TEMA IV: INTRODUCCIÓN A LA TEORÍA DE NÚMEROS: ARITMETICA MODULAR.

OBJETIVOS GENERALES

1. **Conocer los conjuntos de números naturales y números enteros, sus propiedades y operaciones.**
2. **Entender ambos como ejemplos de conjuntos discretos.**
2. **Conocer nociones básicas de aritmética modular.**

OBJETIVOS ESPECÍFICOS

- ✓ **Comprender las dos formas de definición del conjunto de los números naturales.**
- ✓ **Conocer las propiedades básicas de los números naturales y sus operaciones.**
- ✓ **Conocer las propiedades básicas de los números enteros y sus operaciones.**
- ✓ **Conocer la relación de divisibilidad en el conjunto de los números enteros.**
- ✓ **Reconocer la importancia del teorema fundamental de la aritmética.**
- ✓ **Saber calcular el máximo común divisor y el mínimo común múltiplo de dos enteros.**
- ✓ **Saber usar el algoritmo de la división entre números enteros.**

OBJETIVOS ESPECÍFICOS

- ✓ **Saber obtener la identidad de Bezout de dos números enteros.**
- ✓ **Saber calcular el máximo común divisor de dos números enteros mediante el algoritmo de Euclides.**
- ✓ **Saber calcular, si existen, todas las soluciones enteras de una ecuación del tipo a.x + b.y = c donde a, b y c son número enteros.**
- ✓ **Conocer el concepto de congruencia.**
- ✓ **Conocer los conjuntos de las clases de restos módulo n.**
- ✓ **Realizar con soltura operaciones de la aritmética modular (aritmética en $\mathbb{Z}_n$).**
- ✓ **Saber cuando un elemento en $\mathbb{Z}_n$ es una unidad y saber calcular el inverso de dicho elemento.**

OBJETIVOS ESPECÍFICOS

- ✓ **Conocer el concepto de divisor de cero y saber cuando un elemento es divisor de cero en $\mathbb{Z}_n$.**
- ✓ **Resolver congruencias lineales y sistemas de congruencias.**
- ✓ **Conocer el concepto de sistema de numeración.**
- ✓ **Saber pasar un número de cualquier sistema de numeración a otro con distinta base.**

BIBLIOGRAFÍA

- **"Matemática discreta para la computación". M.A. García-Muñoz. Servicio de Publ. Univ. Jaén. 2010.**
- "Matemática discreta y combinatoria". R. P. Grimaldi. Addison-Wesley Iberoamericana, 1989.
- "Matemática discreta", F. García Merayo. Paraninfo, 2001.
- "Problemas resueltos de Matemática discreta", F. García Merayo y otros. Paraninfo, 2003.
- "Álgebra abstracta aplicada". A. Vera López y otros autores. 1992
- "201 problemas resueltos de Matemática Discreta". V. Meavilla Seguí. Universidad Zaragoza, 2000.
- "Matemática Discreta y sus aplicaciones". K. H. Rosen. McGraw-Hill, 2004.

DESARROLLO TEÓRICO

IV.1 Introducción.
IV.2 Números naturales y enteros.
IV.3 Divisibilidad en el conjunto de los números enteros
IV.4 Congruencia. Sistemas de congruencias.
IV.5 Sistemas de numeración.

1. INTRODUCCIÓN

Tanto el conjunto de los números naturales como el conjunto de los números enteros son conjuntos conocidos. Todos estamos familiarizados con dichos conjuntos y con sus operaciones:

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

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

La parte de la matemática discreta que trata de los números enteros y sus propiedades recibe el nombre de **teoría de números**. Esta teoría es parte importante de la aritmética, el álgebra y la geometría, y el primer matemático que la creo como ciencia algebraica fue Gauss (el príncipe de las matemática) al publicar en 1801 su obra "Disquisitiones Aritmeticae".

Se dice que Gauss describió las Matemáticas como la "Reina de las ciencias" y la teoría de números como la "Reina de las Matemáticas."

Lo primero que haremos en este tema es introducir de forma rigurosa estos conjuntos. Como veremos existe varias formas de introducirlos y nosotros elegiremos la **forma axiomática** que consiste en caracterizar el conjunto de los números naturales por algunas de sus propiedades que se imponen como axiomas, de manera que cualquier otra propiedad se deduce (usando las reglas de la lógica) de estos axiomas. Esta forma de introducir los números naturales se debe a Peano. Una vez definido el conjunto de los números naturales podremos construir el conjunto de los enteros como el conjunto que, en cierto sentido, completa al conjunto de los números naturales.

En tales conjuntos tenemos definidas operaciones por todos conocidas, la suma y la multiplicación, y de las propiedades que satisfagan estas operaciones deduciremos la **estructura algebraica** de dichos conjuntos. El estudio de las estructuras algebraicas es importante y abre todo un campo de las matemáticas conocido como **Álgebra**. El Álgebra se basa en el estudio de la estructura profunda de los conjuntos dotados de operaciones y permite describir sus propiedades y estudiar características generales (podríamos decir que el Álgebra estudia las reglas del juego).

La noción de divisibilidad de la que se deriva el concepto de número primo es de gran importancia en criptografía o estudio de los mensajes secretos. Aunque en le anillo de los números enteros no se puede dividir, ya que los cocientes no son enteros, si se puede hacer una división entera, obteniendo un cociente y un resto. Precisamente basada en estos restos se encuentra la **aritmética modular**, utilizada ampliamente en la ciencia de la computación y particularmente en encriptación de mensajes.

Algunos resultados de teoría elemental de números se han utilizado para diseñar algoritmos de cifrado que son muy seguros. Las propiedades particulares de "clave pública" de estos algoritmos los hacen ideales para el cifrado de datos enviados a través de Internet y, de este modo, permiten que el comercio electrónico sea viable.

La teoría de números estudia las propiedades de la divisibilidad de los números enteros, que desde antiguo han fascinado al hombre por considerarlos mágicos. Así Fermat conjeturó, y después Lagrange demostró, que cualquier número natural puede expresarse como la suma de cuatro cuadrados. Otro ejemplo de esta magia es los números triangulares 1, 3, 6, 10, 15,..., números que representados mediante puntos forman triángulos equiláteros. En general, el n-ésimo viene dado por (n(n+1))/2.

2. NÚMEROS NATURALES Y ENTEROS

El conjunto de los números naturales se puede construir de dos formas:

a) De forma **axiomática**: establecemos una serie de axiomas y a partir de ellos probamos una serie de teoremas que son sus propiedades (Peano, Hilbert).

b) Como un conjunto de clases de equivalencia de la relación de cardinabilidad entre conjuntos (Cantor, Frege, Rusell).

Elegimos la axiomática que consiste en caracterizar el conjunto de los números naturales mediante algunas propiedades que se imponen como axiomas, de forma que cualquier otra propiedad se prueba a partir de estos axiomas usando reglas lógicas.

Sea $\mathbb{N}$ el conjunto formado por un número infinito de objetos indefinidos que llamamos **números naturales:**

$$\mathbb{N} = \{0, 1, 2, 3, 4,...\}$$

Axioma 1: El número 0 es natural ($\mathbb{N} \neq \emptyset$).

Axioma 2: Para todo elemento $n \in \mathbb{N}$, se tiene que $n + 1 \in \mathbb{N}$.

Axioma 3 (Axioma de inducción): Si A es un subconjunto no vacío de $\mathbb{N}$, tal que:

i) $0 \in A$,

ii) Si $n \in A$, entonces $n + 1 \in A$,

entonces $A = \mathbb{N}$.

Estos números son realmente "naturales", en el sentido de que surgen cuando contamos conjuntos finitos.

La **suma de números naturales** es una aplicación

$$+: \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},$$

de manera que para cada par de números naturales n, m existe un único número natural n + m. Esta operación se define por inducción mediante las reglas:

i) $n + 0 = n$, $\forall n \in \mathbb{N}$,

ii) $n + (m + 1) = (n + m) + 1$, $\forall n, m \in \mathbb{N}$.

Proposición 4.1. La suma de números naturales satisface:

i) **Elemento neutro**:
Existe $0 \in \mathbb{N}$ tal que $0 + n = n = n + 0$, $\forall n \in \mathbb{N}$.

ii) **Conmutativa**, $n + m = m + n$, $\forall n, m \in \mathbb{N}$.

iii) **Asociativa**, $(n + m) + p = n + (m + p)$, $\forall n, m, p \in \mathbb{N}$.

iv) **Cancelativa**,
Dados $n, m, p \in \mathbb{N}$, si $n + m = n + p$, entonces $m = p$.

El **producto de números naturales** es una aplicación

$$\cdot : \mathbb{N} \times \mathbb{N} \longrightarrow \mathbb{N},$$

de manera que para cada par de números naturales n, m existe un único número natural $n \cdot m$. Esta operación de nuevo se define de forma inductiva mediante:

i) $n \cdot 0 = 0$, $\forall n \in \mathbb{N}$,

ii) $n \cdot (m + 1) = (n \cdot m) + n$, $\forall n, m \in \mathbb{N}$.

Proposición 4.2. El producto de números naturales satisface:

i) **Elemento cero**: $\exists 0 \in \mathbb{N}$ tal que $0 \cdot n = 0 = n \cdot 0$, $\forall n \in \mathbb{N}$.

ii) **Elemento neutro**: $\exists 1 \in \mathbb{N}$ tal que $1 \cdot n = n = n \cdot 1$, $\forall n \in \mathbb{N}$.

iii) **Conmutativa**, $n \cdot m = m \cdot n$, $\forall n, m \in \mathbb{N}$.

iv) **Asociativa**, $(n \cdot m) \cdot p = n \cdot (m \cdot p)$, $\forall n, m, p \in \mathbb{N}$.

v) **Cancelativa**,
Dados $n, m, p \in \mathbb{N}$, si $n \cdot m = n \cdot p$ y $n \neq 0$, entonces $m = p$.

vi) **Distributivas**, $n \cdot (m + p) = n \cdot m + n \cdot p$, $\forall n, m, p \in \mathbb{N}$.

Proposición 4.3. El conjunto de los números naturales $\mathbb{N}$ es un conjunto ordenado por la relación binaria

$n \leq m$ si y solo si $\exists a \in \mathbb{N}$ tal que $m = n + a$.

Proposición 4.4. $\mathbb{N}$ respecto al orden anterior es:

i) un conjunto totalmente ordenado.

ii) un conjunto bien ordenado.

El conjunto de los números enteros surge para resolver problemas que en $\mathbb{N}$ no tienen solución. Por ejemplo, la ecuación $x + b = a$ cuando $a < b$ no tiene solución en $\mathbb{N}$, ya que $a – b$ no tiene sentido en dicho conjunto.

La construcción del conjunto de los números enteros consiste en encontrar un conjunto dotado de una operación interna (+) inducida por la correspondiente operación interna suma en $\mathbb{N}$, y en el que todo elemento tenga simétrico respecto de esa operación. De esta forma la ecuación $x + b = a$ siempre admitirá una solución en el nuevo conjunto de números. Tal simétrico lo notaremos por $–a$ para todo $a \in \mathbb{N}$.

En la vida moderna, a menudo se necesitan números negativos. Por ejemplo: Si tengo 50 euros en mi cuenta bancaria, y saco 53 euros, entonces deberé 3 euros al banco. Este ejemplo simple capta la idea del número -3 y también sugiere una definición matemática.

Continuando esta línea de pensamiento, notamos que si mi cuenta originalmente tiene 10 euros, y retiro 13 euros, entonces el resultado final sería el mismo: un saldo de -3; Y de manera similar si no tenía dinero y retiré 3 euros, y así sucesivamente.

Resumiendo, cada una de estas situaciones es un par de números (i, j), donde i es la cantidad originalmente en la cuenta, y j es la cantidad retirada. La idea es que los pares (50, 53), (10, 13), (0, 3), ... son todos equivalentes, y cada uno de ellos define el número -3.

Para definir el conjunto $\mathbb{Z}$, partimos del conjunto dado por el producto cartesiano de $\mathbb{N}$ consigo mismo, es decir:

$$\mathbb{N} \times \mathbb{N} = \{(n, m) / n, m \in \mathbb{N}\}$$

y sobre el definimos la relación binaria que denotaremos mediante el símbolo ~

$$(n, m) \sim (n', m') \text{ si y sólo si } n + m' = m + n'.$$

Proposición 4.5. La relación ~ en $\mathbb{N} \times \mathbb{N}$ es una relación de equivalencia.

Llamaremos **número entero** a cada una de las clases de equivalencia obtenidad en $\mathbb{N} \times \mathbb{N}$ al definir la relación de equivalencia ~.
Llamaremos **conjunto de los números enteros** y lo denotaremos por $\mathbb{Z}$ al conjunto cociente $\mathbb{N} \times \mathbb{N} /\sim$.

Si consideramos como representantes de cada clase los que tiene al menos una de sus componentes nula, se tiene que las distintas clases son:

(I) La clase $[(a, 0)] = \{(a + k, k) / k \in \mathbb{N}\}$ es un número enteros que designamos por a, para cualquier $a \in \mathbb{N}^* = \mathbb{N} - \{0\}$. Denotarmos por $\mathbb{Z}^+$ al conjunto formado por tales enteros que llamaremos **enteros positivos**.

(II) La clase $[(0, a)] = \{(k, a + k) / k \in \mathbb{N}\}$ es un número entero que denotaremos por –a, para todo $a \in \mathbb{N}^*$. Designamos con $\mathbb{Z}^-$ al conjunto formado por dichos enteros que llamaremos **enteros negativos**.

(III) La clase $[(0, 0)] = \{(k, k) / k \in \mathbb{N}\}$ es un número entero que denotamos por 0.

Utilizando esta nueva notación para representar los números enteros, por lo que el conjunto de los números enteros vendrá dado por:

$$\mathbb{Z} = \{...,–3, –2, –1, 0, 1, 2, 3,...\}.$$

Inducida por la suma de números naturales podemos definir la **suma de números enteros** como la operación interna dada por

$$+: \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

de manera que para cada par de números enteros a, b existe un único número entero a + b.

Proposición 4.6. La suma de números enteros satisface:

i) **Elemento neutro**: $\exists\ 0 \in \mathbb{Z}$ tal que $0 + a = a = a + 0$, $\forall a \in \mathbb{Z}$.

ii) **Conmutativa**, $a + b = b + a$, $\forall a, b \in \mathbb{Z}$.

iii) **Asociativa**, $(a + b) + c = a + (b + c)$, $\forall a, b, c \in \mathbb{Z}$.

iv) **Cancelativa**,

Dados $a, b, p \in \mathbb{Z}$, si $a + p = b + p$, entonces $a = b$.

v) **Elemento simétrico,**

$\forall a \in \mathbb{Z}$, existe $-a \in \mathbb{Z}$ tal que $(-a) + a = 0 = a + (-a)$.

La existencia de $-a$ nos permite definir la operación **sustracción** o **diferencia** como sigue:

$$x - y = x + (-y)$$

La **multiplicación de números enteros** es una aplicación

$$. : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z}$$

de manera que para cada par de números enteros a, b existe un único número entero a . b.

Proposición 4.7. El producto de números enteros satisface:

i) **Elemento cero**: $\exists\ 0 \in \mathbb{Z}$ tal que $0 . a = 0 = a . 0$, $\forall a \in \mathbb{Z}$.

ii) **Elemento neutro**: $\exists\ 1 \in \mathbb{Z}$ tal que $1 . a = a = a . 1$, $\forall a \in \mathbb{Z}$.

iii) **Conmutativa**, $a . b = b . a$, $\forall a, b \in \mathbb{Z}$.

iv) **Asociativa**, $(a . b) . c = a . (b . c)$, $\forall a, b, c \in \mathbb{Z}$.

v) **Cancelativa**,

Dados $a, b, p \in \mathbb{Z}$, si $a . p = b . p$ y $p \neq 0$, entonces $a = b$.

vi) **Distributivas**, $a . (b + c) = a . b + a . c$, $\forall a, b, c \in \mathbb{Z}$.

vii) **Regla de los signos:** $(-a) . b = -(a . b) = a . (-b)$;

$-(-a) = a$; y $(-a) . (-b) = a . b$

Proposición 4.8. $\mathbb{Z}$ es un **dominio de integridad**, el producto de dos elementos distintos de cero es distinto de cero, es decir, si a . b = 0 entonces a = 0 o b = 0.

Proposición 4.9. Inducida por la relación de orden en el conjunto de los números naturales, podemos definir una relación de orden en $\mathbb{Z}$ mediante

$a \leq b$ si y solo si $b - a \in \mathbb{N}$.

Proposición 4.10. El conjunto $\mathbb{Z}$ respecto al orden anterior es un conjunto totalmente ordenado, pero no es un conjunto bien ordenado.

3. DIVISIBILIDAD EN EL CONJUNTO DE LOS NÚMEROS ENTEROS

Dados a, b ∈ ℤ. Diremos que a es **divisor** de b, a **divide** a b, a es **factor** de b y lo representamos mediante a | b, si y solo si existe un número entero c tal que a . c = b, es decir,

$$a \mid b \Leftrightarrow \exists c \in \mathbb{Z} \text{ tal que } a \cdot c = b$$

En tal caso también diremos que b es **múltiplo** de a, es decir, b ∈ å.

Proposición 4.11. La relación binaria ser divisor en ℤ

$$a \leq b \text{ si y sólo si a es divisor de b}$$

es reflexiva y transitiva, es decir, es un preorden en ℤ.

Observación: 1 es divisor y 0 es múltiplo de cualquier entero.

Ejercicio 1: Probar que si c|a y c|b entonces c|(ma+nb) para todo m, n ∈ ℤ.

Un número entero p ∈ ℤ se dice que es **primo** si y sólo si p ≠ 0, ±1 y sus únicos divisores son el ±1 y ± p. Notar que si p es primo entonces – p también es primo. Diremos que un número entero es **compuesto** si no es primo, es decir, tiene divisores distintos de si mismo y de la unidad.

En aritmética elemental un ejercicio estándar es "factorizar" un entero. Por ejemplo: $396 = 2^2 \cdot 3^2 \cdot 11$.

Teorema 4.12. (Teorema Fundamental de la Aritmética) Todo número entero distinto de ±1 y 0 admite una descomposición única (salvo el orden y opuestos) como producto de números primos positivos, es decir:

$$\forall a \in \mathbb{Z} - \{0, \pm 1\}, \quad a = \pm p_1^{\alpha_1} . p_2^{\alpha_2} \ldots p_r^{\alpha_r} \quad \text{con } p_i < p_j \text{ si } i < j.$$

A la expresión anterior se le conoce como la **descomposición en factores primos** de a.

Ejercicio 2: Encontrar la factorización en primos de 2010.

Proposición 4.13. Dado $a = \pm p_1^{\alpha_1}.p_2^{\alpha_2}....p_r^{\alpha_r} \in \mathbb{Z}$ y $a \neq 0, \pm 1$, un elemento $b \in \mathbb{Z}$ es un divisor de a si y sólo si todos los factores primos de b son factores primos de a con exponentes menores o iguales a los de b, es decir:

$$b = \pm p_1^{\beta_1}.p_2^{\beta_2}....p_r^{\beta_r} \quad \text{con } 0 \leq \beta_i \leq \alpha_i, \forall i = 1,\ldots,r.$$

Ejercicio 3: Usar la solución de ejercicio 2 y la proposición previa para encontrar el conjunto de los divisores positivos de 2010.

De acuerdo con la definición de divisor, el conjunto D_m de los divisores de un entero m contiene ambos enteros positivos y negativos.

Dados dos enteros $a, b \in Z - \{0, \pm 1\}$ diremos que $D_a \cap D_b$ es el conjunto de los divisores comunes de a y b. Este conjunto es no vacío, ya que contiene al 1. Además cada comun divisor c satisface $c \leq a$ y $c \leq b$, por tanto el conjunto tiene un máximo.

Dados $a, b \in \mathbb{Z} - \{0, \pm 1\}$. Llamaremos **máximo común divisor** de a y b al número entero $d \in \mathbb{Z}$ que satisface:

i) $d \mid a$ y $d \mid b$,

ii) Si existe $d' \in \mathbb{Z}$ tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.

Al máximo común divisor de a y b lo denotamos por:

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

Dados a, b $\in \mathbb{Z}$ - {0, ±1}. Llamaremos **mínimo común múltiplo** de a y b al número entero M $\in \mathbb{Z}$ que satisface:

i) a | M y b | M,

ii) Si existe M' $\in \mathbb{Z}$ tal que a | M' y b | M', entonces M | M'.

Al mínimo común múltiplo de a y b lo denotamos por:

$$M = [a, b] = m.c.m\{a, b\}.$$

De forma análoga podemos definir el máximo común divisor y mínimo común múltiplo de $a_1, a_2,...,a_n \in \mathbb{Z}$.

Ejercicio 4: Obtener el máximo común divisor y el mínimo común múltiplo de 2010 y 650.

Proposición 4.14. Dados a y b $\in \mathbb{Z}$ - {0, ±1} tales que:

$$a = \pm p_1^{\alpha_1}.p_2^{\alpha_2}....p_s^{\alpha_s}.p_{s+1}^{\alpha_{s+1}}...p_r^{\alpha_r}$$

$$b = \pm p_1^{\beta_1}.p_2^{\beta_2}....p_s^{\beta_s}.p_{s+1}^{\beta_{s+1}}...p_r^{\beta_r}$$

con $\alpha_i, \beta_j \geq 0$, $\forall i = 1,2,\ldots,r$. Entonces:

$$d = (a, b) = \pm p_1^{f_1}.p_2^{f_2}....p_s^{f_s}.p_{s+1}^{f_{s+1}}...p_r^{f_r}$$

con $f_i = \min\{\alpha_i, \beta_i\}$ $\forall i = 1,2,\ldots,r$ y

$$M = [a, b] = \pm p_1^{g_1}.p_2^{g_2}....p_s^{g_s}.p_{s+1}^{g_{s+1}}...p_r^{g_r}$$

con $g_i = \max\{\alpha_i, \beta_i\}$ $\forall i = 1,2,\ldots,r$.

Por tanto, d es el producto de los divisores comunes elevados al menor exponente y M es el producto de los divisores (comunes y no comunes) elevados al mayor exponente.

Proposición 4.15. Sean a y b $\in \mathbb{Z} - \{0, \pm 1\}$, entonces

$$[a, b] \cdot (a, b) = a \cdot b.$$

Continuamos ahora con el proceso simple de divider un entero entre otro. En los primeros cursos de primaria aprendemos a divider y obtener restos. Por ejemplo, aprendemos algo que podríamos expresar mediante "26 dividido entre 3 cabe a 8 con resto 2" (3 cabe ocho veces en 26 sobrándonos 2). Esto es,

$$26 = 3 \cdot 8 + 2.$$

El número 8 se le llama cociente y al 2 se le llama resto. Lo importante es que el resto tiene que ser menor que 3. Es cierto que $26 = 3 \cdot 7 + 5$ pero sabemos que tenemos que tomar el menor valor, de forma que la cantidad "sobrante" sea lo más pequeña posible.

Lo anterior lo vamos a poder hacer con cualquiera dos enteros a y b ($b \neq 0$), como muestra el siguiente resultado:

Teorema 4.16. (Algoritmo de la división) Sean a y b $\in \mathbb{Z}$, y $b \neq 0$. Entonces existen números enteros q y r tales que

$$a = b \cdot q + r$$

con $0 \leq r < |b|$. Además q y r son únicos.

En lo anterior, q es llamado **cociente**, r es el **resto**, a el **dividendo** y b el **divisor**.
Nótese que si el resto es cero, entonces b es un divisor de a.

Ejercicio 5: Obtener el cociente y el resto para los siguientes valores de a y b:

a) a = 37 y b = 5,
b) a = –93 y b = 7
c) a = 48 y b = –9
d) a = –53 y b = –6

Otro resultado importante es que el máximo común divisor mcd{a, b} se puede expresar siempre como combinación lineal entera de a y b. Este resultado se conoce como la identidad de Bezout:

Proposición 4.17. (Identidad de Bezout) Dados a, b $\in \mathbb{Z}$ - {0, ±1}. Entonces existen unos únicos número u, v $\in \mathbb{Z}$ tales que

$$(a, b) = a \cdot u + b \cdot v.$$

Dos número enteros a y b diremos que son **primos relativos** si y sólo si d = (a, b) = 1.

Corolario 4.27. Si a y b $\in \mathbb{Z}$ - {0, ±1} son primos relativos, entonces existen unos únicos números u, v $\in \mathbb{Z}$ tales que

$$1 = a \cdot u + b \cdot v.$$

Ejercicio 6: Comprobar que 42 y 55 son coprimos.

Como consecuencia del algoritmo de la división, obtenemos un nuevo método para calcular el máximo común divisor ya que para enteros grandes, el método anterior basado en obtener la factorización de los números es tedioso y lento. Este nuevo método es más eficiente. Se llama **algoritmo de Euclides** y está basado en el siguiente resultado:

Lema 4.18. Dados a, b números enteros y b ≠ 0, si a = b . q + r con q, r$\in \mathbb{Z}$ dados por el algoritmo de la división, entonces

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

Antes de describir el algoritmo de Euclides, comenzamos con un ejemplo para mostrar como aplicando el resultado anterior varias veces encontramos el máximo común divisor de dos números.

Ejemplo: Obtener usando el algoritmo de la división y el lema previo el m.c.d.{2010, 560}.

Primero aplicamos el algoritmo de la división a los números a = 2010 y b = 560, obtenemos:

$$2010 = 3 \cdot 560 + 330$$

Por el lema previo, m.c.d.{2010, 560} = m.c.d.{560,330}, por tanto, aplicando una vez el algoritmo de la división hemos reducido el tamaño de los números involucrados.

Ahora aplicamos el algoritmo de la división a 560 y el resto obtenido en el paso previo, 330:

$$560 = 1 \cdot 330 + 230.$$

Por el lema anterior, m.c.d.{2010, 560} = m.c.d.{560,330} = m.c.d.{330, 230}. Aplicando de nuevo el algoritmo de la división:

$$330 = 1 \cdot 230 + 100,$$

por tanto, m.c.d.{2010, 560} = m.c.d.{560,330} = m.c.d.{330, 230} = m.c.d.{230, 100}.

Continuando de la misma forma aplicando repetidamente el algoritmo de la división, pronto obtenemos un resto igual a cero:

$$230 = 2 \cdot 100 + 30.$$
$$100 = 3 \cdot 30 + 10.$$
$$30 = 3 \cdot 10 + \mathbf{0}.$$

Y por el lema previo:

$$\begin{aligned} \text{mcd}\{2010, 560\} &= \text{mcd}\{560,330\} \\ &= \text{mcd}\{330, 230\} \\ &= \text{mcd}\{230, 100\} \\ &= \text{mcd}\{100, 30\} \\ &= \text{mcd}\{30, 10\} \\ &= \text{mcd}\{10, 0\} = 10. \end{aligned}$$

Dados a, b $\in \mathbb{Z} - \{0, \pm 1\}$. Como (a, b) = (|a|, |b|) podemos suponer que $a \geq b > 0$. Aplicando el algoritmo de la división entre a y b obtenemos dos enteros q_1 y r_1 tales que

$$a = b \cdot q_1 + r_1 \text{ con } 0 \leq r_1 < b,$$

y el problema de calcular el mcd{a, b} se reduce a calcular el mcd{b, r_1} que son números más pequeños. De hecho, puede ocurrir que:

- $r_1 = 0$, entonces mcd{a, b} = mcd{b, 0} = b.
- $r_1 \neq 0$, en cuyo caso podemos volver a aplicar el algoritmo de la división a b y r_1 y obtenemos

$$b = r_1 \cdot q_2 + r_2 \text{ con } 0 \leq r_2 < r_1,$$

y el problema de nuevo se reduce a calcular el mcd{r_1, r_2}, pudiendo ocurrir que:

- $r_2 = 0$, y entonces mcd{a, b} = mcd{b, r_1}=mcd{r_1, 0}= r_1
- $r_2 \neq 0$, y así podríamos volver a aplicar el algoritmo de la división ahora entre r_1 y r_2, obteniendo

$$r_1 = r_2 \cdot q_3 + r_3 \text{ con } 0 \leq r_3 < r_2.$$

Así sucesivamente se calcularían sucesivas divisiones con restos cada vez más pequeños. Tales números $r_1 > r_2 > r_3 > \ldots$ constituirán una sucesión de números naturales decrecientes y acotada por el 0, tras un número finito de pasos obtendremos un resto igual a $r_s = 0$, es decir, r_{s-1} divide a r_{s-2}:

$$\ldots\ldots\ldots\ldots$$
$$r_{s-3} = r_{s-2} \cdot q_{s-1} + r_{s-1} \text{ con } 0 \leq r_{s-1} < r_{s-2},$$
$$r_{s-2} = r_{s-1} \cdot q_s + 0.$$

y así se tiene:

$mcd\{a, b\} = mcd\{b, r_1\} = mcd\{r_1, r_2\} = ... = mcd\{r_{s-2}, r_{s-1}\} = mcd\{r_{s-1}, 0\} = r_{s-1}$,

es decir, el máximo común divisor de a y b vendrá dado por el último resto distinto de 0.

Ejemplo: Calcular el m.c.d{3120, 270}

El algoritmo de Euclides nos proporciona algo extra. Trabajando hacia atrás a través de los calculos realizados en el algoritmo, podemos obtener la identidad de Bezout, es decir, podemos expresar el m.c.d.{a, b} como una combinación lineal entera de a y b:

$$r_{s-1} = mcd\{a, b\} = a \cdot u + b \cdot v$$

En el ejemplo anterior, calculamos m.c.d.{2010,560} = 10.
Primero, reescribimos la penultima aplicación del algoritmo de la división $100 = 3 \cdot 30 + 10$ aislando el máximo común divisor a un lado de la igualdad, manteniendo lo demás al otro lado:

$$10 = 100 + \mathbf{30} \cdot (-3)$$

Nótese que el "símbolo –" se pone al cociente y no al divisor. Ahora a partir de la igualada obtenida tras la aplicación previa del algoritmo de la división, $230 = 2 \cdot 100 + 30$, despejamos su resto 30 y el resultado $230 + 100 \cdot (-2)$ lo escribimos en lugar de 30 en la primera igualdad, simplificando después como sigue:

$$10 = 100 + \mathbf{(230 + 100 \cdot (-2))} \cdot (-3) = 230 \cdot (-3) + 100 \cdot 7$$

Repetimos el proceso con las aplicaciones previas del algoritmo de la división:

$$100 = 330 + 230 \cdot (-1) \longrightarrow 10 = 230 \cdot (-3) + (330 + 230 \cdot (-1)) \cdot 7 = 330 \cdot 7 + 230 \cdot (-10)$$

$$230 = 560 + 330 \cdot (-1) \longrightarrow 10 = 330 \cdot 7 + (560 + 330 \cdot (-1)) \cdot (-10) = 560 \cdot (-10) + 330 \cdot 17$$

Finamente, a partir de la igualdad obtenida tras la primera aplicación del algoritmo de la división $2010 = 3 \cdot 560 + 330$, aislamos el resto, $330 = 2010 + 560 \cdot (-3)$ y reeplazamos 330 por $2010 + 560 \cdot (-3)$ en la última igualdad, y simplificamos:
$10 = 560 \cdot (-10) + 330 \cdot 17 = 560 \cdot (-10) + (2010 + 560 \cdot (-3)) \cdot 17$

Por tanto, trabajando hacia atras el algoritmo de Euclides, sucesivamente reemplando el resto y simplificando, obtenemos:

$$10 = 2010 \cdot 17 + 560 \cdot (-61).$$

De hecho, se tiene el siguiente resultado:

Lema 20. Para cada $i \geq 1$, existe números enteros u_i y v_i tales que

$$r_i = a \cdot u_i + b \cdot v_i$$

donde r_i son los distintos restos que se obtiene al aplicar el algoritmo de Euclides al calcular el mcd{a, b}.

Tales números vienen dados inductivamente por las formulas:

$$u_0 = 0, \qquad v_0 = 1,$$
$$u_1 = 1, \qquad v_1 = -q_1,$$
$$u_i = u_{i-2} - u_{i-1} \cdot q_i, \qquad v_i = v_{i-2} - v_{i-1} \cdot q_i,$$

en las que q_i son los respectivos cocientes de las divisiones.

En particular, los números u y v de la identidad de Bezout vendrán dados por las formulas:

$$u = u_{s-3} - u_{s-2} \cdot q_{s-1}, \qquad v = v_{s-3} - v_{s-2} \cdot q_{s-1}.$$

Como hemos visto anteriormente, trabajando hacia atras el algoritmo de Euclides, sucesivamente reemplando el resto y simplificando, habiamos obtenemos:

$$10 = 2010 \cdot 17 + 560 \cdot (-61).$$

Mediante el otro método usando las fórmulas:

$u_i = u_{i-2} - u_{i-1} \cdot q_i$,

$v_i = v_{i-2} - v_{i-1} \cdot q_i$,

i	q_i	r_i	u_i	v_i
0	-	560	0	1
1	3	330	1	-3
2	1	230	-1	4
3	1	100	2	-7
4	2	30	-5	18
5	3	10	17	-61

Ejercicio 8: Obtener la identidad de Bezout para los números del ejercicio previo.

Otra aplicación del algoritmo de Euclides es el calculo de todas las soluciones enteras de las ecuaciones lineales en dos variables

$$a.x + b.y = c, \qquad a, b, c \in \mathbb{Z}.$$

Este problema se conoce como la **ecuación lineal diofántica** (es una ecuación lineal en la que sólo se buscan soluciones enteras).

Teorema 4.21. La ecuación anterior tiene solución en $\mathbb{Z}$ si y sólo si m.c.d.{a, b} | c.

Proposición 4.22. Si (x_0, y_0) es una solución en $\mathbb{Z}$ de la ecuación anterior, el resto de soluciones enteras de dicha ecuación vendrán dadas por las formulas:

$$\begin{cases} x = x_0 - k\,\frac{b}{d} \\ y = y_0 + k\,\frac{a}{d} \end{cases} \qquad \forall k \in \mathbb{Z}, \text{ donde } d = \text{m.c.d.}\{a, b\} \text{ y } k \text{ es un parámetro.}$$

Ejercicio 9: Obtener la solución entera de la ecuación lineal

$$2010 \cdot x - 560 \cdot y = 50.$$

4. CONGRUENCIAS. SISTEMAS DE CONGRUENCIAS

Sea $n \in \mathbb{Z} - \{0\}$ y $a, b \in \mathbb{Z}$. Diremos que **a es congruente con b módulo n** y lo denotamos $a \equiv b \bmod n$ si y sólo si $a - b$ es múltiplo de n, es decir,

$$a \equiv b \bmod n \Leftrightarrow \exists\, k \in \mathbb{Z} \text{ tal que } a = b + k.n$$

Equivalentemente, $a \equiv b \bmod n \Leftrightarrow n \mid (a - b)$.

Si a y b no son congruentes módulo n, se denota $a \not\equiv b \bmod n$.

Una razón para tener en cuenta este nuevo concepto es que algunos problemas que involucran el uso de números enteros muy grandes se pueden simplificar trabajando módulo n para algún $n \in \mathbb{Z}$. En realidad, lo hacemos todo el tiempo en la vida cotidiana. Por ejemplo:

I) No decimos “Nos vemos en 195 minutos”, en su lugar solemos decir “Nos vemos en tres horas y quince minutos (y cuarto)” ya que $195 \equiv 15 \bmod 60$.

II) Si sabemos que tenemos el examen final en 45 días, y necesitamos saber, ¿qué día de la semana será? Como $45 \equiv 3 \bmod 7$, la respuesta es que serán 3 días más tarde que hoy; Por lo tanto, si hoy es lunes, entonces en 45 días será jueves.

Proposición 4.23. Sea n un entero positivo fijo. Entonces, para todo $a, b \in \mathbb{Z}$, $a \equiv b \bmod n$ si y sólo si a partir de a y b obtenemos el mismo resto tras dividir ambos por n. (Demostración ejercicio 4.62).

Proposición 4.24. La relación de congruencia es una relación de equivalencia en $\mathbb{Z}$. Al conjunto cociente de la relación de congruencia lo denotamos por

$$\mathbb{Z}_n = \mathbb{Z} / \equiv \bmod n = \{ \bar{a} / a \in \mathbb{Z} \}$$

y se le llama **conjunto de las clases de restos o residuos módulo n**.

El **residuo** de un entero a módulo n es un número b tal que $a \equiv b \bmod n$ y $0 \leq b < n$. En otras palabras el residuo de a módulo n es el resto que obtenemos tras dividir a entre n.

Proposición 4.25. Los elementos de $\mathbb{Z}_n$ son los distintos restos que se obtienen al dividir entre n, es decir: $\mathbb{Z}_n = \{ \bar{0}, \bar{1}, \bar{2}, ..., \}$ y así $\text{card}(\mathbb{Z}_n) = n$ para $n > 1$.

Ejercicio 10: Obtener $\mathbb{Z}_5$ y describir sus elementos.

La suma, la resta y la multiplicación se comportan muy bien con respecto a las congruencias. A la división no le ocurre lo mismo.

Proposición 4.26. Sea n un entero positivo fijo. Si $a \equiv b \bmod n$ y $c \equiv d \bmod n$, entonces $(a + c) \equiv (b + d) \bmod n$, $(a - c) \equiv (b - d) \bmod n$, y $(a \cdot c) \equiv (b \cdot d) \bmod n$.

El resultado previo nos permite definir las operaciones aritméticas de suma, resta y multiplicación en $\mathbb{Z}_n$, lo que nos permite hablar de aritmética modular. Si $\bar{a}$ y $\bar{b}$ son clases de congruencia módulo n, es decir, elementos de $\mathbb{Z}_n$ entonces

$$\bar{a}+\bar{b}=\overline{a+b} \qquad \bar{a}-\bar{b}=\overline{a-b} \qquad \bar{a}\cdot\bar{b}=\overline{a\cdot b}$$

Esto es,

$\bar{a}+\bar{b}=\overline{a+b}=\bar{c}$ donde $\bar{c}\in\mathbb{Z}_n$ tal que $c\equiv(a+b) \bmod n$

$\bar{a}-\bar{b}=\overline{a-b}=\bar{s}$ donde $\bar{s}\in\mathbb{Z}_n$ tal que $s\equiv(a-b) \bmod n$

$\bar{a}\cdot\bar{b}=\overline{a\cdot b}=\bar{p}$ donde $\bar{p}\in\mathbb{Z}_n$ tal que $p\equiv(a.b) \bmod n$

Por tanto, las tablas de operaciones de $\mathbb{Z}_5$ son:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Ejercicio 11: Construir las tablas de operaciones de $\mathbb{Z}_7$.

Es fácil observar, que es posible evaluar aparentemente difíciles expresiones módulo n sin recurrir a la calculadora o al ordenador.

Ejercicio 12: Calcular

a) $5^8 \bmod 14$.

b) $(29 \cdot (-47))^{12} \bmod 31$

Proposición 4.27. La suma y el producto en $\mathbb{Z}_n$ satisface las siguientes propiedades:

i) **Asociativa para la suma**,
$(\overline{a} + \overline{b}) + \overline{c} = \overline{a} + (\overline{b} + \overline{c}), \quad \forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n.$

ii) **Elemento neutro para la suma**:
Existe $\overline{0} \in \mathbb{Z}_n$ tal que $\overline{0} + \overline{a} = \overline{a} = \overline{a} + \overline{0}, \forall\ \overline{a} \in \mathbb{Z}_n.$

iii) **Conmutativa para la suma**,
$\overline{a} + \overline{b} = \overline{b} + \overline{a}, \quad \forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n.$

iv) **Elemento simétrico respecto de la suma,**
$\forall\ \overline{a} \in \mathbb{Z}_n$, existe $\overline{-a} \in \mathbb{Z}_n$ tal que $(\overline{-a}) + \overline{a} = \overline{0} = \overline{a} + (\overline{-a}).$

v) **Asociativa para el producto**,
$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{a} \cdot (\overline{b} \cdot \overline{c}), \quad \forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n.$

vi) **Elemento neutro para el producto**:
Existe $\overline{1} \in \mathbb{Z}_n$ tal que $\overline{1} \cdot \overline{a} = \overline{a} = \overline{a} \cdot \overline{1}, \forall\ \overline{a} \in \mathbb{Z}_n.$

vii) **Conmutativa para el producto**,
$\overline{a} \cdot \overline{b} = \overline{b} \cdot \overline{a}, \quad \forall\ \overline{a}, \overline{b} \in \mathbb{Z}_n.$

viii) **Distributivas**,
$\overline{a} \cdot (\overline{b} + \overline{c}) = \overline{a} \cdot \overline{b} + \overline{a} \cdot \overline{c}, \quad \forall\ \overline{a}, \overline{b}, \overline{c} \in \mathbb{Z}_n.$

Un elemento $\overline{a} \neq \overline{0}$ en $\mathbb{Z}_n$ se dice que es un **divisor del cero** si existe otro elemento $\overline{b} \neq \overline{0}$ en $\mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{0}$. Diremos que $\mathbb{Z}_n$ es un **dominio de integridad** si no tiene divisores de cero.

Proposición 4.28. Un elemento $\overline{a} \in \mathbb{Z}_n$ distinto de $\overline{0}$ es un divisor de cero en $\mathbb{Z}_n$ si y sólo si a y n no son primos relativos, es decir, $(a, n) \neq 1$. (Demostración ejercicio 4.69).

Corolario 4.29. $\mathbb{Z}_n$ es un dominio de integridad si y sólo si n es un número primo. (Demostración ejercicio 4.69).

Ejercicio 13: Obtener un divisor del cero en $\mathbb{Z}_{42}$. ¿Es posible obtener un divisor del cero en $\mathbb{Z}_{43}$?

Un elemento $\overline{a} \neq \overline{0}$ en $\mathbb{Z}_n$ es una **unidad** en $\mathbb{Z}_n$ si tiene inverso (elemento simétrico para el producto), es decir, si existe otro elemento $\overline{b} \neq \overline{0}$ en $\mathbb{Z}_n$ tal que $\overline{a} \cdot \overline{b} = \overline{1}$. Diremos que $\mathbb{Z}_n$ es un **cuerpo** si todo elemento no nulo de $\mathbb{Z}_n$ es una unidad.

Proposición 4.30. Un elemento $\overline{a} \in \mathbb{Z}_n$ distinto de $\overline{0}$ es una unidad en $\mathbb{Z}_n$ si y sólo si a y n son primos relativos, es decir, $(a, n) = 1$. (Demostración ejercicio 4.71).

Corolario 4.31. $\mathbb{Z}_n$ es un cuerpo si y sólo si n es un número primo. (Demostración ejercicio 4.71).

Ejercicio 14: Comprobar que $\overline{5}$ es una unidad en $\mathbb{Z}_{42}$. ¿Es $\mathbb{Z}_{42}$ un cuerpo? ¿Y $\mathbb{Z}_{43}$?

En la práctica, una forma de encontrar el inverso de $\overline{a} \in \mathbb{Z}_n$ es ir probando realizando los distintos productos con todos los elementos de $\mathbb{Z}_n$, es decir, calcular $\overline{a} \cdot \overline{1}$, $\overline{a} \cdot \overline{2}$, $\overline{a} \cdot \overline{3}$,…, hasta encontrar uno que nos de igual a $\overline{1}$. Sin embargo si n es grande, el método anterior no es el más aconsejable. Otra aplicación de la identidad de Bezout es el cálculo de inversos en $\mathbb{Z}_n$:

Corolario 4.32. Si $\overline{a} \in \mathbb{Z}_n$ tal que (a, n) = 1, entonces el inverso de $\overline{a}$ en $\mathbb{Z}_n$ es $\overline{u}$ donde $u \in \mathbb{Z}$ tal que $1 = a.u + n.v$ es la identidad de Bezout.

Ejercicio 15: Obtener el inverso de $\overline{5}$ en $\mathbb{Z}_{322}$.

Las operaciones aritméticas en $\mathbb{Z}_n$ nos van a permitir plantear ecuaciones o sistemas de ecuaciones en $\mathbb{Z}_n$.
Sea $n \in \mathbb{Z}$ con $n > 1$. Una congruencia de la forma

$$a \cdot x \equiv b \bmod n,$$

donde a, b son enteros, $a \neq 0$ y x es una variable, se le llama **ecuación congruencia lineal** o, simplemente, **congruencia lineal:**
Usualmente estaremos interesado en las soluciones entre $0 \leq x < n$.
Ejemplo:

$2x \equiv 4 \bmod 5$	$\rightarrow$ Solución: x = 2
$2x \equiv 5 \bmod 6$	$\rightarrow$ No tiene solución
$6x \equiv 12 \bmod 30$	$\rightarrow$ Soluciones: 2, 7, 12, 17, 22 y 27.

Por tanto, una congruencia lineal puede no tener solución, tener una única solución o varias soluciones (Recordadr que una ecuación ordinaria $a \cdot x = c$ tiene solución única).

Proposición 4.33. La congruencia $a \cdot x \equiv b \bmod n$ tiene una solución si y sólo si $d = mcd\{a, n\} \mid b$. Si d divide a b y x_0 es una solución de la congruencia entre $0 \leq x_0 < n/d$, entonces existen exactamente d soluciones entre $0 \leq x_0 < n$, a saber

$$x_0,\ x_0 + \frac{n}{d},\ x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d}$$

Si a y n son primos relativos, es decir, $mcd\{a, n\} = 1$, la congruencia $a \cdot x \equiv b \bmod n$ tiene una única solución entre $0 \leq x_0 < n$, ya que si $mcd\{a, n\} = 1$, entonces existe el inverso de a en $\mathbb{Z}_n$ y teniendo en cuenta la proposición 26, es decir, la multiplicación se comporta bien con respecto a las congruencias:

$$\left.\begin{array}{l} a \cdot x \equiv b \bmod n \\ a^{-1} \equiv a^{-1} \bmod n \end{array}\right\} \Rightarrow a^{-1} \cdot (a \cdot x) \equiv a^{-1} \cdot b \bmod n \Rightarrow x \equiv a^{-1} \cdot b \bmod n$$

Ejercicio 16: Resolver las congruencias lineales
a) $5 \cdot x \equiv 4 \bmod 322$.
b) $3 \cdot x + 2 \equiv 1 \bmod 7$

Hemos visto que una congruencia lineal es similar a una simple ecuación lineal. ¿Qué será un sistema de ecuaciones?

De la misma forma que en $\mathbb{Z}_n$ podemos plantear y resolver ecuaciones lineales, podemos también plantear y resolver **sistemas de congruencias lineales**:

$$\begin{array}{c} x \equiv a_1 \bmod p_1 \\ x \equiv a_2 \bmod p_2 \\ \ldots\ldots\ldots\ldots \\ x \equiv a_n \bmod p_n \end{array}$$

con $a_i, p_i \in \mathbb{Z}$ y $p_i > 1$, para todo $i = 1, 2, \ldots, n$.

Teorema 4.34. (Teorema Chino del resto) Sean $a_1, a_2,..., a_n \in \mathbb{Z}$ y $p_1, p_2,..., p_n \in \mathbb{Z}$ tal que son primos relativos dos a dos (m.c.d$\{p_i, p_j\} = 1$ si $i \neq j$). Entonces:

i) Existe $a \in \mathbb{Z}$ tal que $a \equiv a_i \bmod p_i$, $\forall i = 1,2,...,n$.

ii) Si $\exists a' \in \mathbb{Z}$ tq $a' \equiv a_i \bmod p_i$, $\forall i=1,2,...,n$,

$\Rightarrow a \equiv a' \bmod (p_1.p_2...p_n)$.

Algoritmo Chino del resto

Consideremos el sistema de congruencias:

$$\begin{aligned} x &\equiv a_1 \bmod p_1 \\ x &\equiv a_2 \bmod p_2 \\ &\cdots\cdots \\ x &\equiv a_r \bmod p_r \end{aligned}$$

tal que $(p_i, p_j) = 1$ si $i \neq j$, entonces el teorema anterior nos asegura que dicho sistema tiene solución.

Paso 1: Llamamos $M_1= 1$, $M_2= p_1$, $M_3= p_1.p_2,...,$ $M_r=p_1.p_2...p_{r-1}$.

Paso 2: Hallamos $u_k \in \mathbb{Z}$ tal que $u_k.M_k \equiv 1 \bmod p_k$, $\forall k=1,2,...,r$.

Paso 3: Hallamos $b_1 \in \mathbb{Z}$ tal que $b_1 \equiv a_1 \bmod p_1$.

Paso 4: Hallamos $w_2 \in \mathbb{Z}$ tal que $w_2 \equiv (a_2 - b_1).u_2 \bmod p_2$.

Paso 5: Hallamos $b_2 = b_1 + w_2. M_2$

Paso 4bis: $\forall k \geq 3$ calculamos $w_k \in \mathbb{Z}$ tal que $w_k \equiv (a_k - b_{k-1}).u_k \bmod p_k$.

Paso 5bis: $\forall k \geq 3$ calculamos $b_k = b_{k-1} + w_k. M_k$.

Paso 6: La solución del sistema es $x = b_r$.

Ejercicio 17: Resolver el siguiente enigma (Sun Tzu's, 400-460BC)

"Hay ciertas cosas cuyo número es desconocido. Cuando las dividimos entre 3, el resto es 2; cuando las dividimos entre 5, el resto es 3; y cuando las dividimos entre 7, el resto es 2. ¿Cúal es el número de cosas?"

5. SISTEMAS DE NUMERACIÓN

Teniendo en cuenta que el conjunto de números naturales es infinito, necesitamos infinitas palabras para nombrarlos e infinitos símbolos para escribirlos. De aquí la necesidad de buscar un conjunto finito de palabras, símbolos y reglas que nos permitan utilizar los números naturales con precisión y comodidad.

Un **sistema de numeración** es un par {S, R} donde S es un conjunto de símbolos y R un conjunto de reglas y convenios que utilizamos para nombrar y escribir los números empleando la menor cantidad posible de palabras y símbolos. Los símbolos de S se llaman **cifras** o **dígitos** y al cardinal del conjunto S se le llama **base** del sistema de numeración.

A lo largo de la historia, se han usado gran variedad de sistemas de numeración para representar los números. El sistema de numeración que nos es más familiar es el hindú-árabe que usa 10 dígitos:

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

los 10 primeros números naturales. Escribimos cada número de derecha a izquierda como una secuencia finita formada a partir de los símbolos anteriores de manera que el valor de dichos símbolos depende de la posición que ocupe: Por ejemplo, en el número 17457

- El primer número representa cuantas unidades tiene.
- El segundo representa cuantas decenas tiene.
- El tercero representa cuantas centenas tiene.
- El cuarto cuantos miles tiene y así sucesivamente.

Además, el sistema es aditivo y multiplicativo. El valor de un número viene dado multiplicando el valor de la posición por el correspondiente dígito y finalmente sumando los resultados:

Valor posición:	**decenas de millar**	**unidades de millar**	**centenas**	**decenas**	**unidades**
Dígito:	1	7	4	5	7
Number: 17457=	$1 \cdot 10^4 +$	$7 \cdot 10^3 +$	$4 \cdot 10^2 +$	$5 \cdot 10^1 +$	$7 \cdot 10^0$

Los primeros en utilizar este sistema fueron los Babilonios hace más de 3000 años, estos los pasaron a los Hindúes que a su vez lo trasmitieron a los Árabes 600 años A.C. Estos lo introdujeron en Europa en el año 1200 D.C. Este sistema no fue utilizado por los Egipcios, los Chinos y los Griegos. La mayoría de los sistemas de numeración mas antiguos no tenían característica posicional, lo que complicaba la aritmética. Babilonios, chinos, indios y el sistema mayas si empleaban el principio del valor de la posición.

Se podría haber utilizado otro entero distinto de 10, de hecho, los Babilonios a veces usaban un sistema de numeración de base 60, los Mayas otro con base 20 y es bien sabido, con la aparición de las computadores ha tenido gran auge al sistema binario (base 2), el sistema octal (base 8) y al sistema hexadecimal (base 16).

Usamos el sistema decimal, probablemente porque tenemos 10 dedos en nuestras manos. Literalmente, la palabra dígito significa dedo.

Cuando la base del sistema es mayor de 10, se añaden las primeras letras del alfabeto, así para el sistema hexadecimal el conjunto S viene dado por:

$$S = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F\}$$

de manera que A = 10, B = 11, C = 12, …, F = 15.

Teorema 4.35 (Teorema Fundamental de la Numeración) Sea $b \geq 2$, un número entero. Cualquier entero positivo n se puede escribir de forma única en base b como:

$$n = d_k b^k + ... + d_2 b^2 + d_1 b^1 + d_0 b^0$$

con k, $d_i \in \mathbb{Z}$ y $0 \leq d_i < b$, $\forall i = 0,1,...,k$. A lo anterior se le llama la **representación en base b de n** y para abreviar escribiremos

$$n = (d_k\ d_{k-1} ...\ d_1\ d_0)_b$$

Podemos obtener la representación de un entero en base b mediante un algoritmo que consiste en una sucesión de divisiones entre b y hacer un seguimiento de los restos de estas divisiones.

Ejercicio 18: Encontrar la representación en base 2 de 67, la representación en base 8 de 678 y la representación en base 16 de 725.

El proceso recíproco es muy simple: para convertir representaciones en base b a su equivalente entero, simplemente sumamos la correspondiente serie.

Ejercicio 19: Encontrar el entero (en base 10) equivalente a cada una de las siguientes representaciones: $(1010100)_2$, $(146)_8$ y $(A7C)_{16}$.

“Hay 10 tipos de personas en este mundo: los que pueden leer binario y los que no”