Tema 6. Teoría de números elemental

6.0. Contenido y documentación

H6a_EstructurasAlgebraicas.pdf

H6b_TeoriaNumeros.pdf

H6c_Congruencias.pdf

6.1. Operaciones binarias

*Definición. Dado un grupo A y dos elementos $a, b \in A$. Definimos una **operación binaria** como aquella mediante la que, a partir de un par ordenado $(a, b) \in A \times A$, hacemos corresponder un número $c \in A$.*

En $\mathbb{N}$ (resp. $\mathbb{Z}$) podemos definir las operaciones binarias suma ($+$) y producto escalar ($\cdot$). Esto quiere decir que para cada par $(a, b) \in \mathbb{N} \times \mathbb{N}$ (resp. $\mathbb{Z} \times \mathbb{Z}$) tenemos un número $a + b \in \mathbb{N}$ (resp. $\mathbb{Z}$) para la operación suma, y otro $ab \in \mathbb{N}$ (resp. $\mathbb{Z}$) para la operación producto escalar.

Todas las operaciones binarias cumplen las siguientes propiedades:

- **Conmutativa**. $a + b = b + a$ y $ab = ba$.
- **Asociativa**. $(a + b) + c = a + (b + c)$.

- **Elemento neutro (suma)**. $\forall a \in \mathbb{Z}$ se tiene que $a + 0 = a$.
- **Elemento neutro (producto)**. $\forall a \in \mathbb{N}$ (res. $\mathbb{Z}$) se tiene que $a \cdot 1 = a$.
- **Elemento inverso (suma)**. $\forall a \in \mathbb{Z}, \exists a' \in \mathbb{Z} : a + a' = 0$, habitualmente, $a' = -a$.
- **Distributiva**. $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$.

Habitualmente, decimos que $\mathbb{Z}$ con las operaciones suma ($+$) y producto escalar ($\cdot$) es un **anillo conmutativo**.

6.1.1. Propiedades relacionadas con la divisibilidad

*Definición. Dados dos enteros $a, b \in \mathbb{Z}$ con $b \neq 0$. Decimos que a es **divisible** por b si $\exists q \in \mathbb{Z} : a = qb$*
.
Nota. También se aplica para $a, b \in \mathbb{N}$ si $q \in \mathbb{N}$.
Notación. $b|a$

> Teorema (**Algoritmo de la división**). Sean $a, b \in \mathbb{Z}$ dos enteros con $b \neq 0$. Entonces, $\exists q, r \in \mathbb{Z} : a = qb + r$, con q y r únicos y con $0 \leq r \leq |b|$.

Nota. Si $a, b \in \mathbb{N}$, entonces $q, r \in \mathbb{N} \cup \{0\}$.

6.1.2. Orden natural de $\mathbb{Z}$

En $\mathbb{Z}$ podemos definir el **orden natural** ($\leq$), un orden total que cumple las siguientes propiedades:

- **Principio del mínimo**. Para todo conjunto $A \subset \mathbb{Z}$, no vacío y acotado inferiormente, se cumple que A tiene un elemento mínimo.
- **Principio del máximo**. Para todo conjunto $A \subset \mathbb{Z}$, no vacío y acotado inferiormente, se cumple que A tiene un elemento máximo.

6.2. Divisibilidad

6.2.1. Máximo común divisor

*Definición. Dados tres enteros $a, b, r \in \mathbb{Z}$ con $a, b, r \neq 0$. Decimos que r es un **divisor común** de a y b si $r|a$ y $r|b$.*
Nota. Normalmente, solo consideramos los divisores positivos.

Usaremos con frecuencia que si $r|a$ y $r|b$, entonces $r \leq |a|$ y $r \leq |b|$, es decir, $r \leq \min\{|a|, |b|\}$. Por tanto, el conjunto de divisores comunes de a y b, $D = \{r \in \mathbb{N} : r|a \wedge r|b\}$ está acotado superiormente por $\min\{|a|, |b|\}$, siempre y cuando $D \neq \emptyset$. Luego, por el Principio del máximo, $\exists \max D$.

*Definición. Dados dos enteros $a, b \in \mathbb{Z}$ y el conjunto de sus divisores comunes $D = \{r \in \mathbb{N} : r|a \wedge r|b\}$. Decimos que r_0 es el **máximo común divisor** de a y b si $r_0 = \max D$.*
Notación. $\operatorname{mcd}(a, b)$.

6.2.2. Algoritmo de Euclides

> Lema 1. Sean $a, b, c, r \in \mathbb{Z}\backslash\{0\}$ cuatro enteros tales que $a = cb + r$. Entonces, $\operatorname{mcd}(a, b) = \operatorname{mcd}(b, r)$.

Demostración.
Sean $p = \text{mcd}\ (a, b)$ y $q = \text{mcd}\ (b, r)$.
Por una parte, $p|a$ y $p|b$, por lo que $\exists s, t \in \mathbb{Z} : a = sp \wedge b = tp$. Si suponemos que $r = a - cb = sp - ctp = p(s - ct)$, entonces $p|r$ y $p \leq \text{mcd}\ (b, r) = q$.
Por otra parte, $q|b$ y $q|r$, por lo que $\exists u, v \in \mathbb{Z} : b = uq \wedge r = vq$. Si suponemos que $a = cb + r = cuq + vq = q(cu + v)$, entonces $q|a$ y $q \leq \text{mcd}\ (a, b) = p$.
Luego, como $p \leq q$ y $p \geq q$, entonces $p = q \Leftrightarrow \text{mcd}\ (a, b) = \text{mcd}\ (b, r)$. □

> Lema 2. Sean $a, b \in \mathbb{Z}\backslash\{0\}$ tales que $b|a$. Entonces, $\text{mcd}\ (a, b) = |b|$.

Demostración.
Obviamente, $|b|$ divide a b y a, por lo que es divisor común de ambos. Cualquier otro divisor común tiene que ser menor que $\min\{|a|, |b|\} = |b|$, por lo que $|b|$ es el mayor de los divisores comunes de a y b. □

A partir de los dos lemas anteriores, podemos establecer un procedimiento que nos permite calcular el $\text{mcd}\ (a, b)$ para cualquier $a, b \in \mathbb{Z}\backslash\{0\}$. Este procedimiento se conoce como el **Algoritmo de Euclides**.

Caso general.
Suponemos cuatro enteros $a, b, c_0, r_1 \in \mathbb{Z}$ tales que $a = c_0 b + r_1$, con $0 \leq r_1 < |b|$.
- Si $r_1 = 0$, entonces $b|a$. Aplicando el Lema 2, $\text{mcd}\ (a, b) = |b|$.
- Si $r_1 \neq 0$, entonces, aplicamos el Lema 1 para deducir que $\text{mcd}\ (a, b) = \text{mcd}\ (b, r_1)$. Así, podemos decir que $b = c_1 r_1 + r_2$ con $0 \leq r_2 < |r_1|$ y volver a empezar.

6.3. Números primos

Definición. Dados dos enteros $a, b \in \mathbb{Z}\backslash\{0\}$. Decimos que a y b son ***coprimos*** *si* $\text{mcd}\ (a, b) = 1$.

Ejemplo 1. Sea $k \in \mathbb{N}$ arbitrario. Demostrar que $7k + 3$ y $5k + 2$ son coprimos.
Tenemos que demostrar que $\text{mcd}\ (7k + 3, 5k + 2) = 1$. Aplicamos el Algoritmo de Euclides, de forma que $7k + 3 = (5k + 2) + 2k + 1$, por lo que $\text{mcd}\ (7k + 3, 5k + 2) = \text{mcd}\ (5k + 2, 2k + 1)$. Seguimos aplicando este procedimiento, de forma que $5k + 2 = 2(2k + 1) + k$, $2k + 1 = 2(k) + 1$ y $k = k(1)$. Luego, concluimos que $\text{mcd}\ (7k + 3, 5k + 2) = \text{mcd}\ (k, 1) = 1$, por lo que $7k + 3$ y $5k + 2$ son coprimos.

6.4. Aplicaciones del Algoritmo de Euclides

> Teorema (Identidad de Bézout). Sea $a, b, m \in \mathbb{Z}\backslash\{0\}$ tres enteros tales que $m = \text{mcd}\ (a, b) > 0$. Entonces, $\exists u, v \in \mathbb{Z} : m = ua + vb$.

Demostración.
Por el Algoritmo de Euclides, tenemos que $a = c_0 b + r_1$, $b = c_1 r_1 + r_2 \ldots$ de forma que $m = \text{mcd}\ (a, b) = r_{n-1}$.
Si despejamos los restos de las expresiones anteriores, obtenemos que $r_{n-1} = r_{n-3} - c_{n-2} r_{n-2} = \ldots = ua + vb$. □

Ejemplo 2. Encontrar $u, v \in \mathbb{Z}$ tales que $6 = 102u + 18v$.
Aplicamos el Algoritmo de Euclides, de forma que $102 = 5 \cdot 18 + 12$, $18 = 12 + 6$ y $12 = 2 \cdot 6$. Así, tenemos que $6 = 18 - 12 = 18 - (102 - 5 \cdot 18) = -102 + 6 \cdot 18$. Luego, $u = -1$ y $v = 6$.

> Corolario. Sean $a, b \in \mathbb{Z} \backslash \{0\}$ dos enteros. Entonces, a y b son coprimos si y solo si $\exists u, v \in \mathbb{Z} : ua + vb = 1$.

Demostración.
$\Rightarrow$) Es trivial.
$\Leftarrow$) Si $m|a$ y $m|b$, entonces $\exists k, l \in \mathbb{Z} : a = km$ y $b = lm$. Luego $ua + vb = ukm + vlm = m(uk + vl)$, de forma que $m|(ua + vb) = 1$. Si $m|1$, entonces $m \in \{-1, 1\}$ y como $m > 0$, pues $m = 1$. Luego, $\text{mcd}\ (a, b) = 1$. □

> Lema de Euclides. Sean $a, b, c \in \mathbb{Z}$ tres enteros tales que $a|bc \wedge \text{mcd}\ (a, b) = 1$. Entonces, $a|c$.

Demostración.
Sabemos que $\text{mcd}\ (a, b) = 1$, entonces $\exists x, y \in \mathbb{Z} : ax + by = 1$, de forma que $acx + bcy = c$. Además, sabemos que $a|bc$, por lo que $a|bcy$ y $a|acx$. Luego, $a|(acx + bcy) = c \Rightarrow a|c$. □

6.5. Ecuaciones Diofánticas

Definición. Dados tres enteros $a, b, c \in \mathbb{Z}$. Llamamos ***ecuación diofántica*** *a aquella de la forma $ax + by = c$.*
Nota. Nos interesa encontrar sus soluciones $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

> Proposición. Sea $a, b, c, d \in \mathbb{Z}$ cuatro enteros tales que $\text{mcd}\ (a, b) = d$. Entonces, la ecuación diofántica $ax + by = c$ tiene soluciones enteras $\text{mcd}\ (x, y)$ si y solo si $d|c$.

Demostración.
$\Rightarrow$) Suponemos que existen soluciones enteras, de forma que $\exists u, v \in \mathbb{Z} : au + bv = c$. Como $d|a$ y $d|b$, entonces $\exists p, q \in \mathbb{Z} : a = pd \wedge b = qd$, de forma que $c = au + bv = pdu + qdv = d(pu + qv)$. Luego, $d|c$.
$\Leftarrow$) Si $d = \text{mcd}\ (a, b)|c$, entonces $\exists m \in \mathbb{Z} : c = md$. Por la Identidad de Bézout, $\exists u, v \in \mathbb{Z} : au + bv = d$, por lo que $c = md = mua + mvb$. Si ponemos que $x = mu$ e $y = mv$, tenemos que (mu, mv) es una solución entera de $ax + by = c$. □

> Teorema. Sean $a, b, c \in \mathbb{Z}$ tres enteros, $d = \text{mcd}\ (a, b)$ y $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ una solución particular de la ecuación diofántica $ax + by = c$. Entonces, cualquier solución de la misma es de la forma $(x, y) = \begin{cases} x = x_0 + \frac{b}{d}n \\ y = y_0 - \frac{a}{d}n \end{cases}, n \in \mathbb{Z}$.

Demostración.
Primero, consideramos $x = x_0 + \frac{b}{d}n$ e $y = y_0 - \frac{a}{d}n$ y comprobamos que $ax + by = a\left(x_0 + \frac{b}{d}n\right) + b\left(y_0 - \frac{a}{d}n\right) = ax_0 + \frac{ab}{d}n + by_0 - \frac{ab}{d}n = ax_0 + by_0 = c$. Por lo que efectivamente, (x, y) es solución.
Después, consideramos una solución arbitraria (x, y), de forma que $ax + by = c$ y $ax_0 + by_o = c$, por lo que $a(x - x_0) + b(y - y_0) = 0$ y $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$.
Así, $\frac{b}{d}|\frac{a}{d}(x - x_0) \Rightarrow \frac{b}{d}|(x - x_0)$, ya que $\text{mcd}\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. De forma que $x - x_0 = n\frac{b}{d} \Rightarrow x = x_0 + \frac{b}{d}n$, con $n \in \mathbb{Z}$.
De igual forma, $\frac{a}{d}|\frac{b}{d}(y_0 - y) \Rightarrow \frac{a}{d}|(y_0 - y)$, e $y_0 - y = n\frac{a}{d} \Rightarrow y = y_0 - \frac{a}{d}n$, con $n \in \mathbb{Z}$. $\square$

6.6. Mínimo común múltiplo

*Definición. Dados tres enteros $a, b, r \in \mathbb{Z}$ con $a, b, r \neq 0$. Decimos que r es un **múltiplo común** de a y b si $a|r$ y $b|r$.*
Nota. Normalmente, solo consideramos los múltiplos positivos.

Definimos el conjunto de múltiplos comunes de a y b como $M = \{r \in \mathbb{N} : a|r \wedge b|r\} = \{r \in \mathbb{N} : \exists k, l \in \mathbb{Z} \text{ con } r = ka = lb\}$. El conjunto M siempre es distinto del vacío, ya que $|ab| \in M$.

*Definición. Dados dos enteros $a, b \in \mathbb{Z}\backslash\{0\}$ y el conjunto de sus múltiplos comunes $M = \{r \in \mathbb{N} : a|r \wedge b|r\}$. Decimos que r_0 es el **mínimo común múltiplo** de a y b si $r_0 = \min M$.*
Notación. $\text{mcm}\ (a, b)$

6.7. Teorema Fundamental de la Aritmética

> **Teorema Fundamental de la Aritmética**. Para todo número natural $n \in \mathbb{N}$, existen una serie de números primos $p_1, p_1, ..., p_s$ y de números naturales $\alpha_1, \alpha_2, ..., \alpha_s \in \mathbb{N}$ tale que $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_s^{\alpha_s}$. Esta factorización es única salvo orden.

Usando el Teorema Fundamental de la Aritmética, podemos factorizar dos números $a, b \in \mathbb{N}$ como productos de los mismos primos (admitiendo 0 como exponente). De forma que $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_s^{\alpha_s}$ y $b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_s^{\beta_s}$, con $\alpha_i, \beta_i \in \mathbb{N} \cup \{0\}, \forall i$. Entonces, resulta que:
- $\text{mcd}\ (a, b) = p_1^{\min\{\alpha_1, \beta_1\}} \cdot p_2^{\min\{\alpha_2, \beta_2\}} \cdot ... \cdot p_s^{\min\{\alpha_s, \beta_s\}}$.
- $\text{mcm}\ (a, b) = p_1^{\max\{\alpha_1, \beta_1\}} \cdot p_2^{\max\{\alpha_2, \beta_2\}} \cdot ... \cdot p_s^{\max\{\alpha_s, \beta_s\}}$.

6.8. Congruencias

*Definición. Sean $a, b \in \mathbb{Z}$ y $n \in \mathbb{N}$ con $n > 1$. Decimos que a es **congruente con** b **módulo** n si $n|(b - a)$.*
Notación. $a \equiv b\ (n)$.

En $\mathbb{Z}$ podemos definir el conjunto cociente de la congruencia como $\mathbb{Z}/_{\equiv(n)} = \mathbb{Z}/_{n\mathbb{Z}} = \mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$.

*Definición. Dado un número natural $n \in \mathbb{N}$ con $n > 1$. Definimos un **sistema completo de restos módulo** n como un conjunto de n enteros donde cada uno es un representantes de cada una de las clases $\overline{0}, \overline{1}, ..., \overline{n-1}$.*

> Proposición. Sean $n \in \mathbb{N}\backslash\{1\}$ y $a \in \mathbb{Z}$ tales que $\text{mcd}\ (a, n) = 1$; y $r_1, r_2, ..., r_n$ un sistema completo de restos módulo n. Entonces, $ar_1, ar_2, ..., ar_n$ también lo es.

Demostración.
Suponemos que $\exists i, j \in \{1, 2, ..., n\} : i \neq j \wedge \overline{ar_i} = \overline{ar_j}$. Entonces, $n|(ar_1 - ar_j) \Rightarrow n|a(r_1 - r_j)$. Pero sabemos que $\text{mcd}\ (n, a) = 1$, luego, $n|(r_i - r_j) \Rightarrow \overline{r_i} = \overline{r_j}$, lo que nos lleva a una contradicción. □

6.8.1. Operaciones y congruencias

Para que una operación $(*)$ con clases de equivalencia esté bien definida, se necesita que dicha operación cumple que $\overline{a} * \overline{b} = \overline{a * b}$. En $\mathbb{Z}_n$ esto se cumple para las operaciones suma $(+)$ y producto escalar $(\cdot)$.

> Teorema. Sean $a, b, c, d \in \mathbb{Z}$ cuatro enteros y $n \in \mathbb{N}$ un natural con $n > 1$, tales que $\overline{a} = \overline{c}\ (n)$ y $\overline{b} = \overline{d}\ (n)$. Entonces, $\overline{a + b} = \overline{c + d}\ (n)$ y $\overline{ab} = \overline{cd}\ (n)$.

Demostración.
Si $\overline{a} = \overline{c}\ (n)$ y $\overline{b} = \overline{d}\ (n)$, entonces $\exists r, s \in \mathbb{Z} : a - c = rn \wedge b - d = sn$.
- $(a - c) + (b - d) = rn + sn \Leftrightarrow (a + b) - (c + d) = n(r + s) \Leftrightarrow n|((a + b) - (c + d))$. Luego, $\overline{a + b} = \overline{c + d}\ (n)$.
- $b(a - c) + c(b - d) = brn + csn \Leftrightarrow ab - bc + bc - cd = n(br + cs) \Leftrightarrow n|(ab - cd)$. Luego, $\overline{ab} = \overline{cd}\ (n)$.

> Corolario. Sean $a, c \in \mathbb{Z}$ dos enteros y $n \in \mathbb{N}$ un natural con $n > 1$ tales que $\overline{a} = \overline{c}\ (n)$. Entonces, $\overline{ma} = \overline{mc}\ (n)$ y $\overline{a^m} = \overline{c^m}\ (n)$, para todo $m \in \mathbb{N}$.

6.8.2. Teorema de Fermat

> Teorema Pequeño de Fermat. Sea p un número primo y $a \in \mathbb{N}$ un natural tales que $p \nmid a$. Entonces, $a^{p-1} \equiv 1\ (p)$.

Demostración.
Como p es primo y $p \nmid a$, entonces $\text{mcd}\ (p, a) = 1$. De esta forma, $\{0, 1, ..., p - 1\}$ es un sistma completo de restos módulo p y $\{0, a, ..., a(p - 1)\}$ también lo es.
Por lo tanto, cada $i \in \{1, 2, ..., p - 1\}$ es congruente con $ja\ (p)$ para algún $j \in \{1, 2, ..., p - 1\}$. Si multiplicamos todos los i, j, tenemos que $1 \cdot 2 \cdot ... \cdot p - 1 \equiv a \cdot 2a \cdot ... \cdot a^{p-1}(p - 1)\ (p) \Leftrightarrow (p - 1)! \equiv a^{p-1}(p - 1)!\ (p)$, de forma que $p|(a^{p-1}(p - 1)! - (p - 1)!) = ((p - 1)!(a^{p-1} - 1))$. Luego, $\text{mcd}\ (p, (p - 1)!) = 1$, por lo que $p|(a^{p-1} - a) \Rightarrow a^{p-1} \equiv 1\ (p)$. □

> Corolario. Sea p un número primo y $a \in \mathbb{N}$ un natural tales que $p \nmid a$. Entonces, $a^p \equiv a \ (p)$ o, equivalentemente, $p|(a^p - p)$.

6.9. Propiedades algebraicas de $\mathbb{Z}_n$

Sea $\mathbb{Z}_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$ el conjunto cociente de $\mathbb{Z}$ respecto a la relación de equivalencia $\equiv \ (n)$. Podemos afirmar que $\mathbb{Z}_n$ es un **anillo conmutativo**, ya que las operaciones suma ($+$) y producto escalar ($\cdot$) cumples las siguientes propiedades:

- **Conmutativa**. $\overline{a} + \overline{b} = \overline{b} + \overline{a}$ y $\overline{a}\overline{b} = \overline{b}\overline{a}$.
- **Asociativa**. $(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c})$ y $(\overline{a}\overline{b})\overline{c} = \overline{a}(\overline{b}\overline{c})$.
- **Distributiva**. $\overline{a}(\overline{b} + \overline{c}) = \overline{a}\overline{b} + \overline{a}\overline{c}$.
- **Elemento neutro**. $\overline{a} + \overline{0} = \overline{a}$ y $\overline{a} \cdot \overline{1} = \overline{a}$.

6.9.1. Propiedad del inverso multiplicativo

*Definición. Dados p un número primo y $\overline{a} \in \mathbb{Z}_p \backslash \{\overline{0}\}$ una clase de equivalencia. Definimos el **inverso multiplicativo** de $\overline{a}$ en $\mathbb{Z}_p \backslash \{\overline{0}\}$ como un elemento $\overline{b} \in \mathbb{Z}_p \backslash \{\overline{0}\}$ tal que $\overline{a}\overline{b} = \overline{b}\overline{a} = \overline{1} \ (p)$.*

> Proposición. Sea p un número primo. Entonces, $\forall \overline{a} \in \mathbb{Z}_p \backslash \{0\}$ existe un único $\overline{b} \in \mathbb{Z}_p \backslash \{\overline{0}\}$ tal que $\overline{b}$ es el inverso multiplicativo de $\overline{a}$.

Demostración.
Si p es un número primo, entonces, $\text{mcd} \ (a, p) = 1$; y, por la Identidad de Bézout, $\exists b, c \in \mathbb{Z} : ab + pc = 1$, de forma que $pc = 1 - ab$ y $p|(1 - ab) \Leftrightarrow ab \equiv 1 \ (p)$. Quedando demostrada la existencia de $\overline{b}$.
Ahora suponemos que existen dos números $b, c \in \mathbb{Z}$ tales que $\overline{a}\overline{b} = \overline{1}$ y $\overline{ac} = \overline{1}$, es decir, $ab \equiv 1 \ (p)$ y $ac \equiv 1 \ (p)$. De esta forma, $ab - ac \equiv 0 \ (p)$ y $p|(ab - ac) = a(b - c)$. Sabemos que $p \nmid a$, por lo que $p|(b - c) \Leftrightarrow b \equiv c \ (p)$ y $\overline{b} = \overline{c}$. Quedando demostrada la unicidad de $\overline{b}$. □

---

*Definición. Un **cuerpo** es un conjunto, C, cerrado respecto a las operaciones suma y producto escalar, es decir, $\forall a, b \in C$ se tiene que $a + b, a \cdot b \in C$.*

6.10. Ecuaciones con congruencias

*Definición. Dados dos enteros $a, b \in \mathbb{Z}$ y un natural $n \in \mathbb{N} \backslash \{1\}$. Definimos una **ecuación con congruencias** como aquella de la forma $ax = b \ (n)$.*

> Teorema. Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N} \backslash \{1\}$ y $\text{mcd} \ (a, n) = \text{mcd} \ (a, -n) = d$. Entonces:
>
> - Si $d \nmid b$, la ecuación $ax \equiv b \ (n)$ no tiene soluciones en $\mathbb{Z}$.
> - Si $d|b$, la ecuación $ax \equiv b \ (n)$ tiene en $\mathbb{Z}$ exactamente d soluciones no congruentes entre sí módulo n.

Demostración.
- Si $d \nmid b$, entonces no existe ningún par $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ que sea resultado de la ecuación diofántica $ax + ny = b$. Por lo que no existe solución para la ecuación $ax \equiv b\ (n)$.
- Si $d|b$, entonces $ax + ny = b$ tiene soluciónes enteras (x, y) definida como $x = x_0 + \frac{n}{d}k$ e $y = y_0 - \frac{a}{d}k$, con $k \in \mathbb{Z}$; siendo (x_0, y_0) una solución particular de $ax - ny = b$.
Suponemos dos soluciones $x_1 = x_0 + \frac{n}{d}k_1$ y $x_2 = x_0 + \frac{n}{d}k_2$, con $k_1, k_2 \in \mathbb{Z}$, de forma que $x_1 \equiv x_2\ (n)$. De esta forma, $n|(x_1 - x_2) = \left(x_0 + \frac{n}{d}k_1 - x_0 - \frac{n}{d}k_2\right) = \frac{n}{d}(k_1 - k_2)$. Como $n|\frac{n}{d}$, entonces $n|(k_1 - k_2) \Leftrightarrow k_1 \equiv k_2\ (d)$. □

6.10.1. Teorema Chino del Resto

> Teorema Chino del Resto. Sean $a_1, a_2, ..., a_k \in \mathbb{Z}$ una serie de enteros y $m_1, m_2, ..., m_k \in \mathbb{N}$ una serie de naturales coprimos dos a dos. Entonces, el sistema de congruencias $\begin{cases} x \equiv a_1\ (m_1) \\ x \equiv a_2\ (m_2) \\ \dots \\ x \equiv a_k\ (m_k) \end{cases}$ tiene solución única módulo $M = m_1 \cdot m_2 \cdot ... \cdot m_k$.

Demotración.
- Existencia. Para $j \in \{1, 2, ..., k\}$, definimos M_j como $M_j = \frac{M}{m_j} = m_1 \cdot m_2 \cdot ... \cdot m_{j-1} \cdot m_{j+1} \cdot m_k$. Por hipótesis, $i \neq j \Rightarrow \text{mcd}\ (m_i, m_j) = 1$, por lo que $\text{mcd}\ (m_j, M_j) = 1$. Así, $\overline{M}_j$ tiene un único inverso en $\mathbb{Z}_{mj}$, $\overline{b}_j$ tal que $M_j b_j \equiv 1\ (m_j)$.

Para lo valores de $a_1, a_2, ..., a_k$ dados y los $b_1, b_2, ..., b_k$ obtenidos, si $x = \sum_{i=1}^{k} a_i M_i b_i$. Entonces, $\forall j \in \{1, 2, ..., k\}$ tenemos que $a_j M_j b_j \equiv a_j\ (m_j)$ y $M_i \equiv 0\ (m_j)$, para $i \neq j$. De forma que $a_i M_i b_i \equiv 0\ (m_j)$ y $x \equiv a_j\ (m_j)$, con $j = 1, 2, ..., k$.
- Unicidad. Suponemos que existen dos soluciones x e y para el sistema. Por hipótesis, sabemos que $\forall j \in \{1, 2, ..., k\}$ tenemos que $x \equiv a_j\ (m_j) \wedge y \equiv a_j\ (m_j)$, de forma que $x - y \equiv 0\ (m_j) \Leftrightarrow m_j|(x - y)$. Así, tenemos que $\text{mcm}\ (m_1, ..., m_k)|(x - y) \Rightarrow M|(x - y)$, ya que los m_i son coprimos dos a dos. Luego, $x \equiv y\ (M)$, de forma que $\overline{x} = \overline{y}$. Llegando a una contradicción. □

6.11. Función de Euler

*Definición. Dado un número natural $n \in \mathbb{N}$. Definimos la **función de Euler** $\phi : \mathbb{N} \to \mathbb{N}$ como $\phi(n) = |\{k \in \mathbb{N} : 1 \leq k \leq n \text{ con } \text{mcd}\ (n, k) = 1\}|$. Es decir, la función determina el cardinal del conjunto de números coprimos menores o iguales que n.*

Algunas de las principales propiedades de la función de Euler son:

1. Sean $n, m \in \mathbb{N}$ dos naturales con $\text{mcd}\ (n, m) = 1$. Entonces, $\phi(nm) = \phi(n) \cdot \phi(m)$.
2. Sea $k \in \mathbb{N}$ un natural y p un número primo. Entonces, $\phi(p^k) = p^{k-1}(p - 1)$.

3. Sea $n \in \mathbb{N}$ un natural. Entonces, $\phi(n) = n \cdot \prod_{i=1}^{j} \left(1 - \frac{1}{p_i}\right)$, siendo p_i un número primo tal que $p_i | n$.

> **Teorema de Euler**. Sean $a, n \in \mathbb{N}$ dos naturales con $\text{mcd}\,(a, n) = 1$. Entonces, $a^{\phi(n)} \equiv 1\ (n)$.

Ejemplo 3. Encontrar los último dos dígitos del número 123^{442}.
Tenemos que encontrar la solución de la ecuación $123^{442} \equiv x\ (100)$.
Primero, vemos que $100 = 2^2 \cdot 5^2$, de forma que $\phi(100) = 100 \cdot \left(1 - \frac{1}{2}\right) \cdot \left(1 - \frac{1}{5}\right) = 40$.
A continuación, simplificamos la congruencia: $123 = 100 + 23 \Rightarrow 123 \equiv 23\ (100)$, de forma que $123^{442} \equiv 23^{442}\ (100)$. Vemos que $442 = 11 \cdot 40 + 2$, de forma que $(23^{11})^{40} \cdot 23^2 \equiv 23^{442}$. Por el Teorema de Euler, sabemos que $(23^{11})^{40} \equiv 1\ (100)$, luego $23^{442} \equiv 23^2\ (100)$. Por último, tenemos que $23^2 = 529 = 5 \cdot 100 + 29$, por lo que $123^{442} \equiv 29\ (100)$; y las últimas dos cifras de 123^{442} son 29.

> Lema. Sean $x, y \in \mathbb{Z}$ dos enterio y $n \in \mathbb{N}\backslash\{1\}$ un natural tales que $x \equiv y\ (n)$. Entonces, $\text{mcd}\,(x, n) = \text{mcd}\,(y, n)$.

Demostración.
Si $x \equiv y\ (n)$, entonces $\exists k \in \mathbb{Z} : x - y = kn$, es decir, $y = x - kn$. Es evidente, que, siendo $m = \text{mcd}\,(x, n)$, $m|x \wedge m|n$, por lo que $m|(x - kn) = y$. Por lo tanto, como $m|n \wedge m|y$, sabemos que $\text{mcd}\,(x, n)|\text{mcd}\,(y, n)$.
De la misma forma, obtenemos que $\text{mcd}\,(y, n)|\text{mcd}\,(x, n)$. Luego, $\text{mcd}\,(x, n) = \text{mcd}\,(y, n)$. □

6.11.2. Sistema reducido de restos

*Definición. Sea $n \in \mathbb{N}\backslash\{1\}$. Definimos un **sistema reducido de restos módulo** n como el conjunto de enteros $\{r_i : i \in I\} \subset \mathbb{Z}$ tal que:*
- $\forall x \in \mathbb{Z}$ con $\text{mcd}\,(x, n) = 1$, existe un $i \in I$ tal que $x \equiv r_i\ (n)$.
- para todo $i, j \in I$ con $i \neq j$, se tiene que $r_i \not\equiv r_j\ (n)$.
- $\forall i \in I$ se tiene que $\text{mcd}\,(r_i, n) = 1$.
Nota. Es evidente que $|I| \leq n$ y que un sistema reducido de restos se obtiene de un sistema completo, quitando los r_i que no son coprimos con n.

De esta forma, el cardinal de un sistema reducido de restos módulo n viene definido por la función de Euler como $\phi(n)$.

> Proposición. Sean $n \in \mathbb{N}\backslash\{1\}$ y $a \in \mathbb{Z}$ tales que $\text{mcd}\,(a, n) = 1$; y $r_1, r_2, ..., r_n$ un sistema reducido de restos módulo n. Entonces, $ar_1, ar_2, ..., ar_n$ también lo es.