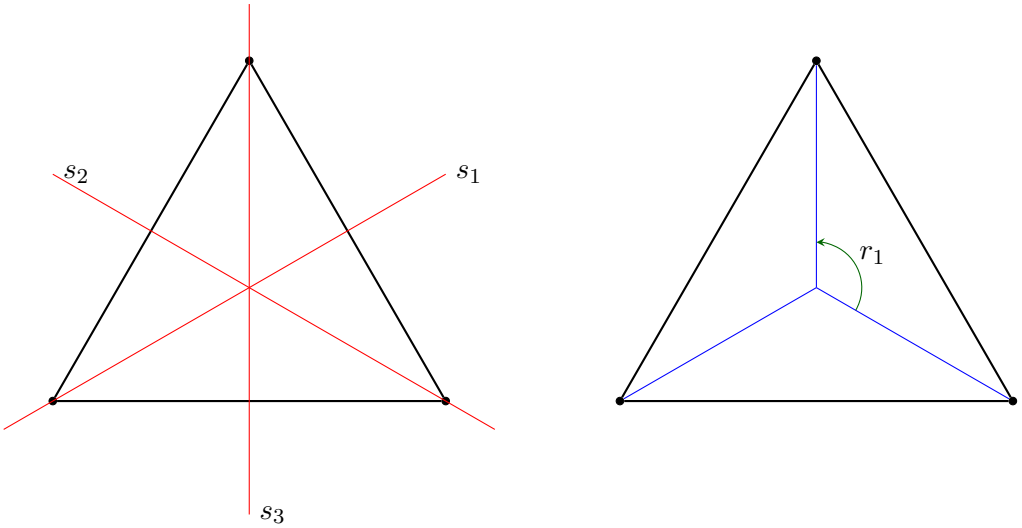

Figura 3.1: Simetrías y rotaciones de D_3.

Observaciones 3.6.2. *Por simplicidad llamaremos $s = s_1$ y $r = r_1$. Tenemos las siguientes propiedades:*

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

Dejamos como ejercicio completar la Tabla de Cayley de D_3:

$\circ$	id	s	sr	sr^2	r	r^2
id	id	s	sr	sr^2	r	r^2
s	s	id	r	r^2	sr	sr^2
sr	sr		id			
sr^2	sr^2			id		
r	r				r^2	id
r^2	r^2				id	r

.

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 y s_4 y tres rotaciones antihorarias r_1, r_2 y r_3 con centro en el centro del cuadrado y ángulos 90, 180 y 270 grados, ver Figura 3.2. Así que tenemos que

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

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 $r_3 = r_1^3$.

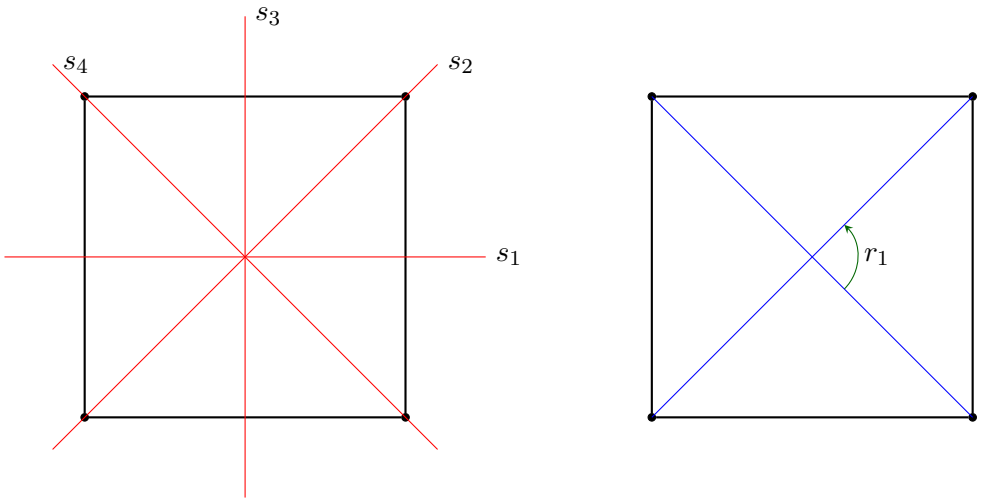

Figura 3.2: Simetrías y rotaciones de D_4.

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

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

En general, para cualquier $n \geq 3$, si P_n es un polígono regular con n lados se define $D_n = \{f : \mathbb{R}^2 \to \mathbb{R}^2 : f$ es un movimiento del plano y $f(P_n) = P_n\}$. En D_n está el movimiento identidad, id, n simetrías axiales y $n-1$ rotaciones antihorarias. Por la tanto D_n tiene $2n$ elementos. De forma análoga a lo hecho antes se prueba que:

Proposición 3.6.3. $(D_n, \circ, \mathrm{id})$ *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 ángulo $\frac{360}{n}$ grados, tenemos que

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

Observar que $|D_3| = 6 = 3! = |S_3|$. Existe una clara correspondendia biyectiva entre los elementos de D_3 y los de S_3: si numeramos los vértices del triángulo con los números del 1 al 3, entonces a cada elemento de D_3 le hacemos corresponder la permutación que realiza en sus vértices. Por ejemplo, si la numeración la hacemos en orden antihorario, entonces la permutación $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ corresponde a la rotación r_1. Por otro lado cada permutación de S_3 determina un único movimiento de D_3 y por lo tanto la correspondencia es biyectiva. Esto no pasa en los otros grupos dihedrales, ya que $|D_n| = 2n \neq n! = |S_n|$ si $n \geq 4$. Si bien a cada movimiento le podemos asociar una permutación, esta correspondencia no es biyectiva. Por ejemplo, para $n = 4$, si numeramos los vértices del cuadrado de forma ordenada en sentido antihorario, no existe ningún movimiento de D_4 que realice la permutación $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$.

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).
Veamos algunos ejemplos:

Ejemplos 3.7.2. *1. Todo grupo $(G, *, e)$ tiene dos subgrupos que llamamos* triviales*; estos son $H = \{e\}$ y $H = G$.*

2. Si consideramos el grupo $(\mathbb{Z}, +, 0)$ y tomamos $H = 2\mathbb{Z} = \{2z : z \in \mathbb{Z}\}$, entonces, como la suma de enteros pares es par, el 0 es par y el opuesto de un par también es par, resulta que $2\mathbb{Z}$ es subgrupo de $\mathbb{Z}$ ($2\mathbb{Z} < \mathbb{Z}$).

3. De forma análoga, si para cualquier $n \in \mathbb{Z}$ consideramos $H = n\mathbb{Z} = \{nz : z \in \mathbb{Z}\}$ entonces $n\mathbb{Z} < \mathbb{Z}$. Dejamos como ejercicio probar que para cualquier subgrupo H de $\mathbb{Z}$, existe un $n \in \mathbb{Z}$ tal que $H = n\mathbb{Z}$ (sugerencia: considerar n como el menor entero positivo en H).

4. El conjunto de los enteros impares no es un subgrupo de $\mathbb{Z}$ pues no contiene al 0.

5. Si consideramos el grupo $(\mathbb{R}^*, \times)$ tenemos que $H = \{-1, 1\} < \mathbb{R}^*$ y también que $H = \{2^n : n \in \mathbb{Z}\} < \mathbb{R}^*$.

6. Para el grupo $(M_{n\times n}(\mathbb{R}), +)$ el conjunto $H = \{M \in M_{n\times n}(\mathbb{R}) : M$ es simétrica$\}$ es un subgrupo.

7. Los conjuntos $H_1 = \{\mathrm{Id}, \tau_1\}$ y $H_2 = \{\mathrm{Id}, \sigma_1, \sigma_2\}$ son subgrupos de S_3.

8. El conjunto $H = \{\overline{1}, \overline{3}\}$ es un subgrupo de $U(8)$ (observar que como $\overline{3} \times \overline{3} = \overline{1}$ se tiene que H es cerrado por la operación y por inversos, pues $\overline{3}$ es inverso de sí mismo.)

9. En D_3 tenemos que $H = \{\mathrm{id}, s\}$ y $H_2 = \{\mathrm{id}, r, r^2\}$ son subgrupos de D_3.

Ahora nos concentraremos en las potencias de un elemento dado.

Definición 3.7.3. Si $(G, *, e)$ es un grupo definimos las potencias de g como $g^0 = e$ y si $n \in \mathbb{Z}^+$

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

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

Las siguientes propiedades son fáciles de probar y quedan como ejercicio:

Proposición 3.7.4. *Para todo $g \in G$ y $m, n \in \mathbb{Z}$ valen:*

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

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 $e \in \langle g \rangle$; además 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.) Veamos algunos ejemplos.

Ejemplos 3.7.5. *1. Si e es el neutro del grupo, es claro que $\langle e\rangle = \{e\}$.*

2. *En $(\mathbb{Z},+)$ tenemos que $\langle 1\rangle = \mathbb{Z}$ y por lo tanto $\mathbb{Z}$ es cíclico. Además tenemos que $\langle 2\rangle = \langle -2\rangle = 2\mathbb{Z}$ y en general, $\langle n\rangle = n\mathbb{Z}$.*
3. *En $(\mathbb{R}^*,\times)$ tenemos que $\langle 1\rangle = \{1\}$, $\langle -1\rangle = \{-1,1\}$ y $\langle 2\rangle = \left\{1, 2^n, \frac{1}{2^m} : m,n \in \mathbb{Z}^+\right\}$. Es claro que $\mathbb{R}^*$ no es cíclico.*
4. *$(\mathbb{Z}_n,+)$ es cíclico pues $\mathbb{Z}_n = \langle \overline{1}\rangle$.*
5. *En $(\mathbb{Z}_6,+)$, $\langle \overline{2}\rangle = \{\overline{0},\overline{2},\overline{4}\} = \langle \overline{4}\rangle$, $\langle \overline{3}\rangle = \{\overline{0},\overline{3}\}$ y $\langle \overline{1}\rangle = \mathbb{Z}_6 = \langle \overline{5}\rangle$.*
6. *En $U(8)$ tenemos que $\langle \overline{1}\rangle = \{\overline{1}\}$, $\langle \overline{3}\rangle = \{\overline{1},\overline{3}\}$, $\langle \overline{5}\rangle = \{\overline{1},\overline{5}\}$ y $\langle \overline{7}\rangle = \{\overline{1},\overline{7}\}$. Por lo tanto $U(8)$ NO es cíclico.*
7. *En $U(7)$ tenemos que $\langle \overline{1}\rangle = \{\overline{1}\}$, $\langle \overline{2}\rangle = \{\overline{1},\overline{2},\overline{4}\} = \{\overline{4}\}$, $\langle \overline{3}\rangle = \{\overline{1},\overline{3},\overline{2},\overline{6},\overline{4},\overline{5}\} = \mathbb{Z}_7 = \langle \overline{5}\rangle$ y $\langle \overline{6}\rangle = \{\overline{1},\overline{6}\}$. Por lo tanto $U(7)$ es cíclico y tanto $\overline{3}$ como $\overline{5}$ lo generan.*

En los ejemplos anteriores vemos que si $g^n = e$ para algún n, entonces el subgrupo $\langle g\rangle$ es finito. En breve veremos cuántos elementos tiene este subgrupo exactamente. Antes necesitamos la siguiente definición.

Definición 3.7.6. Sea $(G,*,e)$ un grupo y $g \in G$. Definimos el **orden** del elemento g (y lo escribiremos $\mathrm{o}(g)$) de la siguiente manera:

- si $g^n \neq e$ para todo $n \in \mathbb{Z}^+$, decimos que $\mathrm{o}(g) = \infty$;
- en caso contrario, definimos $\mathrm{o}(g) = \min\{n \in \mathbb{Z}^+ : g^n = e\}$.

Veamos primero algunos ejemplos basados en los cálculos de los Ejemplos 3.7.5.

Ejemplos 3.7.7. *1. En cualquier grupo, si e es el neutro del grupo, es claro que $\mathrm{o}(e) = 1$.*

2. *En $(\mathbb{Z},+)$ tenemos que $\mathrm{o}(0) = 1$ y $\mathrm{o}(z) = \infty$ para todo $z \neq 0$.*
3. *En $(\mathbb{R}^*,\times)$ tenemos que $\mathrm{o}(1) = 1$, $\mathrm{o}(-1) = 2$ y $\mathrm{o}(r) = \infty$ para todo $r \neq \pm 1$.*
4. *En $(\mathbb{Z}_6,+)$, $\mathrm{o}(\overline{0}) = 1$, $\mathrm{o}(\overline{1}) = 6 = \mathrm{o}(\overline{5})$, $\mathrm{o}(\overline{2}) = 3 = \mathrm{o}(\overline{4})$ y $\mathrm{o}(\overline{3}) = 2$.*
5. *En $(U(8),\times)$ tenemos que si $\overline{a} \neq \overline{1}$, $\mathrm{o}(\overline{a}) = 2$.*
6. *En $(U(7),\times)$ tenemos que $\mathrm{o}(\overline{2}) = 3 = \mathrm{o}(\overline{4})$, $\mathrm{o}(\overline{3}) = 6 = \mathrm{o}(\overline{5})$ y $\mathrm{o}(\overline{6}) = 2$.*
7. *En $D(n)$, para una simetría s_i se tiene que $\mathrm{o}(s_i) = 2$ para todo $i = 1,\cdots,n$. Y para las rotaciones r_j tenemos que $\mathrm{o}(r_j) = n$, para todo $j = 1,\cdots,n-1$.*

Tenemos las siguientes propiedades.

Proposición 3.7.8. *Si $(G,*,e)$ es un grupo y $g \in G$ entonces:*

1. *Si $n \in \mathbb{Z}^+$, tenemos que*
$$\mathrm{o}(g) = n \Leftrightarrow \begin{cases} g^n = e \text{ y} \\ \text{si } g^m = e \Rightarrow n \mid m. \end{cases} \tag{3.7.1}$$
2. *Si $n \in \mathbb{Z}^+$ entonces $\mathrm{o}(g) = n$ si y sólo si* $\begin{cases} g^n = e \text{ y} \\ g^d \neq e \ \forall\ d \mid n,\ d \neq n,\ d > 0. \end{cases}$

3. *Si* $n \in \mathbb{Z}^+$ *entonces* $\mathrm{o}(g) = n$ *si y sólo si* $\begin{cases} g^n = e \text{ y} \\ g^{\frac{n}{p}} \neq e \ \forall\ p \mid n,\ p \neq n,\ p \text{ primo.} \end{cases}$

4. *Se tiene que* $g^m = e \Leftrightarrow \mathrm{o}(g) \mid m$.

5. *Si* $\mathrm{o}(g)$ *es finito, entonces* $g^m = g^k$ *si y sólo si* $m \equiv k \pmod{\mathrm{o}(g)}$.

6. *Si* $\mathrm{o}(g) = \infty$ *y* $m \neq k$ *entonces* $g^m \neq g^k$.

7. *Si* $\mathrm{o}(g)$ *es finito y* $k \in \mathbb{Z}$, *entonces* $\mathrm{o}\left(g^k\right) = \dfrac{\mathrm{o}(g)}{\mathrm{mcd}(k, \mathrm{o}(g))}$.

8. *Si* $\mathrm{o}(g)$ *es finito y* $k \in \mathbb{Z}$, *entonces* $\mathrm{o}(g) = \mathrm{o}\left(g^k\right)$ *si y sólo si* $\mathrm{mcd}(k, \mathrm{o}(g)) = 1$.

Demostración. 1. Veamos primero el directo: si $n = \mathrm{o}(g)$, por definición tenenos que $g^n = e$. Además, 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 (exponente) positiva de g con la que se obtiene e, y $0 \leq r < n$ concluimos que debe ser $r = 0$ y por lo tanto $n \mid m$.

   Para el recíproco es evidente que si $n \in \mathbb{Z}^+$, $g^n = e$ y si cada vez que $g^m = e$ se tiene que $n \mid m$, entonces n es la menor potencia positiva (exponente) de g con la cual se llega a e y por lo tanto $n = \mathrm{o}(g)$.

2. Para el directo, si $n = \mathrm{o}(g)$, por definición sabemos que $g^n = e$. Ahora, si $g^d = e$ con $d \mid n$, $d \neq n$, por la parte 1 sabemos que $n \mid d$, lo que implica que $n = d$ lo cuál contradice la hipótesis sobre d. Concluimos que no existe tal d.

   Para el recíproco, supongamos que $m = \mathrm{o}(g) \neq n$, que por definición de orden cumple $m < n$. Sabemos que $g^m = e$ y por la parte 1, $m \mid n$, que contradice la hipótesis. Por lo tanto $n = \mathrm{o}(g)$.

3. El directo es similar a la demostración anterior ya que $\frac{n}{p} \mid n$.

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

4. Se deduce de la primer parte de la proposición.

5. Tenemos que $g^m = g^k$ si y sólo si $g^m \left(g^k\right)^{-1} = e$; si y sólo si, $g^{m-k} = e$. Y por la primer parte, ésto sucede si y sólo si $\mathrm{o}(g) \mid (m - k)$; es decir, si y sólo si $m \equiv k \pmod{\mathrm{o}(g)}$.

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 $\mathrm{o}(g)$ es finito.

7. (Esta parte es un ejercicio del práctico, pero por su importancia, la desarrollamos aquí). Llamemos $n = \mathrm{o}(g)$, y $d = \mathrm{mcd}(n, k)$. Entonces tenemos que $n = dn'$, $k = dk'$ siendo n' y k' enteros coprimos. Entonces queremos probar que $\mathrm{o}(g^k) = n'$. Usando la primer parte, debemos probar dos cosas: que $(g^k)^{n'} = e$ y que si $(g^k)^m = e$ entonces $n' \mid m$. Veamos lo primero: $(g^k)^{n'} = \left(g^{dk'}\right)^{n'} = g^{dn'k'} = g^{nk'} = (g^n)^{k'} = e^{k'} = e$. Para los segundo: si $\left(g^k\right)^m = e$ entonces $g^{km} = e$ y como $n = \mathrm{o}(g)$, por la primer parte tenemos que $n \mid (km)$. Cancelando d obtenemos que $n' \mid (k'm)$, y como $\mathrm{mcd}(n', k') = 1$, por el Lema de Euclides concluímos que $n' \mid m$.

8. Es claro por la parte anterior.

□

La siguiente proposición relaciona el orden de un elemento con la cantidad de elementos del subgrupo que genera.

Proposición 3.7.9. *Si $(G, *, e)$ es un grupo y $g \in G$ entonces:*

$$|\langle g \rangle| = \mathrm{o}(g).$$

Demostración. Si $\mathrm{o}(g) = \infty$, por la parte (4) de la proposición anterior, 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 $|\langle g \rangle| = \#\left\{g^k : k \in \mathbb{Z}\right\} = \infty = \mathrm{o}(g)$.

Ahora si $\mathrm{o}(g) = n$ es finito, por la parte (3) de la proposición anterior tenemos que $g^m = g^k$ si y sólo si $k \equiv m \pmod{n}$ y por lo tanto $\langle g \rangle = \left\{g^k : k \in \mathbb{Z}\right\} = \left\{g^0 = e, g, g^2, \cdots, g^{n-1}\right\}$ y entonces $|\langle g \rangle| = \#\left\{g^0 = e, g, g^2, \cdots, g^{n-1}\right\} = n = \mathrm{o}(g)$. □

Corolario 3.7.10. *Sea G un grupo de orden* **finito**. *Entonces:*

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

Demostración.

1. G es cíclico si y sólo si existe $g \in G$ tal que $\langle g \rangle = G$. Como $|G|$ es finito, ésto sucede si y sólo existe $g \in G$ tal que $|\langle g \rangle| = |G|$. Y como $|\langle g \rangle| = \mathrm{o}(g)$ queda demostrada la primer parte.
2. Tenemos que $G = \left\langle g^k \right\rangle$ si y sólo si $|G| = \mathrm{o}\left(g^k\right)$. Como $|G| = \mathrm{o}(g)$, tenemos que $G = \left\langle g^k \right\rangle$ si y sólo si $\mathrm{o}\left(g^k\right) = \mathrm{o}(g)$ y por la parte (8) de la Proposición 3.7.8, tenemos que $\mathrm{o}\left(g^k\right) = \mathrm{o}(g)$ si y sólo si $mcd(k, \mathrm{o}(g)) = 1$ y como $\mathrm{o}(g) = |G|$ se concluye lo deseado.
3. Al ser $G = \langle g \rangle$ y G finito, tenemos que $G = \left\{e = g^0, g, g^2, \cdots, g^{|G|-1}\right\} = \left\{g^k : k \in \{0, \cdots, |G| - 1\}\right\}$. Junto con lo visto en la parte anterior concluimos que $\{h \in G : \langle h \rangle = G\} = \left\{g^k : k \in \{0, \cdots, |G| - 1\} \text{ y } \mathrm{mcd}(k, |G|) = 1\right\}$ y este conjunto tiene cardinal $\varphi(|G|)$.

□

Por ejemplo, en el grupo dihedral D_n, los elementos tienen orden 1, 2 o n y por lo tanto D_n **no es cíclico** ya que no tiene elementos de orden $2n$. La siguiente proposición es un ejercicio del repartido de práctico:

Proposición 3.7.11. *Sea G un grupo cíclico, entonces todo subgrupo de G también es cíclico.*

Demostración. Sugerencia: si $G = \langle g \rangle$ y $H < G$, probar que $H = \langle g^n \rangle$ siendo $n = \min\{m \in \mathbb{Z}^+ : g^m \in H\}$. □

3.8. Teorema de Lagrange

En esta sección veremos uno de los principales teoremas de la teoría: el orden de un subgrupo divide al orden del grupo. Además veremos importantes consecuencias.

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 $C_1, C_2, \cdots, C_k$ 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 ($C_i \cap C_j = \emptyset$ si $i \neq j$). 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 $\left(g(g')^{-1}\right)^{-1} \in H$. 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 $C = \{hg' : h \in H\}$. Además, 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 3.8.2. *Si $(G, *, e)$ es un grupo de orden finito y $g \in G$ tenemos que*

1. $\mathrm{o}(g) \mid |G|$.
2. $g^{|G|} = e$.
3. *Si $|G|$ es primo, entonces G es cíclico.*
4. $G = \langle g \rangle$ *si y sólo si* $g^d \neq e$ *para todo* $d \mid |G|$, $d \neq |G|$.
5. $G = \langle g \rangle$ *si y sólo 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 $|H| = \mathrm{o}(g)$ (Proposición 3.7.9). Entonces, por el Teorema de Lagrange tenemos que $\mathrm{o}(g) = |H|$ divide a $|G|$ y hemos probado la primer parte.

Además, como $|G|$ es un múltiplo de $\mathrm{o}(g)$, se deduce que $g^{|G|} = e$ (segundo ítem de la Proposición 3.7.8).

Para la tercer parte, como $|G| \geq 2$ 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 último, las partes 4 y 5 son consecuencia de las partes 2 y 3 de la Proposición 3.7.1. □

En particular, si $G = U(n)$, como $|G| = \varphi(n)$ obtenemos que para todo $\overline{a} \in U(n)$, $\overline{a}^{\varphi(n)} = \overline{1}$. Es decir, que para todo a coprimo con n, $a^{\varphi(n)} \equiv 1 \pmod{n}$ y por lo tanto hemos obtenido el **Teorema de Euler** como consecuencia del Teorema de Lagrange.

3.9. Homomorfismos

Ahora hablaremos de las funciones entre grupos que *preservan las operaciones*:

Definición 3.9.1. Sean $(G, *)$ y $(K, \star)$ dos grupos. Una función $f : G \to K$ es un **homomorfismo** o **morfismo de grupos** si para todo $g, g' \in G$, $f(g * g') = f(g) \star f(g')$.

Veamos algunos ejemplos:

Ejemplos 3.9.2. *1. Si e_K es el neutro de K, entonces la función $f : G \to K$ dada por $f(g) = e_K$ para todo $g \in G$, es un homomorfismo (llamado el* **homomorfismo trivial***).*

2. La función identidad $\mathrm{Id} : G \to G$ es un homomorfismo.

3. La función $f : (\mathbb{Z}, +) \to (\mathbb{R}^*, \times)$ dada por $f(n) = 2^n$ es un homomorfismo pues $2^{n+m} = 2^n 2^m$ para todo $n, m \in \mathbb{Z}$.

4. Dado cualquier grupo $(G, *)$ y un elemento fijo $g \in G$, la función $f : (\mathbb{Z}, +) \to (G, *)$ dada por $f(n) = g^n$ es un homomorfismo pues $g^{n+m} = g^n * g^m$ para todo $n, m \in \mathbb{Z}$.

5. La función $f : M_{n\times n}(\mathbb{R}) \to (\mathbb{Z}, +)$ dada por $f(M) = \mathrm{traza}(M)$ es un homomorfismo.

Tenemos las siguientes propiedades:

Proposición 3.9.3. *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. *$f\left(g^{-1}\right) = f(g)^{-1}$.*
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 $\mathrm{o}(f(g))$ también es finito y además divide a $\mathrm{o}(g)$.*

Demostración. 1. Como e_G es el neutro de G tenemos que $e_G * e_G = e_G$. Aplicando f a ambos lados tenemos que $f(e_G * e_G) = f(e_G)$. Ahora, como f es homomorfismo, tenemos que $f(e_G) \star f(e_G) = f(e_G)$ y cancelando $f(e_G)$ obtenemos que $f(e_G) = e_K$.

2. Ejercicio.

3. Ejercicio.

4. Sea $n = \mathrm{o}(g)$; entonces $g^n = e_G$ y aplicando f a ambos lados obtenemos $f\left(g^n\right) = f(e_G)$. Ahora, usando las propiedades (1) y (3) obtenemos que $f(g)^n = e_K$. Por lo tanto $\mathrm{o}(f(g))$ divide a $n = \mathrm{o}(g)$.

□

Ejemplo 3.9.4. *Veamos cuántos homomorfismos $f : U(8) \to \mathbb{Z}_3$ hay. Por la propiedad (1), tenemos que $f(\overline{1}) = \overline{0}$. Por otro lado en $U(8)$, $\mathrm{o}(\overline{3}) = \mathrm{o}(\overline{5}) = \mathrm{o}(\overline{7}) = 2$ y entonces, por la propiedad (4) tenemos que $\mathrm{o}(f(\overline{3})) \mid 2$. Pero en $\mathbb{Z}_3$ tenemos elementos de orden 1 (el $\overline{0}$) y de orden 3 ($\overline{1}$ y $\overline{2}$). Así que la única posiblidad es que $\mathrm{o}(f(\overline{3})) = 1$ y entonces $f(\overline{3}) = \overline{0}$. De forma análoga debemos tener $f(\overline{5}) = f(\overline{7}) = \overline{0}$ y por lo tanto el único homomorfismo $f : U(8) \to \mathbb{Z}_3$ es el trivial.*

Definición 3.9.5. Sean $(G, *, e_G)$ y $(K, \star, e_K)$ grupos y $f : G \to K$ un homomorfismo. Definimos:

1. el **núcleo** de f, $\mathrm{Ker}(f) = \{g \in G : f(g) = e_K\}$; y
2. la **imagen** de f, $\mathrm{Im}(f) = \{k \in K : \exists g \in G : f(g) = k\} = \{f(g) : g \in G\}$.

Veamos algunos ejemplos:

Ejemplos 3.9.6. *1. Si e_K es el neutro de K, y consideramos el homomorfismo trivial $f : G \to K$ dado por $f(g) = e_K$ entonces $\mathrm{Ker}(f) = G$ e $\mathrm{Im}(f) = \{e_K\}$.*

2. *Para la función identidad* $\mathrm{Id} : G \to G$ *tenemos que* $\mathrm{Ker}(\mathrm{Id}) = \{e_G\}$ *e* $\mathrm{Im}(\mathrm{Id}) = G$.

3. *Para el homomorfismo* $f : (\mathbb{Z}, +) \to (\mathbb{R}^*, \times)$ *dado por* $f(n) = 2^n$ *tenemos que* $\ker(f) = \{0\}$ *e* $\mathrm{Im}(f) = \langle 2 \rangle$.

4. *Si consideramos el homomorfismo* $f : (\mathbb{Z}, +) \to (U(7), \times)$ *dado por* $f(n) = \overline{2}^n$. *Observar que en* $U(7)$ *el* $o(\overline{2}) = 3$ *y por lo tanto* $f(n) = \begin{cases} \overline{1} & \text{si } n \equiv 0 \pmod 3 \\ \overline{2} & \text{si } n \equiv 1 \pmod 3 \\ \overline{4} & \text{si } n \equiv 2 \pmod 3. \end{cases}$

   Por lo tanto tenemos que $\mathrm{Ker}(f) = \{n : n \equiv 0 \pmod 3\} = 3\mathbb{Z}$ *e* $\mathrm{Im}(f) = \langle \overline{2} \rangle = \{\overline{1}, \overline{2}, \overline{4}\}$.

5. *Dado cualquier grupo* $(G, *)$ *y un elemento fijo* $g \in G$, *para el homorfismo* $f : (\mathbb{Z}, +) \to (G, *)$ *dado por* $f(n) = g^n$ *tenemos claramente que* $\mathrm{Im}(f) = \langle g \rangle$. *Por otro lado, si* $\mathrm{o}(g) = \infty$, *como* $g^n \neq e_G$ *para todo* $n \neq 0$, *tenemos que* $\mathrm{Ker}(f) = \{0\}$. *Y si* $\mathrm{o}(g) = m$ *es finito, entonces tenemos que* $g^n = e_G$ *si y sólo si* $m \mid n$. *Entonces en este caso* $\mathrm{Ker}(f) = \{n \in \mathbb{Z} : m \mid n\} = m\mathbb{Z}$.

Proposición 3.9.7. *Sean* $(G, *, e_G)$ *y* $(K, \star, e_K)$ *dos grupos y* $f : G \to K$ *un homomorfismo, entonces:*

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

Demostración.

1. Por definición es claro que $\mathrm{Ker}(f) \subset G$. Como $f(e_G) = e_K$ tenemos que $e_G \in \mathrm{Ker}(f)$. Ahora, si $g, g' \in \mathrm{Ker}(f)$, entonces $f(g * g') = f(g) \star f(g') = e_K \star e_K = e_K$ y por lo tanto $g * g' \in \mathrm{Ker}(f)$. Además $f\left(g^{-1}\right) = f(g)^{-1} = e_K^{-1} = e_K$ y entonces $g^{-1} \in \mathrm{Ker}(f)$. Hemos probado que $\mathrm{Ker}(f)$ contiene al neutro de G, y que es cerrado por la operación y por inversos; por lo tanto es un subgrupo de G.

2. Ejercicio.

3. Si f es inyectiva el neutro de e_K tiene a lo sumo una sóla preimagen por f. Y como $f(e_G) = e_K$ concluimos que $\mathrm{Ker}(f) = \{e_G\}$.

   El recíproco: si $\mathrm{Ker}(f) = \{e_G\}$ veamos que f es inyectiva. Sean $g, g' \in G$ tales que $f(g) = f(g')$; entonces $f(g) \star f((g'))^{-1} = e_K$ y por lo tanto $f\left(g * (g')^{-1}\right) = e_K$. Entonces $g * (g')^{-1} \in \mathrm{Ker}(f)$ y por hipótesis concluimos que $g * (g')^{-1} = e_G$; por lo tanto, $g = g'$, lo que prueba la inyectividad de f.

4. Es claro.

□

Observar que si G es un grupo finito y $f : G \to K$ es un homomorfismo, como $\mathrm{Ker}(f) < G$, por el Teorema de Lagrange tenemos que

$$|\mathrm{Ker}(f)| \mid |G|.$$

Y de la misma forma, si K es finito tenemos que

$$|\mathrm{Im}(f)| \mid |K|.$$

Existe otra relación entre los órdenes del núcleo y la imagen. El siguiente teorema es consecuencia de un teorema de la teoría de grupos llamado *el Primer Teorema de Isomorfismos*, pero que utiliza conceptos que no veremos en este curso. Daremos una demostración sin utilizar estos conceptos.

Teorema 3.9.8 (Teorema de órdenes). *Sean G y K dos grupos y $f : G \to K$ un homomorfismo. Entonces*

$$|G| = |\operatorname{Ker}(f)| \times |\operatorname{Im}(f)|.$$

Demostración. Para cada $y \in \operatorname{Im}(f)$, sea

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

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

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

y la unión es disjunta; esto es porque:

- Claramente la unión de las preimágenes es un subconjunto de G. A su vez, cada $g \in G$, está en $f^{-1}(f(g))$, así que G está incluído en la unión de todas las preimágenes.
- 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 sólo si $y = y'$.

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

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

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

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

Observar que $\#\{gx : x \in \operatorname{Ker}(f)\} = |\operatorname{Ker}(f)|$ puesto que para cada $x \in \operatorname{Ker}(f)$ tenemos un elemento gx en este conjunto, y no hay repeticiones pues si $x \neq x'$, por la cancelativa se tiene que $gx \neq gx'$.

Probemos entonces que si $y \in \operatorname{Im}(f)$ y fijamos $g \in f^{-1}(y)$, entonces $f^{-1}(y) = \{gx : x \in \operatorname{Ker}(f)\}$.

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

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

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

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

□

Daremos a continuación otra demostración para el mismo teorema; utilizando lo ya probado en el Teorema de Lagrange:

Demostración. Recordamos que en la demostración del Teorema de Lagrange, probamos que si $H < G$, entonces la relación en G dada por $g \sim g' \Leftrightarrow g(g')^{-1} \in H$ es una relación de equivalencia. Además vimos que las clases de equivalencia tienen cardinal $|H|$ y que por lo tanto (como las clases de equivalencia son una partición de G) tenemos que

$$|G| = k|H|$$

donde k es la cantidad de clases de equivalencia.

Ahora usemos ésto para el subgrupo $H = \ker(f)$. Entonces tenemos que $|G| = k|\ker(f)|$ y por lo tanto sólo nos resta probar que en este caso, la cantidad de clases de equivalencia es exactamente $|\operatorname{Im}(f)|$; es decir que $k = |\operatorname{Im}(f)|$.

Observar que $g \sim g' \Leftrightarrow g(g')^{-1} \in \ker(f) \Leftrightarrow f\left(g(g')^{-1}\right) = e_K$ (por definición de $\ker(f)$) $\Leftrightarrow f(g)f((g')^{-1}) = e_K$ (porque f es homomorfismo) $\Leftrightarrow f(g)f((g'))^{-1} = e_K$ (por la propiedad de homomorfismos para inversos) $\Leftrightarrow f(g) = f(g')$ (multiplicamos a ambos lados por $f(g')$).

Es decir que

$$g \sim g' \Leftrightarrow f(g) = f(g').$$

Por lo tanto, dado $g \in G$, tenemos que su clase de equivalencia es $[g] = \{g' \in G : \ f(g) = f(g')\}$; es decir que si $y = f(g)$, entonces

$$[g] = \{g' \in G : \ f(g') = y\} = f^{-1}(y).$$

Entonces cada clase de equivalencia es exactamente el conjunto de preimágenes por f de un elemento $y \in \operatorname{Im}(f)$ y entonces (como además dos elementos distintos en $\operatorname{Im}(f)$ tienen conjuntos de preimágenes disjuntos), tenemos que hay tantas clases de equivalencia como elementos en $\operatorname{Im}(f)$; es decir que $k = |\operatorname{Im}(f)|$ y entonces

$$|G| = k|\ker(f)| = |\operatorname{Im}(f)| \times |\ker(f)|.$$

□

Proposición 3.9.9. *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*

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

está bien defínida y es un homomorfismo si y sólo si $\operatorname{o}(k) \mid \operatorname{o}(g)$.

Demostración. El directo de la proposición es consecuencia de la parte 4 de la Proposición 3.9.3.

Para el recíproco tenemos que verificar dos cosas, primero que f está bien defínida y luego que es un homomorfismo. Para ver que está 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 $n \equiv m \pmod{\operatorname{o}(g)}$, o sea que $\operatorname{o}(g) \mid n - m$, pero $\operatorname{o}(k) \mid \operatorname{o}(g)$ entonces $\operatorname{o}(k) \mid n - m$ y por lo tanto $k^n = k^m$. Verificar que f es un homomorfismo queda como ejercicio. □

Observación 3.9.10. 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 $\operatorname{o}(f(g)) \mid \operatorname{o}(g)$.

Demostración. Es claro por la proposición anterior. □

El siguiente corolario es una clara consecuencia del Teorema 3.9.8 y el Teorema de Lagrange.

Corolario 3.9.11. *Sean G y K grupos finitos.*

1. *Si $f : G \to K$ es un homomorfismo, entonces $|\operatorname{Im}(f)|$ divide a $\operatorname{mcd}(|G|, |K|)$.*
2. *Si $|G|$ y $|K|$ son coprimos, entonces el único homomorfismo $f : G \to K$ es el trivial.*

Ejemplos 3.9.12. *Veamos algunos ejemplos de cuántos homomorfismos hay entre dos grupos G y K.*

1. *Si $G = \mathbb{Z}_7$ y $K = S_6$ entonces por el corolario anterior hay un solo homomorfismo (el trivial), ya que $|\mathbb{Z}_7| = 7$ y $|S_6| = 6!$ que son coprimos.*
2. *Sean $G = \mathbb{Z}_9$ y $K = D_3$. Como $\mathbb{Z}_9 = \langle \overline{1} \rangle$ y $|\mathbb{Z}_9| = 9 = 3^2$, por la Observación 3.9.10, un homomorfismo queda determinado por $f\left(\overline{1}\right)$, que tiene que ser un elemento de D_3 cuyo orden divida a 9. Tendremos entonces 3 homomorfismos, dos corresponden a los dos elementos de orden 3 de K, que son r y r^2, y el otro es el homomorfismo trivial.*

Definición 3.9.13. Dados dos grupos $(G, *, e_G)$ y $(K, \star, e_K)$, una función $f : G \to K$ es un **isomorfismo** si es un homomorfismo biyectivo. Decimos que G y K son **isomorfos** si existe un isomorfismo $f : G \to K$.

Las siguientes observaciones son fáciles de probar y quedan como ejercicio.

Observaciones 3.9.14. *Tenemos que*

1. *Un homomorfismo $f : G \to K$ es un isomorfismo si y sólo si $\operatorname{Ker}(f) = \{e_G\}$ e $\operatorname{Im}(f) = K$.*
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 sólo si K es abeliano.*
5. *Si $f : G \to K$ es un isomorfismo y $g \in G$ entonces $o(g) = o(f(g))$.*

Por la observación (3), si bien $\mathbb{Z}_6$ y S_3 tienen la misma cantidad de elementos, no son isomorfos ya que el primero es abeliano y el segundo no lo es.

Capítulo 4

Raíces Primitivas

4.1. Raíces Primitivas

En esta seccción nos concentraremos en determinar para cuáles $n \in \mathbb{Z}^+$, el grupo $U(n)$ es cíclico, y en caso que lo sea veremos cómo hallar sus generadores.

Definición 4.1.1. Dado un $n \in \mathbb{Z}^+$, un entero $g \in \{1, \cdots, n\}$ es **raíz primitiva módulo** n, si $\langle \overline{g} \rangle = U(n)$.

Veamos los primeros ejemplos.

Ejemplos 4.1.2. *1. Para $n = 1$ tenemos que $U(1) = \{\overline{1}\} = \langle \overline{1} \rangle$ y por lo tanto $g = 1$ es (la única) raíz primitiva módulo 1.*

2. Para $n = 2$ tenemos que $U(2) = \{\overline{1}\} = \langle \overline{1} \rangle$ y por lo tanto $g = 1$ es (la única) raíz primitiva módulo 2.

3. Para $n = 3$ tenemos que $U(3) = \{\overline{1}, \overline{2}\} = \left\{\overline{2}^2, \overline{2}\right\} = \langle \overline{2} \rangle$ y por lo tanto $g = 2$ es (la única) raíz primitiva módulo 3.

4. Para $n = 4$ tenemos que $U(4) = \{\overline{1}, \overline{3}\} = \left\{\overline{3}^2, \overline{3}\right\} = \langle \overline{3} \rangle$ y por lo tanto $g = 3$ es (la única) raíz primitiva módulo 4.

5. Para $n = 5$ tenemos que $U(5) = \{\overline{1}, \overline{2}, \overline{3}, \overline{4}\}$. Observar que $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8} = \overline{3}$ y $\overline{2}^4 = \overline{6} = \overline{1}$. Por lo tanto $U(5) = \langle \overline{2} \rangle$ y entonces $g = 2$ es raíz primitiva módulo 5.

También, como $\overline{4}^2 = \overline{16} = \overline{1}$, tenemos que $\langle \overline{4} \rangle = \{\overline{1}, \overline{4}\} \neq U(5)$ y por lo tanto **no es raíz primitiva módulo 5**.

Tenemos que $\overline{3}^2 = \overline{9} = \overline{4}$, $\overline{3}^3 = \overline{12} = \overline{2}$ y $\overline{3}^4 = \overline{6} = \overline{6} = \overline{1}$, y por lo tanto $U(5) = \langle \overline{3} \rangle$ y entonces $g = 3$ también es raíz primitiva módulo 5. Hemos visto que para $n = 5$, hay dos raíces primitivas módulo 5.

6. Para $n = 8$, vimos en el ejemplo (6) de los Ejemplos 3.7.5 que $U(8)$ no es cíclico y por lo tanto **no existen raíces primitivas módulo** 8.

7. Para $n = 9$ tenemos que $U(9) = \{\overline{1}, \overline{2}, \overline{4}, \overline{5}, \overline{7}, \overline{8}\}$. Observar que $\overline{2}^2 = \overline{4}$, $\overline{2}^3 = \overline{8}$, $\overline{2}^4 = \overline{7}$, $\overline{2}^5 = \overline{5}$ y $\overline{2}^6 = \overline{1}$; así que $U(9) = \langle \overline{2} \rangle$ y por lo tanto 2 es raíz primitiva módulo 9. Dejamos como ejercicio verificar que también $U(9) = \langle \overline{5} \rangle$ y por lo tanto 5 también es raíz primitiva módulo 9. Como $\langle \overline{1} \rangle = \{\overline{1}\}$, $\langle \overline{4} \rangle = \{\overline{1}, \overline{4}, \overline{7}\} = \langle \overline{7} \rangle$ y $\langle \overline{8} \rangle = \{\overline{1}, \overline{8}\}$, concluímos que el resto de los candidatos no son raíces primitivas módulo 9.

Vemos entonces que hay casos para los cuales no existen raíces primitivas módulo n y otros casos para los que sí existen, y que por lo general, si hay una raíz primitiva módulo n, entonces hay más de una. Veamos primero esto último: en el caso de que exista una raíz primitiva, cuántas hay.

Proposición 4.1.3. *Sea $n \in \mathbb{Z}^+$. Si existe una raíz primitiva módulo n, entonces hay $\varphi(\varphi(n))$ raíces primitivas módulo n.*

Demostración. Si existe g raíz primitiva módulo n, entonces $\langle \overline{g} \rangle = U(n)$. Como $U(n)$ es finito, por la última parte del Corolario 3.7.10 tenemos que $U(n)$ tiene $\varphi(|U(n)|)$ generadores; y al ser $|U(n)| = \varphi(n)$ concluímos que $U(n)$ tiene $\varphi(\varphi(n))$ generadores distintos. Es decir, tiene $\varphi(\varphi(n))$ raíces primitivas. □

Observar que en particular (por la segunda parte del Corolario 3.7.10) si g es raíz primitiva módulo n, entonces el conjunto de raíces primitivas módulo n son los restos de dividir entre n los elementos del conjunto

$$\left\{ g^k : k \in \{1, \cdots, \varphi(n) - 1\} \text{ y } \operatorname{mcd}(k, \varphi(n)) = 1 \right\}.$$

Ahora veamos algunos resultados que nos facilitarán verificar si un entero g es raíz primitiva módulo n o no, sin tener que calcular todas las potencias de g.

Proposición 4.1.4. *Sea $n \in \mathbb{Z}^+$ y $g \in \{1, \cdots, n\}$, entonces las siguientes afirmaciones son equivalentes.*

1. *g es raíz primitiva módulo n.*
2. *$\operatorname{mcd}(g, n) = 1$ y el orden de $\overline{g}$ en $U(n)$ es $\varphi(n)$.*
3. *$\operatorname{mcd}(g, n) = 1$ y $g^d \not\equiv 1 \pmod{n}$ para todo d divisor de $\varphi(n)$ y $d \neq \varphi(n)$.*
4. *$\operatorname{mcd}(g, n) = 1$ y $g^{\frac{\varphi(n)}{p}} \not\equiv 1 \pmod{n}$ para todo p primo divisor de $\varphi(n)$.*

Demostración.

1. $\Leftrightarrow$ 2. Tenemos, por definición que g es raíz primitiva módulo n si y sólo si $U(n) = \langle \overline{g} \rangle$. Por la Proposición 3.7.9, esto pasa si y sólo si $\overline{g} \in U(n)$ y $o(\overline{g}) = |U(n)| = \varphi(n)$; si y sólo si $\operatorname{mcd}(g, n) = 1$ y el orden de $\overline{g}$ en $U(n)$ es $\varphi(n)$.

2. $\Leftrightarrow$ 3. Ahora, si consideramos $G = U(n)$, por la primer parte del Corolario 3.8.2 tenemos que si $\overline{g} \in U(n)$, entonces $o(\overline{g})$ divide a $|U(n)| = \varphi(n)$. Es decir $o(\overline{g}) = d$ con d divisor de $\varphi(n)$. Por lo tanto $o(\overline{g}) = \varphi(n)$ si y sólo si $\overline{g}^d \neq \overline{1}$ para todo d divisor de $\varphi(n)$ y $d \neq \varphi(n)$; es decir, si y sólo si $g^d \not\equiv 1 \pmod{n}$ para todo d divisor de $\varphi(n)$ y $d \neq \varphi(n)$.

3. $\Leftrightarrow$ 4. Observar primero que si $m \in \mathbb{Z}$ y d es un divisor de m y $d \neq m$, entonces existe un primo p divisor de m tal que $\frac{m}{p}$ es múltiplo de d. Esto es porque si consideramos la descomposición factorial de $m = p_1^{a_1} \cdots p_k^{a_k}$ si d es un divisor positivo de m, por el Corolario 1.7.6, tenemos que $d = p_1^{b_1} \cdots p_k^{b_k}$ con $b_i \leq a_i$ para todo $i = 1, \cdots, k$. Y si $d \neq m$ entonces para algún i, $b_i < a_i$ y entonces $\frac{m}{p_i}$ es múltiplo de d.

   Ahora bien, volviendo a lo que queremos demostrar. Tenemos entonces que si d es un divisor de $\varphi(n)$, y $d \neq \varphi(n)$, por lo visto recién existe un primo p divisor de $\varphi(n)$ tal que $\frac{\varphi(n)}{p}$ es múltiplo de d; es decir, existe $c \in \mathbb{Z}$ tal que $cd = \frac{\varphi(n)}{p}$. Entonces si $g^{\frac{\varphi(n)}{p}} \not\equiv 1 \pmod{n}$ tenemos que $g^d \not\equiv 1 \pmod{n}$ (pues si tuviéramos que $g^d \equiv 1 \pmod{n}$ elevando ambos lados por c obtendríamos que $g^{\frac{\varphi(n)}{p}} \equiv 1 \pmod{n}$.) Esto prueba que $4 \Rightarrow 3$. Es claro que $3 \Rightarrow 4$ pues $d = \frac{\varphi(n)}{p}$ es un divisor de $\varphi(n)$ y $d \neq \varphi(n)$.

□

Ejemplo 4.1.5. *Vamos a probar que 11 es raíz primitiva módulo 41. Por la proposición anterior tenemos que probar que $11^{\frac{\varphi(41)}{p}} \not\equiv 1 \pmod{41}$ para $p = 2, 5$ ya que $\varphi(41) = 40 = 2^3 5$. Usando exponenciación rápida:*

n	$11^{2^n} \pmod{41}$
0	*11*
1	$121 \equiv -2$
2	*4*
3	*16*
4	$256 \equiv 10$

Ahora $\frac{\varphi(41)}{2} = 2^2 5 = 20 = 2^4 + 2^2$ *y* $\frac{\varphi(41)}{5} = 8 = 2^3$, *por lo que* $11^{\frac{\varphi(41)}{2}} \equiv 10 \cdot 4 \pmod{41} \equiv 40 \pmod{41} \not\equiv 1 \pmod{41}$, *y* $11^{\frac{\varphi(41)}{5}} \equiv 16 \pmod{41} \not\equiv 1 \pmod{41}$.

El siguiente teorema nos dice en qué casos pueden existir raíces primitivas módulo n. La demostración es un ejercicio del repartido práctico.

Teorema 4.1.6. *Sea* $n \in \mathbb{Z}^+$. *Si existe una raíz primitiva módulo* n, *entonces*

- $n = 1, 2, 4$ *o*
- $n = p$ *con* p *primo impar, o*
- $n = p^k$ *con* p *primo impar y* $k \in \mathbb{Z}^+$ *o*
- $n = 2p^k$ *con* p *primo impar y* $k \in \mathbb{Z}^+$.

El objetivo de lo que resta de esta sección es probar (o dar ideas de las demostraciones) que vale el recíproco del teorema anterior. Es decir, que en todos los casos listados en el teorema anterior, existen raíces primitivas. Probaremos la existencia para el caso de $n = p$ primo impar, y mostraremos como a partir de una raíz primitiva módulo p, podemos obtener raíces primitivas para los otros casos.

Para demostrar la existencia de raíces primitivas módulo p, daremos una demostración que no es constructiva (en el repartido práctico tienen como ejercicio encontrar un algoritmo para hallar dichar raíces) pero que utiliza resultados que nos parecen importantes de remarcar. Comencemos con algunos lemas previos.

Lema 4.1.7. *En un grupo* G, *si* $x, y \in G$ *son elementos de orden* a, b *respectivamente tales que* $xy = yx$ *y* $\mathrm{mcd}(a, b) = 1$ *entonces el orden de* xy *es* ab.

Demostración. Veamos que $n = ab$ cumple las propiedades de la primer parte de la Proposición 3.7.8. Como $xy = yx$ tenemos que para todo m, $(xy)^m = x^m y^m$. Entonces:

- $(xy)^{ab} = x^{ab} y^{ab} = (x^a)^b \left(y^b\right)^a = e^b e^a = e$.
- Sea $m \in \mathbb{Z}^+$ tal que $(xy)^m = e$; entonces elevando ambos a la b, obtenemos que $(xy)^{mb} = e$ y por lo tanto $x^{mb} y^{bm} = e$ y entonces $x^{mb} = e$. Como $a = o(x)$ concluímos entonces que $a \mid mb$; y como $\mathrm{mcd}(a, b) = 1$, por el Lema de Euclides concluimos que $a \mid m$. De forma análoga se prueba que $b \mid m$. Tenemos entonces que a y b dividen a m y como a y b son coprimos concluimos que $ab \mid m$.

□

Vale la pena remarcar que ambas hipótesis son necesarias en el Lema anterior. Veamos un ejemplo donde el resultado anterior falla cuando los órdenes no son coprimos: en $(\mathbb{Z}_2, +)$, si consideramos $x = y = \overline{1}$, entonces $a = b = 2$, y $x + y = \overline{0}$. Por lo tanto $o(x + y) = o(\overline{0}) = 1 \neq 2 \times 2 = o(x)o(y)$. Veamos ahora un ejemplo donde los órdenes son coprimos pero los elementos no conmutan: en D_3, si consideramos $x = s$ la simetría e $y = r$ la rotación de 120 grados, ya vimos que $rs \neq sr$. Por otro lado tenemos que los elementos tiene órdenes coprimos ya que $o(s) = 2$ y $o(r) = 3$, pero $o(sr) \neq 2 \times 3 = 6$ ya que en D_3 no hay elementos de orden 6.

El siguiente resultado que necesitamos es sobre la cantidad de raíces en $\mathbb{Z}_p$ de un polinomio con coeficientes enteros, cuando p es primo. Observar por ejemplo que si buscamos soluciones enteras a la ecuación $x^2 - x \equiv 0 \pmod 6$, vemos que $x = 0, 1, 3, 4$ son soluciones. Por lo tanto $x^2 - x$, que es un polinomio de grado 2, tiene 4 raíces en $\mathbb{Z}_6$. Esta observación puede sorprender ya que es algo que no sucede cuando consideramos este tipo de ecuaciones en los reales. El motivo por el cual tenemos más raíces que el grado, es porque $x^2 - x = x(x-1)$. Cuando buscamos soluciones de $x(x-1) \equiv 0 \pmod 6$; buscamos los x tal que $6 \mid x(x-1)$. Y esto pasa si $6 \mid x$ (es decir $x \equiv 0 \pmod 6$), o si $6 \mid (x-1)$ (es decir, si $x \equiv 1 \pmod 6$), pero también si $2 \mid x$ y $3 \mid (x-1)$ o si $3 \mid x$ y $2 \mid (x-1)$. El hecho de que 6 no sea primo hace que aparezcan estas últimas soluciones. El siguiente lema muestra que si el módulo es primo, esto último no sucede.

Lema 4.1.8. *Sea $d \in \mathbb{Z}^+$, $f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_1 x + a_0$ con los coeficientes $a_i \in \mathbb{Z}$ para todo i. Entonces si p es primo, la ecuación*

$$f(x) \equiv 0 \pmod p$$

tiene a lo sumo d soluciones en $\mathbb{Z}_p$.

Demostración. Lo demostramos por inducción en d. El resultado es claro si $d = 1$, ya que $x + a_0 \equiv 0 \pmod p$ si y sólo si $x \equiv -a_0 \pmod p$, y por lo tanto hay una única solución módulo p.

Asumamos ahora que $d > 1$ y el resultado es cierto para $d - 1$. Si $f(x) \equiv 0 \pmod p$ no tiene soluciones enteras, ya está. Si tiene una solución entera $x = a$ (es decir que $f(a) \equiv 0 \pmod p$), entonces dividiendo $f(x)$ entre $x - a$ obtenemos que $f(x) = (x-a)q(x) + f(a)$, con $q(x)$ polinomio con coeficientes enteros. Entonces, un entero x cumple que $f(x) = (x-a)q(x) + f(a) \equiv 0 \pmod p$ si y sólo si (como $f(a) \equiv 0 \pmod p$) $(x-a)q(x) \equiv 0 \pmod p$; si y sólo si p divide a $(x-a)q(x)$. Ahora como p es primo, esto último sucede si y sólo si $p \mid (x-a)$ o $p \mid q(x)$. Es decir, si y sólo si $x \equiv a \pmod p$ o $q(x) \equiv 0 \pmod p$. Ahora, $q(x)$ es un polinomio en las mismas hipótesis que f, pero con grado $d-1$, y por lo tanto (por hipótesis inductiva) $q(x) \equiv 0 \pmod p$ tiene a lo sumo $d-1$ soluciones en $\mathbb{Z}_p$. □

Lema 4.1.9. *Sea p primo y d un divisor de $p-1$. Entonces la ecuación $x^d \equiv 1 \pmod p$ tiene exactamente d raíces distintas en $U(p)$.*

Demostración. Si $p - 1 = de$ con $d, e \in \mathbb{Z}^+$, entonces

$$x^{p-1} - 1 = \left(x^d\right)^e - 1 = \left(x^d - 1\right)\left(x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1\right).$$

Llamemos n a la cantidad de soluciones módulo p de $x^d - 1 \equiv 0 \pmod p$ y m a la cantidad de soluciones módulo p de $g(x) = x^{d(e-1)} + x^{d(e-2)} + \cdots + x^d + 1 \equiv 0 \pmod p$. Por Fermat tenemos que la cantidad de soluciones módulo p de $x^{p-1} - 1 \equiv 0 \pmod p$ es exactamente $p-1$. Entonces

$$\begin{aligned} p - 1 = &\text{ cantidad de soluciones módulo } p \text{ de } (x^{p-1} - 1 \equiv 0 \pmod p) \\ &\leq n + m \\ &\leq d + m \\ &\leq d + d(e-1) \\ &= de = p - 1, \end{aligned}$$

donde la primer desigualdad es porque puede haber repeticiones, y la segunda y tercera es por el lema 4.1.8. Por lo tanto, todas las desigualdades son igualdades y en particular $n = d$. □

Ahora sí tenemos todos los ingredientes para probar el teorema principal:

Teorema 4.1.10 (Teorema de la raíz primitiva)**.** *Si p es primo, entonces existen raíces primitivas módulo p.*

Demostración. Si $p-1 = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}$ es la factorización en primos de $p-1$, la idea es encontrar elementos $x_1, x_2, \cdots, x_k$ en $U(p)$ con órdenes $p_1^{d_1}, p_2^{d_2}, \cdots, p_k^{d_k}$ respectivamente. Luego si

$$g = x_1 x_2 \cdots \ x_k,$$

por el Lema 4.1.7 tendremos que $o(g) = o(x_1) \cdots o(x_k) = p-1$ y por lo tanto g será una raíz primitiva módulo p.

Veamos entonces, que para $i = 1, \cdots, k$, existe x_i con orden $p_i^{d_i}$. Por el Lema 4.1.8 sabemos que $x^{p_i^{d_i}} \equiv 1 \pmod{p}$ tiene exactamente $p_i^{d_i}$ soluciones en $U(p)$ y que $x^{p_i^{d_i-1}} \equiv 1 \pmod{p}$ tiene exactamente $p_i^{d_i-1}$ soluciones. Por lo tanto, existe un x_i solución de la primer ecuación y que no es solución de la segunda.

Es decir $x_i^{p_i^{d_i}} \equiv 1 \pmod{p}$ y $x_i^{p_i^{d_i-1}} \not\equiv 1 \pmod{p}$; por lo tanto x_i tiene orden $p_i^{d_i}$. □

Los siguientes lemas (que no demostraremos) muestran que el recíproco del Teorema 4.1.6 es cierto:

Lema 4.1.11. *Sea p un primo impar. Si g es raíz primitiva módulo p entonces g o $g+p$ es raíz primitiva módulo p^2.*

Lema 4.1.12. *Sea p un primo impar. Si g es raíz primitiva módulo p^2, entonces g es raíz primitiva módulo p^k para todo $k \in \mathbb{Z}^+$.*

Lema 4.1.13. *Si p es un primo impar, $k \in \mathbb{Z}^+$ y g es raíz primitiva módulo p^k entonces:*

- *Si g es impar, g es raíz primitiva módulo $2p^k$.*
- *Si g es par, $g+p^k$ es raíz primitiva módulo $2p^k$.*

Demostración. La demostración es un ejercicio del repartido de práctico. Como sugerencia para la primer parte observar que por el Teorema Chino del Resto se cumple que

$$g^n \equiv 1 \pmod{2p^k} \iff \begin{cases} g^n \equiv 1 \pmod{2} \\ g^n \equiv 1 \pmod{p^k}. \end{cases}$$

La primer congruencia del lado derecho se cumple ya que g es impar. Obtenemos entonces que

$$g^n \equiv 1 \pmod{2p^k} \Leftrightarrow g^n \equiv 1 \pmod{p^k}.$$

Para la segunda parte del lema, podemos observar de manera similar que se cumple que

$$\left(g+p^k\right)^n \equiv 1 \pmod{2p^k} \iff \begin{cases} \left(g+p^k\right)^n \equiv 1 \pmod{2} \\ \left(g+p^k\right)^n \equiv 1 \pmod{p^k}. \end{cases}$$

Como antes, la primer congruencia del lado derecho se cumple siempre, y la segunda congruencia se puede reducir a $g^n \equiv 1 \pmod{p^k}$ obteniendo para este caso

$$\left(g+p^k\right)^n \equiv 1 \pmod{2p^k} \iff g^n \equiv 1 \pmod{p^k}.$$

□

Ejemplo 4.1.14. *Utilizando el lema anterior y el Ejemplo 4.1.5 se ve que 11 es raíz primitiva módulo 41^k para todo k entero positivo.*

Concluimos de los lemas y teoremas anteriores:

Teorema 4.1.15. *Sea $n \in \mathbb{Z}^+$. Entonces existe una raíz primitiva módulo n si y sólo si*

- $n = 1,\ 2,\ 4$ *o*
- $n = p$ *con p primo impar, o*
- $n = p^k$ *con p primos impar y $k \in \mathbb{Z}^+$ o*
- $n = 2p^k$ *con p primo impar y $k \in \mathbb{Z}^+$.*

Demostración. El directo es el Teorema 4.1.6. Para el recíproco, los casos $n = 1, 2, 4$ fueron vistos en los ejemplos. El caso $n = p$ con p primo impar, fue probado en el Teorema de la raíz primitiva (Teorema 4.1.10). Por lo tanto tenemos que existe g una raíz primitiva módulo p. Por el Lema 4.1.11 tenemos que existe g' raíz primitiva módulo p^2 ($g' = g$ o $g' = g + p$); luego por el Lema 4.1.12 tenemos que g' es raíz primitiva módulo p^k y por el Lema 4.1.13 tenemos que g' o $g' + p^k$ es raíz primitiva módulo $2p^k$. □

Veamos un ejemplo.

Ejemplo 4.1.16. *Sea $p = 5$.*

1. *Ya vimos en los ejemplos, que $g = 2$ es raíz primitiva módulo 5.*
2. *Por el Lema 4.1.11, sabemos que 2 o 7 es raíz primitiva módulo 25. Como $\varphi(25) = 25 - 5 = 20$, y los primos divisores e 20 son 2 y 5, (por la Proposición 4.1.4) tenemos que 2 es raíz primitiva módulo 25 si sólo si $2^{10} \not\equiv 1 \pmod{25}$ y $2^4 \not\equiv 1 \pmod{25}$. Como $2^{10} \equiv 24 \pmod{25}$ y $2^4 \equiv 16 \pmod{25}$ concluimos que 2 es raíz primitiva módulo 25.*
3. *Por el Lema 4.1.12 tenemos que 2 es raíz primitiva módulo 5^k para todo $k \in \mathbb{Z}^+$.*
4. *Finalmente, por el Lema 4.1.13, tenemos que para cada $k \in \mathbb{Z}^+$, $2 + p^k$ es raíz primitiva módulo 2×5^k.*

Por último, dejamos el siguiente ejercicio para el lector.

Ejercicio 4.1.17. *Sean n entero positivo, $g \in U(n)$, tal que $\mathrm{o}(g) = \frac{\varphi(n)}{2}$ y es impar. Entonces $-g$ es raíz primitiva módulo n.*

Capítulo 5

Criptografía

5.1. Criptosistemas César y Vigenère

Este capítulo está basado en apuntes escritos por el docente Claudio Qureshi en ediciones anteriores del curso. Para comenzar introduciremos dos criptosistemas sencillos para ilustrar algunas técnicas de cifrado.

5.1.1. Método de cifrado César

Lleva este nombre en honor a Julio César, que lo usaba para comunicarse con sus generales. Como primer paso el método enumera las letras del alfabeto, por ejemplo la letra A tiene asignado el 0, la letra B el 1, ..., la letra Z el 26 y a el espacio le asignamos el número 27. La enumeración se puede ver en la tabla más abajo. Luego definimos la clave k como un número entre 0 y 27. Para cifrar un mensaje lo que hacemos es sumarle a cada letra, la clave k y reducir módulo 28. Para descifrar el mensaje debemos restar k a cada letra y reducir módulo 28.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27

Por ejemplo supongamos que queremos cifrar el mensaje "ATACAREMOS POR LA NOCHE", y que el valor de la clave es $k = 16$ (correspondiente a la letra P):

A	T	A	C	A	R	E	M	O	S		P	O	R		L	A		N	O	C	H	E
0	20	0	2	0	18	4	12	14	19	27	16	15	18	27	11	0	27	13	15	2	7	4
16	8	16	18	16	6	20	0	3	7	15	4	2	6	15	27	16	15	1	3	18	23	20
P	I	P	R	P	G	T	A	D	H	O	E	C	G	O		P	O	B	D	R	W	T

En la primer fila se ha colocado el **texto plano (mensaje sin cifrar)**, en la segunda se ha sustituido cada letra por su correspondiente número, en la tercer fila se ha sumado $k = 16$ módulo 28 a cada elemento de la segunda fila. Finalmente sustituímos cada número de la tercer fila por su correspondiente letra y obtenemos el texto cifrado "PIPRPGTADHOECGO POBDRWT".

Observar que para evitar que se vean en el texto cifrado los tamaños de las palabras originales le asignamos al espacio un número.

Es muy sencillo romper este criptosistema por fuerza bruta, pues solo hay que chequear con las 28 posibles claves y ver cuál tiene sentido.

Para el criptosistema César podemos definir la función de cifrado:

$$E : \mathbb{Z}_n \to \mathbb{Z}_n, \qquad E(x) = x + k \pmod{n},$$

donde k es la clave utilizada, y n es la cantidad de caracteres. Entonces podemos decir que el criptosistema César consiste en aplicar dicha función de cifrado a cada letra del texto.

Para descifrar restamos a cada letra la clave k así que la función de descifrado viene dada en este caso por:

$$D : \mathbb{Z}_n \to \mathbb{Z}_n, \qquad D(y) = y - k \pmod{n}.$$

Una posible variante del criptosistema César es el criptosistema afín. Cambiamos la función de cifrado por una función lineal:

$$E : \mathbb{Z}_n \to \mathbb{Z}_n, \qquad E(x) = ax + k \pmod{n}.$$

Pero para poder descifrar el mensaje original la función de cifrado debe ser inyectiva. Queda como ejercicio para el lector probar que la inyectividad de la función de cifrado definida anteriormente es equivalente a pedirle que $\mathrm{mcd}(a, n) = 1$.

Ejercicio 5.1.1. *Probar que la función*

$$E : \mathbb{Z}_n \to \mathbb{Z}_n, \qquad E(x) = ax + k \pmod{n}$$

es biyectiva si y solo si $\mathrm{mcd}(a, n) = 1$.

Así que de ahora en más supondremos que $\mathrm{mcd}(a, n) = 1$. En dicho caso la función de descifrado en el criptosistema afín viene dado por

$$D : \mathbb{Z}_n \to \mathbb{Z}_n, \qquad D(y) = a'(y - k) \pmod{n}$$

donde a' es un inverso de a módulo n. Esto último es fácil de ver, en efecto:

$$ax + k \equiv y \pmod{n} \Leftrightarrow ax \equiv y - k \pmod{n} \Leftrightarrow x \equiv a'(y - k) \pmod{n}.$$

A modo de ejemplo cifremos nuevamente el texto "ATACAREMOS POR LA NOCHE", pero esta vez utilizando un sistema afín con clave $(a, k) = (5, 2)$. Como en el caso anterior asignemos a cada letra un número como en la tabla, de modo que para este caso la cantidad de caracteres codificados es $n = 28$.

A	T	A	C	A	R	E	M	O	S		P	O	R		L	A		N	O	C	H	E
0	19	0	2	0	17	4	12	14	18	26	15	14	17	26	11	0	26	13	14	2	7	4
2	16	2	12	2	6	22	8	18	11	24	23	18	6	24	3	2	24	13	18	12	10	22
C	Q	C	M	C	G	W	I	S	L	Y	X	S	G	Y	D	C	Y	N	S	M	K	W

Al igual que en el criptosistema César, la primer fila representa el texto plano, la segunda de sustituir cada letra por su correspondiente valor, la tercer fila de aplicar la función de cifrado a cada número de la segunda fila (en este caso $E(x) = 5x + 2 \pmod{28}$), la última fila resulta de sustituir cada letra de la tercer fila por su correspondiente valor, obteniendo así el texto cifrado "CQCMCGWISLYXSGYDCYNSMKW".

Aquí se vuelve una tarea más dura poder descifrar el texto sin conocimiento de la clave, por lo menos a mano, pues a fuerza bruta en el peor de los casos deberíamos chequear $\varphi(28) \cdot 28 = 12 \cdot 28 = 336$ casos (contra 28 del sistema César). No obstante con una computadora llevaría un tiempo insignificante. Además puede acelerarse el ataque si agregamos un análisis de frecuencias. Esto es, contar la cantidad de ocurrencias en el texto cifrado de cada símbolo y compararla con las letras que más aparecen en un texto estándar. Por ejemplo, si en el texto cifrado el símbolo que más aparece es la X, lo más probable es que sea una E o una A (que son las letras que más aparecen en los textos en idioma español).

A continuación veremos otra mejora del método César, que es el método Vigenère. En lugar de realizar una sustitución en el texto letra a letra, lo haremos bloque a bloque.

5.1.2. Método de cifrado Vigenère

Aquí la clave consiste en una palabra. El método consiste en repetir debajo del texto cifrado la palabra clave, luego sumar cada letra del texto plano, con la letra de la palabra clave que está debajo de ella (codificando cada letra con un natural como vimos anteriormente) y reduciendo módulo la cantidad de símbolos (por ejemplo 28 en el caso que utilizemos la letras de la A a la Z y el carácter espacio).

A modo de ejemplo cifraremos nuevamente el texto plano "ATACAREMOS POR LA NOCHE", esta vez utilizando el método Vigenère con la palabra clave "PRUEBA":

A	T	A	C	A	R	E	M	O	S		P	O	R		L	A		N	O	C	H	E
P	R	U	E	B	A	P	R	U	E	B	A	P	R	U	E	B	A	P	R	U	E	B
P	K	U	G	B	R	V	C	I	W	A	P	D	I	T	P	B		B	F	W	L	F

Donde la primer fila consiste en el texto plano, en la segunda hemos repetido la palabra clave varias veces (en este caso "PRUEBA"). En la tercera fila aparece el texto cifrado que fue calculado sumando las dos letras de que aparecen en la misma columna, de esa forma obtenemos el texto cifrado "PKUGBRVCIWAPDITPB BFWLF". Para sumar las letras lo que hemos hecho es sumar sus valores numéricos correspondientes módulo 28 y luego sustituimos este valor por su carácter correspondiente, por ejemplo: $\mathsf{A} + \mathsf{P} = 0 + 16 \equiv 16 \pmod{28}$, la letra que corresponde a 16 es P, luego $\mathsf{A} + \mathsf{P} = \mathsf{P}$; $\mathsf{T} + \mathsf{R} = 20 + 18 = 38 \equiv 10 \pmod{28}$, la letra que corresponde a 10 es K, luego $\mathsf{T} + \mathsf{R} = \mathsf{K}$ y así sucesivamente.

Para descifrar el texto simplemente repetimos la palabra clave debajo del texto plano, pero esta vez en vez de sumar, restamos.

Observemos que ahora no es tan fácil chequear a fuerza bruta, la cantidad de claves posibles crece exponencialmente con el tamaño del texto. Este método de cifrado fue bastante utilizado, e incluso considerado invulnerable hasta el siglo XIX, cuando fueron generados algunos métodos para romper este criptosistema.

Un método para romper este criptosistema es el denominado método de Kasiski. Este método consiste primero en hallar el tamaño de la clave. Supongamos que la clave tiene largo k, luego las letras que ocupan lugares congruentes módulo k en el texto fueron cifrados con la misma letra de la palabra clave, y por lo tanto es posible hallar esa letra con un análisis de frecuencias. Para hallar el largo de clave básicamente lo que se hace es buscar secuencias de dos letras (bigramas) o de tres (trigramas) que se repiten en el texto cifrado. Se conjetura que si el texto es suficientemente largo, entonces la distancias entre bigramas o entre trigramas será múltiplo del tamaño de la clave, se obtiene el tamaño de clave probable como el máximo común divisor de tales distancias.

Una mejora sobre el cifrado Vigenère es el sistema de Vernam, el que utiliza una clave aleatoria de longitud igual a la del mensaje. La confianza en este nuevo criptosistema hizo que se utilizase en las comunciaciones confidenciales entre la Casa Blanca y el Kremlin, hasta, por lo menos, el año 1987.

5.2. Criptosistemas de clave privada, métodos de intercambio de clave

Se llaman criptosistemas de clave privada a aquellos criptosistemas que se puede obtener fácilmente la clave de descifrado a partir de la de cifrado.

Por ejemplo los criptosistemas vistos anteriormente son ejemplos de criptosistemas que son muy fáciles de descifrar conociendo la clave de cifrado. En el método César se restaba la clave de cifrado a cada letra, en el afín básicamente hay que hallar un inverso modular que se puede hacer fácilmente a través del Algoritmo de Euclides Extendido y luego obtenemos la función de descifrado que se la aplicamos a cada letra. En el Vigenère es restar la palabra clave reiteradas veces como ya vimos, al igual que en el criptosistema Vernam.

Entonces en estos sistemas, la clave de cifrado ha de ser confidencial entre las personas que llevan la comunicación, dado que a partir de ellas un espía puede calcular la clave de descifrado con facilidad. Pero ¿cómo hacer para intercambiar claves a distancia sin que alguien que pueda interceptar la conversación no sea capaz de encontrar cuál es la clave?

Existen varios métodos para intercambiar claves entre dos personas, entre ellos el que veremos a continuación denominado Método de Diffie-Hellman de intercambio de clave.

5.2.1. Método Diffie-Helmann de intercambio de clave

Supongamos que Ana y Bernardo quieren ponerse de acuerdo en una clave común que sea secreto (o sea que solo ellos conozcan la clave). Pero ellos se encuentran lejos uno del otro y la única forma de comunicarse entre ellos es a través de un canal. El problema es que el canal está interceptado por espías que pueden acceder a la conversación de Ana y Bernardo.[1] Diffie-Helman nos da un posible método para resolver el problema:

1. Ana y Bernardo se ponen de acuerdo en un primo p y raíz primitiva g con $1 < g < p$.
2. Ana elige un número al azar n.
3. Bernardo elige un número al azar m.
4. Ana calcula $g^n \pmod p$ y se lo manda por el canal.
5. Bernardo calcula $g^m \pmod p$ y se lo manda por el canal.
6. La clave común es $c \equiv g^{nm} \pmod p \equiv (g^n)^m \pmod p \equiv (g^m)^n \pmod p$, que tanto Ana como Bernardo pueden calcular.

El espía que accede a la conversación puede conocer p, g, g^n y g^m. Si el espía con esos datos fuese capaz de calcular g^{nm} entonces hemos fallado en el intento de acordar la clave común. Pero la única manera (conocida) de calcular g^{nm} es calculando previamente n o m. Esto en general es un problema computacionalmente difícil y es conocido como el problema del logaritmo discreto en $U(p)$.

Problema del logaritmo discreto en $U(p)$: Dados un primo p, g una raíz primitiva módulo p y $a \in U(p)$, hallar un m tal que $g^m \equiv a \pmod p$. A un tal m se le llama logaritmo discreto de a en base g y se lo denota por $m = \operatorname{dlog}_g a$.

Se puede probar fácilmente que el logaritmo discreto de un número, si existe, no es único sino que está determinado módulo $p - 1$. La prueba se deja como ejercicio para el lector.

En la parte 1 se podría pedir que g solo sea coprimo con p. La ventaja de tomar g raíz primitiva es que tiene orden $p - 1$ que es lo más grande que puede ser y hay por lo tanto más posibilidades para potencias de g. Esto hace que sea más dificil de resolver el logaritmo discreto.

Otra cosa a observar es que tanto Ana en el paso 4 como Bernardo en el paso 5 necesitan calcular $g^n \pmod p$ (y $g^m \pmod p$ respectivamente), esto se puede hacer usando el método de exponenciación rápida 2.7.

Para ilustrar el método veamos un ejemplo con números pequeños:

Ejemplo 5.2.1. *Bernardo y Ana eligen* $p = 97$ *y* $g = 5$. *Ana elige* $n = 31$, *calcula* $5^{31} \equiv 7 \pmod{97}$ *y le comunica el* 7 *a Bernardo por el canal. Bernardo elige* $m = 95$, *calcula* $5^{95} \equiv 39 \pmod{97}$ *y le comunica el* 39 *por el canal. Ahora Ana calcula* $39^{31} \equiv 14 \pmod{97}$ *y Bernardo* $7^{95} \equiv 14 \pmod{97}$, *asi que ambos tienen a* $k = 14$ *como su clave secreta.*

Un ejemplo un poco más real puede obtenerse tomando:

[1] Estamos suponiendo que los espías son atacantes pasivos, es decir, tienen la capacidad de acceder a la información, pero no de modificarla.

Ejemplo 5.2.2. *Como primo* $p = 9345098309485093845098340962 3$ *y* $g = -2$ *(que resulta ser una raíz primitiva módulo* p*). Supongamos que los números secretos de Ana y Bernardo vienen dados por:*

$$n = 183199223755318591716133791 81$$

y

$$m = 8233583624386669568014144030 0.$$

Ana le envía a Bernardo:

$$g^n = 4541677627048536979137594499 8.$$

Bernardo le envía a Ana:

$$g^m = 1504807415177088427182422539 3.$$

La clave secreta común viene dada por:

$$g^{nm} = 8577140947077052121234673954 0.$$

5.3. Criptosistemas de clave pública

Los criptosistemas de clave pública basan su seguridad en que no haya un método eficiente de calcular la clave de descifrado, aún conociendo la clave de cifrado. Estos sistemas tienen la ventaja de que como la clave de cifrado no nos ayuda a calcular la clave de descifrado, puede almacenarse todas las claves de cifrado de muchos usuarios en una guía pública a la cual todos tengan acceso, evitando así que cada vez que dos usuarios quieran comunicarse tengan que ponerse de acuerdo en una clave común. Veremos como ejemplo de criptosistema de clave pública el RSA.

5.3.1. Criptosistema RSA

Este criptosistema creado por Rivest, Shamir y Adleman (RSA) en el año 1977 es uno de los criptosistemas de clave pública más famosos. La idea detrás de este criptosistema es el de construir una función que sea fácil de calcular (en este caso multiplicar dos primos), pero que su inversa sea difícil de calcular (en este caso dado un número que es producto de 2 primos, hallar esos primos). Veamos en qué consiste.

1. Ana elige dos primos (distintos) grandes p y q y calcula $n = pq$.
2. Luego calcula:
$$\varphi(n) = \varphi(p)\varphi(q) = (p-1)(q-1).$$
3. Luego elige un número aleatorio e con:
$$1 < e < \varphi(n) \text{ y } \operatorname{mcd}(e, \varphi(n)) = 1.$$
4. Finalmente Ana tiene definida una función (función de cifrado) definida por:
$$E : \mathbb{Z}_n \to \mathbb{Z}_n : E(x) = x^e \pmod{n}.$$

La clave pública de Ana viene dada por el par (n, e) que puede ser publicada en una guía de claves públicas. Observemos que el par (n, e) nos brinda toda la información necesaria para calcular la función de cifrado E.

Alguien que desee mandarle un mensaje confidencial x a Ana, busca la clave pública de Ana en la guía y le envía el mensaje cifrado $E(x)$.

Con ayuda del Algoritmo de Euclides Ana calcula $d \in \mathbb{Z}^+$ tal que:

$$de \equiv 1 \pmod{\varphi(n)},$$

y podemos definir la función de descifrado como:

$$D : \mathbb{Z}_n \to \mathbb{Z}_n : D(x) = x^d \pmod{n}.$$

Para calcular la función de descifrado es necesario conocer d, que resulta equivalente a conocer los primos p y q que factorizan n. Si los parámetros están bien elegidos, factorizar n llevaría demasiado tiempo, aun usando los mejores algoritmos de factorización conocidos hasta el momento y las computadoras más rápidas en la actualidad. Entonces la seguridad de dicho criptosistema se basa en la dificultad de factorizar números grandes.

Por otra parte observemos que Ana, conociendo d no tiene problema en, dado x, calcular $D(x)$, pues cuenta para ello con algoritmos eficientes para calcular potencias módulo n con el método de exponenciación rápida.

Comenzaremos viendo que efectivamente la función D definida arriba es la función de descifrado.

Proposición 5.3.1. *Sean p, q, n, d y e definidos como antes, y las funciones de cifrado $E(x) = x^e \pmod{n}$ y $D(x) = x^d \pmod{n}$. Entonces se tiene que:*

$$D(E(x)) = x \pmod{n}, \forall x \in \mathbb{Z}_n.$$

Demostración. Como $D(E(x)) = x^{de} \pmod{n}$, debemos probar que $x^{de} \equiv x \pmod{n}$ para todo $x \in \mathbb{Z}$. Conviene aquí separar en casos recordando que d fue elegido tal que $de \equiv 1 \pmod{\varphi(n)}$, donde $\varphi(n) = (p-1)(q-1)$, y por lo tanto existe un k entero tal que $de = (p-1)(q-1)k + 1$.

1. Si p y q dividen a x.

   En este caso tenemos que $pq = n|x$ y por lo tanto también $n|x^{de}$, luego $x^{de} \equiv 0 \equiv x \pmod{n}$.

2. Si p divide a x pero q no divide a x.

   Como $x \equiv 0 \pmod{p}$ entonces $x^{de} \equiv 0 \pmod{p}$. Por otra parte $x^{de} = x^{(p-1)(q-1)k+1} = (x^{q-1})^{(p-1)k} \cdot x \equiv 1 \cdot x = x \pmod{q}$, donde se ha usado el Teorema de Fermat dado que q no divide a x. Así que tenemos:

   $$\begin{cases} x^{de} \equiv x \pmod{p} \\ x^{de} \equiv x \pmod{q} \end{cases}$$

   Luego por la unicidad del Teorema Chino del Resto $x^{de} \equiv x \pmod{n}$.

3. Ni p ni q dividen a x.

   Tenemos que x y n son coprimos, luego por el Teorema de Euler:

   $$x^{\varphi(n)} \equiv 1 \pmod{n}$$

   así que:

   $$x^{de} = x^{\varphi(n)k+1} = (x^{\varphi(n)})^k x \equiv 1 \cdot x = x \pmod{n}.$$

□

5.3.2. Método de cifrado de bloques

Una manera ingenua de cifrar usando RSA es hacerlo letra a letra, es decir asignar a cada letra un valor del 0 al 25 y luego aplicar la función de cifrado a cada letra. Es fácil hacer una tabla de valores de $E(n)$ para $n = 0, 1, 2, \ldots, 25$ y luego en el mensaje cifrado ver a qué letra corresponde cada valor, de esa manera cualquier espía tendría acceso a una conversación confidencial.

Otra forma es usando un método de cifrado de bloques. Si bien existen varios métodos nos centraremos en el ECB (Electronic Codebook), no por ser el más eficiente, sino por ser el más fácil de describir.

Éste, como los otros métodos de cifrado en bloques, es independiente del criptosistema utilizado. Aquí a modo de ejemplo veremos cómo se emplea para un cifrado RSA.

El esquema para RSA sería el siguiente, supongamos que tenemos la clave pública (n, e) y que los caracteres que aparecen en nuestro texto son las 27 letras del alfabeto y el espacio en blanco (en total 28 caracteres) y sea k entero tal $28^k < n < 28^{k+1}$ (observar que ambas desigualdades son estrictas pues n es producto de 2 primos). Ahora separamos nuestro texto en bloques de tamaño k:

b_1	b_2	b_3	$\ldots$	b_t

Sea b_i el bloque i-ésimo, supongamos que $b_i = l_{k-1}l_{k-2}l_{k-3}\ldots l_1 l_0$ donde los l_j son caracteres (en nuestro caso las letras del alfabeto y el espacio). Para cada carácter l_j, sea $\overline{l_j}$ el número asociado, es decir $\overline{A} = 0, \overline{B} = 1, \overline{C} = 2, \ldots \overline{Z} = 26$ y $\overline{Space} = 27$.

Ahora a cada bloque le asignamos un valor entre 0 y $28^k - 1$ de la siguiente manera:

$$x_i = \overline{l_{k-1}} \cdot 28^{k-1} + \overline{l_{k-2}} \cdot 28^{k-2} + \overline{l_{k-3}} \cdot 28^{k-3} + \ldots + \overline{l_1} \cdot 28 + \overline{l_0}.$$

Recíprocamente, cada número entre 0 y $28^k - 1$ tiene un k-bloque (bloque de tamaño k) asociado. Para hallarlo basta escribir al número en base 28 y luego sustituir cada "dígito" por su correspondiente letra, ver 1.1.2.

b_1	b_2	b_3	$\ldots$	b_t
$\downarrow$				
x_1	x_2	x_3	$\ldots$	x_t
$\downarrow$				
y_1	y_2	y_3	$\ldots$	y_t
$\downarrow$				
c_1	c_2	c_3	$\ldots$	c_t

En la primer fila está el texto plano separado en bloques, en la segunda fila cada bloque ha sido sustituido por su valor correpondiente, en la tercer fila se ha aplicado la función de cifrado E, a cada bloque, es decir $E(x_i) = y_i$ (recordemos que como $E : \mathbb{Z}_n \to \mathbb{Z}_n$ tenemos que $0 \leq E(\overline{b_i}) < n$).

Se puede afirmar que $y_i = E(x_i) < 28^{k+1}$ puesto que $n < 28^{k+1}$, así que podemos escribir:

$$y_i = \overline{s_k} \cdot 28^k + \ldots + \overline{s_1} \cdot 28 + \overline{s_0}$$

donde cada $\overline{s_j}$ es un entero entre 0 y 27 (s_j es su carácter correspondiente). Finalmente el $(k+1)$-bloque c_i se define como $c_i = s_k s_{k-1} \ldots s_1 s_0$ y concatenando dichos bloques obtenemos la cuarta fila que es el texto cifrado.

Veamos ésto con un ejemplo.

Ejemplo 5.3.2. *Supongamos que Ana tiene la clave pública $(n, e) = (25573, 1089)$ y que le queremos enviar a Ana el mensaje "PEPITO PIDE PAPA PELADA" utilizando el método de cifrado en bloque ECB codificando cada letra y cada bloque como más arriba.*

Primero observamos que $28^3 < 25573 < 28^4$ y procedemos a partir el texto plano en 3-bloques:

PEP	ITO	PI	DE	PAP	A P	ELA	DA

Ahora calculamos el valor asociado a cada uno de esos 3*-bloques usando la tabla que asocia símbolos con números del principio del capítulo.*

$$\begin{aligned} PEP &= 16 \cdot 28^2 + 4 \cdot 28 + 16 = 12672 \\ ITO &= 8 \cdot 28^2 + 20 \cdot 28 + 15 = 6847 \\ PI &= 27 \cdot 28^2 + 16 \cdot 28 + 8 = 21624 \\ &\vdots \end{aligned}$$

Así que el primer pasaje del texto plano a bloques de números nos queda:

PEP	ITO	PI	DE	PAP	A P	ELA	DA
↓							
12672	6847	21624	2491	12560	772	3444	2379

Ahora aplicamos nuestra función de cifrado a cada bloque de números de la segunda fila obteniendo los siguientes valores:

$$\begin{aligned} 12672^{1089} &\pmod{25573} = 16780 \\ 6847^{1089} &\pmod{25573} = 11127 \\ 21624^{1089} &\pmod{25573} = 12425 \\ &\vdots \end{aligned}$$

Así construimos la tercer fila formado por el texto cifrado dado como bloques de números:

PEP	ITO	PI	DE	PAP	A P	ELA	DA
↓							
12672	6847	21624	2491	12560	772	3444	2379
↓							
16780	11127	12425	5598	15189	8968	5999	834

Finalmente escribimos a cada número de la tercer fila en base 28 *(con* 4 *"dígitos") para ver el bloque correspondiente a cada número.*

Por ejemplo $18461 = 0 \cdot 28^3 + 21 \cdot 28^2 + 11 \cdot 28 + 8$*. Recordemos la correspondencia* $0 \leftrightarrow A, 21 \leftrightarrow U, 11 \leftrightarrow L, 8 \leftrightarrow I$*, entonces* $18461 \leftrightarrow AZIU$*.*

Y así sucesivamente hasta obtener el texto cifrado:

PEP	ITO	PI	DE	PAP	A P	ELA	DA
↓							
12672	6847	21624	2491	12560	772	3444	2379
↓							
16780	11127	12425	5598	15189	8968	5999	834
↓							
AULI	AÑFL	AOWU	AHDZ	ASKN	ALMJ	AHRH	ABBV

Así que el texto cifrado enviado a Ana nos queda:

"AULIAÑFLAOWUAHDZASKNALMJAHRHABBV".

Para descifrar, Ana separará en bloques de a 4 *y decodificará bloque a bloque. A cada bloque descifrado lo escribe con* 3*-dígitos en base* 28 *y luego lo pasa a un bloque formado por* 3 *caracteres.*

Hay que aclarar que lo expuesto aquí es solo una simplificación de la realidad. Por ejemplo vimos que los bloques del texto plano y los del texto cifrado nos quedaron de distinta longitud. Para evitar esto lo que se hace es agrandar el tamaño de los bloques, a los bloques del texto plano se le agrega "para rellenar" un número aleatorio, esto tiene la ventaja de que bloques asociados a números pequeños ya no son tan fáciles de descifrar a fuerza bruta. Otra cuestión es que nosotros utilizamos en general un sistema en base 28, pues fueron la cantidad de caracteres que usamos en nuestro texto, en la práctica suele usarse la base 128 (cantidad de caracteres del código ASCII) o 256 (cantidad de caracteres del código ASCII extendido).

Este método de cifrado en bloques (nos referimos al ECB) tiene la debilidad de que un espía podría buscar la manera de descifrar cada bloque por separado. Como descifrar cada bloque puede ser (y lo será en general) más fácil que descifrar el texto entero esto puede ser una desventaja.

Otros métodos de cifrado en bloques empleados son:

- CBC (Cipher-block chaining)
- PCBC (Propating cipher-block chaining)
- CFB (Cipher feedback)
- OFB (Output feedback)
- SIC (Segmented integer counter)

Para ver como funcionan dichos métodos recomendamos al lector ver por ejemplo la página web: `http://en.wikipedia.org/wiki/Block_cipher_modes_of_operation`

5.3.3. Ataques al RSA

Observemos que si podemos factorizar n, es decir hallar los primos p y q tales que $n = pq$ entonces podemos calcular $\varphi(n) = (p-1)(q-1)$ y usar el Algoritmo de Euclides para calcular d tal que:

$$de \equiv 1 \pmod{\varphi(n)}$$

y de esa forma poder descifrar todos los mensajes que le llegan a Ana. Vale resaltar que existe un algoritmo probabilístico que permite factorizar n conociendo la función de descifrado D (es decir, conociendo d). De forma que resulta equivalente encontrar la función de descifrado D a factorizar n.

Regresando a la parte matemática, si hubiese algún método efectivo para calcular $\varphi(n)$ entonces sería posible factorizar n en forma efectiva, esto queda como ejercicio para el lector.

Ejercicio 5.3.3. *Sea $n = pq$ con p y q primos. Conociendo $\varphi(n)$ describir un método para hallar los primos p y q.*

Otra debilidad del criptosistema puede surgir si no son bien elegidos los parámetros. Por ejemplo si p y q son primos cercanos entonces el Método de Fermat nos otorga un método efectivo de factorizar n.

5.3.4. Método de Fermat

Sea $n = pq$ con $p < q$ primos. Para $s = 1, 2, \ldots$ calculamos $n + s^2$ y paramos cuando nos dé un cuadrado perfecto, digamos $n + s^2 = t^2$ con $t \in \mathbb{Z}^+$. Entonces $p = t - s$ y $q = t + s$.

Para comenzar observemos que:

$$n = pq = \left(\frac{q+p}{2}\right)^2 - \left(\frac{q-p}{2}\right)^2$$

así que el algoritmo se detiene (y por lo tanto es efectivamente un algoritmo) en a lo sumo $s = \frac{q-p}{2}$ pasos.

Por otra parte sean s y t los enteros positivos que nos otorga el algoritmo. Observemos que $q-p < n-p < n-1$ así que por la observación previa $s < (n-1)/2$.

Como $n + s^2 = t^2$ entonces $t > s$ y $n = t^2 - s^2 = (t-s)(t+s)$. Si $t - s = 1$ entonces $t + s = n$, luego $t = (n+1)/2$ y $s = (n-1)/2$ lo cual es absurdo, por lo tanto $t - s$ y $t + s$ son factores de n mayores que 1 asi que $t - s = p$ y $t + s = q$.

Observemos que $q - p = 2s$, luego si $q - p$ es pequeño entonces s también lo es y el algoritmo termina rápido.

Ejemplo 5.3.4. *Sea $n = 9797$, utilizaremos el método de Fermat para factorizarlo. Si $s = 1$ entonces $n + s^2 = 9798$ y $\sqrt{9798} = 98{,}984847...$, por lo tanto $n + s^2$ no es un cuadrado. Si $s = 2$ entonces $n + s^2 = 9801$ y $\sqrt{9801} = 99$ y $n + 2^2 = 99^2$. Concluimos que dos factores de n son $99 - 2 = 97$ y $99 + 2 = 101$ que son primos, luego $n = 97 \cdot 101$.*

Para terminar, si volvemos a analizar detalladamente los pasos a seguir por Ana para la creación de su clave pública, nos topamos con un posible inconveniente en la primer parte.

Ana debe elegir dos primos grandes p y q para formar su número $n = pq$. El problema es que como dijimos, no se conoce ningún algoritmo realmente efectivo para factorizar números grandes en tiempo razonable, entonces ¿Cómo hace Ana para saber elegir los primos p y q que forman n? Ana podría tomar dos números al azar p y q y luego factorizarlos para ver si es primo, pero eso podría llevarle mucho tiempo (¡años o inclusive siglos!).

Afortunadamente es posible decidir si un número es primo o compuesto sin necesidad de encontrar sus factores. Por ejemplo con el Teorema de Fermat, supongamos que queremos ver si $n > 2$ es primo o no, entonces calculamos $2^{n-1} \pmod{n}$, si n fuese primo entonces $2^{n-1} \equiv 1 \pmod{n}$. Así que si esto no se verifica podemos asegurar que n es compuesto (Criterio de primalidad de Fermat) sin tener mayor información sobre su factorización (si diese 1 no podriamos afirmar que fuese primo, pero podríamos probar con otro a, $1 < a < n$, calculando $a^{n-1} \pmod{n}$).

Bibliografía

[1] Kraft, James; Washington, Lawrence *An introduction to number theory with cryptography.* Sep 6, 2013, Chapman and Hall/CRC

[2] Coutinho, Collier *Números Inteiros e Criptografia RSA* IMPA