Capítulo

2

Congruencias

2.1 Definiciones básicas

Definición 2.1.1 *Sea m un entero fijo, diremos que dos enteros a y b son* **congruentes módulo** *m , y usamos la notación*

$$a \equiv b \, mod \, m$$

si y sólo si m divide a $a - b$

Ejemplo: $25 \equiv 4 \, mod \, 7$, pues 7 divide a 25 - 4 = 21.

Observación: Podemos decir que a es congruente a b módulo m si existe un entero k, tal que $a = b + km$.

También se puede definir congruencia, usando el concepto de pertenencia. Más precisamente a es congruente a b módulo m si y sólo si a está en la sucesión de enteros

$$\ldots, b - m, b, b + m, b + 2m, \ldots$$

Cuando a y b no son congruentes módulo m, diremos que son **incongruentes** y lo denotaremos por $a \not\equiv b \, mod \, m$.

La notación de congruencias fue introducida por Gauss en su libro *Disquisitions Arithmeticae*, en 1799. Gauss desarrolló gran parte de la teoría de congruencias, planteó muchos problemas interesantes sobre este tema y resolvió algunos de ellos. Uno de los más importantes fue la resolución de la ecuación cuadrática de congruencias.

La noción de congruencia se utiliza a diario para medir el tiempo. Por ejemplo las horas del día se cuentan módulo 24, los días de la semana se cuentan módulo 7 , etc...

En lo sucesivo, m será un entero positivo fijo.

Teorema 2.1.1 *Sean a, b y c enteros cualesquiera. Entonces se tiene*

1. $a \equiv a \, mod \, m$
2. *Si* $a \equiv b \, mod \, m$, *entonces* $b \equiv a \, mod \, m$.
3. *Si* $a \equiv b \, mod \, m$, *y* $b \equiv c \, mod \, m$, *entonces* $a \equiv c \, mod \, m$.

Demostración:

1) Notemos que m divide a $a - a = 0$, luego $a \equiv a \ mod \ m$.

2) Se tiene que m divide a $b - a$, por hipótesis, luego $m| - (b - a)$, y por lo tanto $m \mid a - b$.

3) Por hipótesis se tiene $m \mid b-a$ y $m \mid c-b$. Luego $m \mid (b-a)+(c-b)$, esto es $m \mid c - a$. Por lo tanto $a \equiv c \ mod \ m$.

♠

Observación: Las tres propiedades anteriores para la relación de congruencia, nos indican que ésta es una relación de equivalencia (Ver Capítulo 1). Como resultado de esto, se obtiene una partición en el conjunto de los enteros en clases de equivalencia disjuntas, las cuales llamaremos **clases de congruencia módulo** m.

Definición 2.1.2 *Sea a un entero cualquiera, entonces la clase de congruencia de a módulo m, es el conjunto*

$$[a] = \{x \ entero \mid x \equiv a \ mod \ m\}$$

El entero a en la definición anterior se llama el **representante de la clase** y puede ser elegido arbitrariamente de entre los elementos de la clase: esto es, si $b \equiv a \ mod \ m$ entonces $[a] = [b]$.

Ejemplo: Si se considera la relación de congruencia módulo 7, se tendrá entonces:

$$[0] = \{\ldots, -14, -7, 0, 7, 14, \ldots\}$$

$$[1] = \{\ldots, -13, -6, 1, 8, 15, \ldots\}$$

$$[2] = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$$

$$\vdots$$

$$[6] = \{\ldots, -8, -1, 6, 13, 20, \ldots\}$$

Ejemplo:. *Las horas.*

Para contar el tiempo en un mismo día, usamos las horas. Un día tiene 24 horas exactas y para contar las horas comenzamos por la hora 1, que es cuando comienza el día. Técnicamente, el día comienza en un instante 0 y contando 12 horas a partir de ese instante, el sol se hallará en la posición más alta del firmamento. Así pues, la primera hora comienza en el instante 0, la segunda después de una hora, ... y así sucesivamente hasta la hora 24. Al finalizar la hora 24 comienza un nuevo día y aquí reiniciamos el conteo de las horas. Es decir contamos las horas módulo 24.

Por ejemplo, si en este momento son las 8 p.m. ¿Qué hora será dentro de 200 horas?

Solución:

En primer lugar, si x es la hora buscada, debemos tener

$$x \equiv 20 + 200 \ mod \ 24$$

luego podemos reducir el lado derecho de esta ecuación "módulo 24". Así se obtiene

$$x \equiv 4 \ mod \ 24$$

Luego la hora x será las 4 a.m.

Ejercicios

1) Probar que las tres definiciones de la noción de congruencia, dadas al comienzo, son equivalentes.

2) Si hoy es jueves, entonces ¿que día de la semana será ...
a) dentro de 20 días?,
b) dentro de 100 días ?

3) Indicar cuáles de las siguientes afirmaciones son correctas y cuáles son falsas

1. $18 \equiv 1 \ mod \ 5$
2. $86 \equiv 1 \ mod \ 5$
3. $100 \equiv 10 \ mod \ 9$
4. $62 \not\equiv 2 \ mod \ 8$
5. $10^3 \equiv 1 \ mod \ 9$
6. $2a \equiv 6 \ mod \ 2$
7. $s^2 + s + 1 \equiv 1 \ mod \ 2$
8. $a(a+1)(a+2) \equiv 0 \ mod \ 3$

4) Probar que si $a \equiv b \ mod \ m$, entonces $a \equiv b \ mod \ k$, para todo k divisor de m. ¿Será cierto el recíproco de este resultado? Dar un contraejemplo.

5) Si hoy es jueves 27 de octubre de 1993, entonces ¿que día de la semana será el 27 de octubre de 1994? Use congruencias para hallar el resultado.

2.2 Propiedades de las Congruencias

A continuación damos una serie de propiedades de las congruencias, relacionadas con la suma y el producto de números enteros.

Teorema 2.2.1 *Si $a \equiv b \ mod \ m$, y c es un entero, se tiene*

1. $a + c \equiv b + c \ mod \ m$.
2. $ac \equiv bc \ mod \ m$

Demostración:

1) Si $a \equiv b \ mod \ m$, se tendrá entonces $m \mid b - a$. Luego $m \mid (a + c) - (b + c)$, y de aquí obtenemos

$$a + c \equiv b + c \ mod \ m$$

2) Se tiene $m \mid a - b$, y por lo tanto $m \mid (a - b)c$. Luego $m \mid ab - ac$, lo cual implica

$$ac \equiv bc \ mod \ m.$$

♠

Ejemplo: La ecuación de congruencia $1 \equiv 10 \ mod \ 9$, se puede multiplicar por 30, para obtener $30 \equiv 300 \ mod \ 9$.

Observación: El recíproco del teorema anterior no es cierto en general. Es decir de la congruencia $ca \equiv cb \ mod \ m$ no se puede inferir $a \equiv b \ mod \ m$. Por ejemplo $12 \equiv 6 \ mod \ 6$, pero $6 \not\equiv 3 \ mod \ 6$.

Seguidamente, daremos un par de propiedades mediante las cuales podemos multiplicar y sumar ecuaciones de congruencias, de la misma forma como se hace para las ecuaciones normales.

Teorema 2.2.2 *Sean a, b y c enteros con*

$$a \equiv b \ mod \ m \quad \text{y} \quad c \equiv d \ mod \ m.$$

Entonces se tiene

1. $a + c \equiv b + d \ mod \ m$

2. $ac \equiv bd \ mod \ m$

Demostración:

1) Si $a \equiv b \ mod \ m$, entonces existe un entero k tal que $a = b + km$. Igualmente de $c \equiv d \ mod \ m$, se obtiene un entero h, tal que $c = d + hm$. Luego

$$a + c = b + d + (h + k)m$$

y de aquí se sigue que:

$$a + c \equiv b + d \ mod \ m.$$

2) También tenemos

$$ac = (b + km)(d + hm) = bd + (bh + dk + hkm)m$$

y de esto se sigue que $ac \equiv bd \ mod \ m$. ♠

Teorema 2.2.3 *(***Congruencia de Polinomios***)*

Sea

$$f(x) = c_n x^n + c_{n-1} x^{n-1} + \ldots + c_1 x + c_0,$$

un polinomio con coeficientes enteros. Entonces si $a \equiv b \ mod \ m$ *se tendrá:*

$$f(a) \equiv f(b) \ mod \ m.$$

Demostración:

Partiendo de la congruencia $a \equiv b \ mod \ m$, y aplicando el teorema anterior parte 2) tantas veces como se desee, deducimos

$$a^i \equiv b^i \ mod \ m \quad \text{para todo } \ 1 \leq i \leq n.$$

Multiplicando cada ecuación por su respectivo coeficiente nos da

$$c_i a^i \equiv c_i b^i \ mod\ m$$

Finalmente, podemos sumar todas estas ecuaciones, gracias al teorema 2.2.1 parte 1), para obtener el resultado deseado

$$c_n a^n + \ldots + c_1 a + c_0 \equiv c_n b^n + \ldots + c_1 b + c_0 \ mod\ m$$

luego, hemos probado $f(a) \equiv f(b)\ mod\ m$.

2.3 Cronología

En esta sección estudiaremos algunas aplicaciones de las congruencias en la cronología, como por ejemplo la determinación del día de la semana de una fecha determinada.

El Calendario Gregoriano

El origen de nuestro calendario actual se encuentra en el **Calendario Juliano**, llamado así por Julio César, quien participó activamente en el diseño de éste. En dicho calendario cada año constaba de 365 días y cada cuatro años había un año bisiesto de 366 días. El calendario de 12 meses comenzaba en el mes de Marzo y finalizaba en Febrero. El nombre y duración de los meses era el siguiente:

Nombre del mes	No. de días	Nombre en Latín
Marzo	30	Martius
Abril	30	Aprilis
Mayo	31	Maius
Junio	30	Junius
Quinto	31	Quintilis
Sexto	31	Sextilis
Septiembre	30	Septembris
Octubre	31	Octobris
Noviembre	30	Novembris
Diciembre	31	Decembris
Enero	31	Januaris
Febrero	28	Februarius

Durante el tiempo de César el mes quinto cambió de nombre por julio, en honor a este emperador. Más tarde, el mismo Julio César decidió que el año debería comenzar en enero. De esta manera quedó organizado el calendario sin sufrir ninguna modificación hasta la reforma del Papa **Gregorio XIII** en 1582.

Los años eran numerados de acuerdo al período de cada emperador, hasta el triunfo del cristianismo, cuando se comenzó a enumerarlos en forma diferente. A partir de entonces, el año 1 fue el nacimiento de Cristo y el día de Navidad el primer día de la Era Cristiana, luego los años se cuentan en sucesión creciente, partiendo desde este inicio. Esta reforma fue hecha en el 533 d.c. durante el período del Emperador Dionisio Exigus.

Una de las motivaciones que han tenido todos los pueblos en el momento de establecer un calendario, es la de ubicar correctamente las fiestas religiosas. Así observamos que en el Calendario Cristiano, el Domingo de Pascua determina las otras fechas movibles como la Ascensión y el Corpus Cristi. Durante el Concilio de Nicea en el 325 d.c. se acordó fijar esta fecha, como el primer domingo después de luna nueva que aparezca en el Equinoccio de Primavera (21 de Marzo) o después . Si la luna nueva aparece un domingo, entonces el Domingo de Pascua será el domingo siguiente.

Si bien el Calendario Juliano funcionó bien durante algunos siglos, la celebración de una Semana Santa a fines del siglo XVI, en donde el Domingo de Pascua correspondió al 11 de Marzo, hizo pensar a muchos que este calendario estaba lejos de ser perfecto. Veamos el por qué de semejante error y las rectificaciones que se le hicieron a el mismo, a fin de ajustarlo al tiempo sideral.

El **año astronómico**, una revolución completa de la tierra alrededor del sol, es de 365 días, 6 horas, 9 minutos y 9.5 segundos. Sin embargo el año visible o **año tropical**, período entre dos equinoccios de primavera, es más corto: 365 días, 5 horas, 48 minutos y 46.43 segundos. El Calendario Juliano suponía que el año tenía 365 días y un cuarto, lo cual excede en 11 minutos y 14 segundos al año tropical. Como consecuencia de esto, se comete un error de un día cada 128 años.

A fin de corregir este error, el Papa Gregorio XIII introdujo una reforma en el calendario, mediante la cual se eliminaron 10 días de la historia . Se decidió que el día siguiente al 4 de octubre de 1582, fuese el 15 de octubre. Además se redujeron los años bisiestos mediante la siguiente convención. Los años bisiestos seculares (divisibles por 100) serían sólo aquellos divisibles por 400. Así, por ejemplo 1800 y 1900 no son bisiestos, pero 2000 será bisiesto.

Esta reforma del Calendario Juliano se conoce con el nombre de **Calendario Gregoriano** y es el calendario que se ha venido usando hasta el presente.

Una vez hecha esta exposición de nuestro calendario, pasemos a calcular los días de la semana de algunas fechas históricas importantes. Nótese la importancia de las congruencias, en cuanto a su capacidad de simplificar los cálculos considerablemente.

Ejemplo: ¿Que día de la semana fue el 19 de abril de 1810?

Solución:

En primer lugar, calculamos el número de años bisiestos entre 1993 y 1810. Vemos que 1812 fue bisiesto y cien años más tarde 1912 ocurrieron 25 años bisiestos (descontamos a 1900 que no fue bisiesto). Entre 1912 y 1993 hay 20 años bisiestos, lo cual da un total de 45 años bisiestos desde 1810 hasta 1993. Luego calculamos el desfase entre ambos años relativo a los días de la semana. En otras palabras nos interesa la diferencia x en días desde 1810 hasta 1993 módulo 7.

Usando congruencias tenemos:

$$365 \equiv 1 \ mod \ 7$$

Multiplicando por el número de años transcurridos

$$183(365) \equiv 183 \ mod \ 7 \equiv 1 \ mod \ 7$$

luego, después de agregar todos los días adicionales, producto de los años bisiestos, tenemos:

$$x \equiv 45 + 1 \ mod\ 7 \equiv 46 \ mod\ 7 \equiv 4 \ mod\ 7$$

Por lo tanto hay un desfase de 4 días en el almanaque del año 1810 con respecto al año 1993. Por comodidad, este desfase lo haremos positivo, $-4 \equiv 3 \ mod\ 7$. Luego el desfase será de tres días contando los días hacia adelante en el tiempo.

Para terminar de resolver el problema, miramos el almanaque de 1993 y vemos que el 19 de abril fue lunes. Luego el 19 de abril de 1810 fue jueves.

De la misma forma como hallamos el día de la semana correspondiente al 19 de abril de 1810, podemos determinar cualquier día de otra fecha en ese año. Basta ubicar la fecha correspondiente en el almanaque de 1993, y entonces agregar tres días más. Es decir, el desfase x da toda la información necesaria. Daremos los desfases para los años en el período de vida del Libertador Simón Bolívar.

Tabla Cronológica

1783	1784	1785	1786	1787	1788	1789	1790	1791	1792
6	1	2	3	5	6	7	1	3	4
1793	1794	1795	1796	1797	1798	1799	1800	1801	1802
4	5	6	1	2	3	4	5	6	7
1803	1804	1805	1806	1807	1808	1809	1810	1811	1812
1	3	4	5	6	1	2	3	4	6
1813	1814	1815	1816	1817	1818	1819	1820	1821	1822
7	1	2	4	5	6	7	2	3	4
1823	1824	1825	1826	1827	1828	1829	1830		
5	7	1	2	3	5	6	7		

Ciclos Lunares

El ciclo lunar o ciclo metónico, es un período igual a 19 años solares. La razón de esto se debe al astrónomo griego Meton (siglo 5 a.c.), quien descubrió que 19 años solares son iguales a 235 meses lunares.

El **mes lunar** o **mes sinódico**, es el intervalo de tiempo entre dos conjunciones consecutivas del sol y la luna (4 fases lunares). Este tiene una duración de 29 días, 12 horas y 44 minutos. En la Iglesia Cristiana hubo necesidad de introducir el ciclo lunar dentro del Calendario, debido a la determinación del Domingo de Pascua, el cual depende de la luna llena, como ya hemos explicado.

Los años del ciclo metónico se llaman **años dorados**. El primer año de un ciclo es aquel en que las fases lunares del mes de enero de dicho año comienzan el 24 de diciembre. Así, por ejemplo en el año 1 de la Era Cristiana se inició un ciclo metónico. Luego en año 1 d.c. tiene número dorado 1, el año 2 d.c. tiene número dorado 2 ,..etc. Luego el año 20 tiene número de oro 1, y asi sucesivamente.

La regla para calcular el número de oro t, de un año x cualquiera es:

$$t \equiv x + 1 \ mod\ 19$$

Por ejemplo 1993 tiene número de oro 18, pues

$$1993 + 1 = 1994 \equiv 18 \ mod\ 19$$

2.4 Trucos de divisibilidad

Existen criterios prácticos para decidir cuándo un número es divisible entre 3,9, 11,$\cdots$ etc. Todos estos criterios están basados en las congruencias y son fáciles de interpretar, una vez vistos los resultados previos, en donde se estudiaron las reglas de manipulación de ecuaciones de congruencias.

Criterio de divisibilidad entre nueve

Proposición 2.4.1 *Un número x es divisible entre nueve si y sólo si la suma de sus dígitos es divisible entre nueve.*

Demostración:

En primer lugar notemos que

$$10 \equiv 1 \ mod\ 9$$

Multiplicando esta ecuación por sí misma tantas veces como se desee

$$10^i \equiv 1 \ mod\ 9 \quad \text{para todo } \ 1 \leq i.$$

Sea ahora x un número positivo cualquiera. Entonces x tiene una descomposición decimal, y por lo tanto existen enteros c_i, $0 \leq i \leq n$, tales que

$$x = c_n 10^n + \ldots c_1 10 + c_0$$

donde $0 \leq c_i \leq 9$, para todo i. Luego

$$x = c_n 10^n + \ldots + c_1 10 + c_0 \equiv c_n + \ldots + c_1 + c_0 \ mod\ 9$$

Como consecuencia de lo anterior, hemos demostrado que x es congruente módulo 9 a la suma de sus dígitos. Entonces x es un múltiplo de 9 si y sólo si la suma de sus dígitos lo es.

Ejemplo: El entero 1575 es divisible entre 9, pues

$$1 + 5 + 7 + 5 = 18 = 2 \times 9.$$

Criterio de divisibilidad entre 3

Proposición 2.4.2 *Un número es divisible entre 3 si y sólo si la suma de sus dígitos es divisible entre 3.*

Veamos ahora otra aplicación práctica de las congruencias, en la obtención de un viejo truco para verificar el resultado de una multiplicación, llamado **Eliminación de los Nueve**. Si se multiplican dos números a y b, para obtener un resultado c, entonces daremos un método para verificar si c es el resultado correcto. Este método falla en un 10 por ciento de los casos, pero sin embargo es apropiado para esta tarea, debido a la simplicidad del mismo.

Eliminación de los nueve

Proposición 2.4.3 *Si en la multiplicación de a por b se obtiene un entero c, entonces al sumar los dígitos de cada una de los tres números se obtienen enteros a', b' y c', los cuales deben satisfacer: $a' \times b' = c'$.*

Daremos un ejemplo práctico para ilustrar este método.

786	$7+8+6=21$	$2+1=3$	3
x219	$2+1+9=12$	$1+2=3$	x3
172134	$1+7+2+1+3+4=18$	$1+8=9$	9

La prueba de la proposición, es una consecuencia del criterio de divisibilidad entre nueve, pues

$$a \equiv a' \ mod\ 9 \quad \text{y} \quad b \equiv b' \ mod\ 9,$$

Luego se tiene

$$ab \equiv a'b' \ mod\ 9$$

o sea

$$c \equiv c' \ mod\ 9.$$

Ejercicios

1) Hallar criterios de divisibilidad para 2 y 5. Justificarlos.

2) Hallar y probar un criterio de divisibilidad para 11.

3) Hallar y probar un criterio de divisibilidad para 7.

4) Existe un método para multiplicar, que fue muy popular en Europa durante la Edad Media, en el cual sólo se requiere la tabla de multiplicación hasta el número cinco. Supongamos que queremos multiplicar 7 por 8. Entonces la diferencia de 8 con 10 es 2 y la diferencia de 7 con 10 es 3. Multiplicando ambas diferencias nos da: $2 \times 3 = 6$. Este es el primer dígito del resultado. Luego a 7 se le resta la diferencia del 8 (o bien a 8 se le resta la diferencia de 7) y en cualquiera de los dos casos nos da 7-3 = 8-2 = 5 . Este es el otro dígito del número buscado. Podemos ilustrar este algoritmo, mediante el diagrama:

Dar una demostración de este algoritmo.

5) Demuestre que el almanaque se repite cada 28 años.

6) Usando la tabla cronológica hallar los días de la semana de las fechas siguientes.

a) 25 de marzo de 1.815
b) 6 de enero de 1.799
c) 24 de diciembre de 1803

7) Demostrar que el error cometido al medir el tiempo con el Calendario Juliano es de un día cada 128 años.

8) Calcular el error que se comete al medir el tiempo con el Calendario Gregoriano.

9) Usando el truco de eliminación de los nueve, verificar las operaciones siguientes.
a) $1.254 \times 456 = 571.824$
b) $6.532 \times 123 = 893.436$
c) $1.223 \times 362 = 442.626$
d) $125 \times 337 = 41.125$

10) Hallar el valor de x que satisfaga
a) $x^2 \equiv -1 \ mod\ 7$
b) $2^x \equiv 1 \ mod\ 5$
c) $x^3 + 4x - 1 \equiv 0 \ mod\ 7$

2.5 Clases de congruencias

Hemos visto que para un número positivo m fijo, la relación módulo m en el conjunto de enteros es de equivalencia. En esta sección, veremos cómo se puede dotar al conjunto de las clases de congruencias de una estructura algebráica.

Supondremos que el lector está familiarizado con los conceptos de **operación binaria, grupo y anillo** . De cualquier forma, daremos un breve repaso a estos conceptos con la finalidad de hacer esta sección autocontenida.

Definición 2.5.1 *Sea A un conjunto no vacío. Una* **operación binaria** *en A es una ley que asocia a cada par de elementos (a, b) de $A \times A$ otro elemento de A el cual será denotado por $a * b$. Esto se simboliza por*

$$* : A \times A \longrightarrow A$$

$$(a, b) \longrightarrow a * b$$

Definición 2.5.2 *Un* **Grupo** *es un conjunto no vacío G, el cual está dotado de una operación binaria $*$, la cual satisface*

1. *Para a y b en G, $a * b$ está en G.*

2. *Para a, b y c en G*

$$(a * b) * c = a * (b * c)$$

3. *Existe un elemento e en G, llamado el elemento neutro de G, el cual satisface:*

$$a * e = e * a = a \quad \textit{para todo } a \textit{ en } G.$$

4. *Para todo a en G, existe un elemento en G, llamado el inverso de a, el cual denotamos por a^{-1}, con la propiedad:*

$$a * a^{-1} = a^{-1} * a = e.$$

Si además de las cuatro propiedades anteriores, el grupo G posee la propiedad adicional

$$a * b = b * a$$

para todo a y b en G, entonces diremos que G es un **grupo abeliano**.

Ejemplo: El conjunto de los números enteros con la suma $(\mathbb{Z}, +)$ es un grupo abeliano.

Ejemplo: El conjunto de las fracciones no nulas bajo el producto, $(\mathbb{Q}^*, .)$ es un grupo abeliano.

Definición 2.5.3 *Sea $\mathbb{R}$ un grupo abeliano con operación *. Diremos que $\mathbb{R}$ es un* **anillo**, *si en $\mathbb{R}$ está definida otra operación $\oplus$, la cual verifica:*

1. *Para a y b en $\mathbb{R}$, $a \oplus b$ está en $\mathbb{R}$.*

2. *para a, b y c en $\mathbb{R}$*

$$(a \oplus b) \oplus c = a \oplus (b \oplus c)$$

3. Para todos a, b y c en $\mathbb{R}$

$$a \oplus (b * c) = a \oplus b * a \oplus c$$

y

$$(a * b) \oplus c = a \oplus c * b \oplus c$$

Notación: El anillo $\mathbb{R}$ con las dos operaciones *, $\oplus$, se denota por $(\mathbb{R}, *, \oplus)$.

Si además el anillo $\mathbb{R}$ satisface la propiedad

$$a \oplus b = b \oplus a \quad \text{para todo } a, b \text{ en } \mathbb{R},$$

entonces diremos que $\mathbb{R}$ es un **anillo conmutativo**.

Si en $\mathbb{R}$ hay elemento identidad para el producto, es decir un elemento llamado "uno" y denotado por 1, tal que

$$1 \oplus a = a \oplus 1 = a$$

para todo a, diremos que $\mathbb{R}$ es un **Anillo Unitario**.

Ejemplo: *Los Enteros*
El conjunto $\mathbb{Z}$ de los números enteros con la suma y multiplicación, es un anillo conmutativo unitario.

Ejemplo: *Los Polinomios*
El conjunto de todos los **Polinomios** en una variable x con coeficientes enteros, con las operaciones de suma y producto de polinomios, es un anillo conmutativo unitario. Este anillo se denota por $\mathbb{Z}[x]$.

Enteros módulo m

A continuación daremos un ejemplo de anillo, que será de importancia fundamental en todo el desarrollo de la teoría de números. Consideremos un entero positivo m, y sea $\mathbb{Z}_m$ el conjunto de clases de equivalencia módulo m. Entonces hay dos operaciones definidas en $\mathbb{Z}_m$.

1. **Suma módulo** m, definida por
$$[a] + [b] = [a + b]$$
2. **Producto módulo** m, definida por
$$[a] \cdot [b] = [a \cdot b]$$

Antes de pasar a ver las propiedades de este par de operaciones, debemos asegurarnos de que no hay ambigüedades en la definición. Esto es, si sumamos dos clases usando distintos representantes: ¿Se obtendrá el mismo resultado? Es decir, si a_1, a_2, b_1, b_2 son enteros tales que

$$[a_1] = [a_2] \quad \text{y} \quad [b_1] = [b_2]$$

entonces debemos asegurarnos, para evitar dudas, que:

$$[a_1] + [b_1] = [a_2] + [b_2]$$

Si esto se cumple, diremos que la suma módulo m **está bien definida**.

Notemos en primer lugar que si $[a_1] = [a_2]$ entonces

$$a_1 \equiv a_2 \ mod \ m$$

Igualmente, de $[b_1] = [b_2]$ se desprende

$$b_1 \equiv b_2 \ mod \ m$$

Por lo tanto podemos sumar ambas congruencias para obtener

$$a_1 + b_1 \equiv a_2 + b_2 \ mod \ m,$$

lo cual implica

$$[a_1 + b_1] = [a_2 + b_2],$$

luego $[a_1] + [b_1] = [a_2] + [b_2]$.

De igual manera, para el producto tenemos

$$[a_1].[b_1] = [a_2].[b_2].$$

Concluimos de esta manera que la suma y el producto módulo m están bien definidas.

Proposición 2.5.1 *Sea m un entero positivo. Entonces el conjunto $\mathbb{Z}_m$ de las clases de congruencias módulo m, con las operaciones de suma y producto módulo m es un anillo conmutativo con unidad.*

Demostración:

Ejercicio. ♠

Ejemplo: Consideremos $\mathbb{Z}_6$, el anillo de los enteros módulo 6. Podemos construir una tabla para la operación de suma, para lo cual colocaremos todos los elementos de $\mathbb{Z}_6$ en la primera columna y en la primera fila de la tabla

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Ejercicio: Analizar la tabla anterior, verificando cada una de las operaciones y responda a las preguntas

1. ¿Por qué la tabla es simétrica con respecto a la diagonal ?
2. ¿Por qué ningún elemento se repite en una misma columna o fila?
3. ¿Por qué aparece el cero en todas las filas y columnas?

Podemos construir una tabla para el producto módulo 6, de la misma forma como lo hicimos para la suma.

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Si analizamos esta tabla, vemos que en la columna del elemento 2, no aparece el elemento 1. Luego no existe elemento x tal que $[2] \cdot [x] = 1$. Por lo tanto los enteros módulo 6 no forman un grupo bajo el producto, pues el elemento [2] no posee inverso.

Definición 2.5.4 *Un anillo conmutativo con unidad $\mathbb{R}$, en donde todo elemento posee inverso bajo el producto, se llama un* **Cuerpo.**

Observación : Si el anillo conmutativo unitario $\mathbb{R}$ es finito, entonces la existencia de elementos inversos para el producto es equivalente a la ley de cancelación para el producto. La cual establecemos a continuación:

Ley de cancelación para el producto: Si a, b y c son elementos de $\mathbb{R}$ tales que $a \neq 0$, entonces

$$a \cdot b = a \cdot c \quad \text{implica} \quad b = c$$

La prueba de esto se deja como ejercicio para el lector.

Veamos bajo que condiciones sobre m, se cumple la ley de cancelación en $\mathbb{Z}_m$.

Teorema 2.5.1 *Sea a un entero positivo y $(a, m) = d$. Entonces si*

$$ab \equiv ac \ mod \ m,$$

se tiene

$$b \equiv c \ mod \ \frac{m}{d}$$

Demostración:

Tenemos por hipótesis que $m \mid a(b-c)$. Luego m/d divide a $a/d(b-c)$ y además $(\frac{m}{d}, \frac{a}{d}) = 1$. Luego concluimos que m/d divide a $b - c$, de donde se obtiene

$$b \equiv c \ mod \ \frac{m}{d}$$

♠

Ejemplo: Sea la congruencia $3 \times 2 \equiv 3 \times 4 \ mod \ 6$. Notar que $(3, 6) = 3$ y por lo cual se tiene $2 \equiv 4 \ mod \ 2$.

Proposición 2.5.2 *Sea p un primo y a un entero positivo, tal que $(p, a) = 1$, entonces si*

$$ab \equiv ac \; mod \; p, \quad se \; tiene \quad b \equiv c \; mod \; p.$$

Finalmente, podemos caracterizar los anillos $\mathbb{Z}_m$, que son cuerpos.

Teorema 2.5.2 *El anillo de clases de congruencias $\mathbb{Z}_p$ es un cuerpo sí y sólo si p es primo.*

Demostración:

Ejercicio. ♠

Ejercicios

1) Construir tablas para las operaciones de suma y producto módulo 7.

2) Usando las tablas anteriores, resolver la congruencias

1. $2a \equiv 3 \; mod \; 7$
2. $5a \equiv 4 \; mod \; 7$

3) Un elemento $a \neq 0$ en un anillo $\mathbb{R}$, se dice que es un **divisor de cero**, si existe un $b \neq 0$ en $\mathbb{R}$, tal que $a \cdot b = 0$. Demostrar que no hay divisores de cero en Z_p, con p primo.

4) Demuestre que el anillo $\mathbb{Z}_m$ tiene exactamente m elementos.

5) Demuestre que en un grupo siempre se puede resolver la ecuación: $a * x = b$.

6) Sea $\mathbb{R}$ un anillo y a, b y c elementos de $\mathbb{R}$. ¿Bajo que condiciones sobre estos elementos, se puede resolver la ecuación: $a \cdot x + b = c$?

7) Demuestre que si $f(x)$ y $h(x)$ son dos polinomios con coeficientes reales, se cumple que

$$f(x)h(x) = h(x)f(x).$$

8) Demuestre que no existe divisores de cero en el anillo de polinomios sobre los reales.

9) Probar que $[a], [b]$ y $[c]$ son tres clases de congruencia módulo m, se cumple que

$$[a] + ([b] + [c]) = ([a] + [b]) + [c].$$

10) Si p es un número primo probar que $\mathbb{Z}_p$ es un cuerpo.

11) Sea A el conjunto de los números reales de la forma $a + b\sqrt{2}$, con a y b números racionales. Probar que A es un cuerpo con las operaciones de suma y producto de números reales.

12) Probar que en la tabla de operación de un grupo no pueden haber elementos repetidos en una misma fila o columna.

2.6 Ecuaciones lineales de congruencia

Una ecuación del tipo

$$a \cdot x \equiv b \; mod \; m \tag{2.1}$$

se llama **ecuación lineal de congruencia**.

Observación: Si x_0 es solución de (2.1), y x_1 es otro entero tal que $x_1 \equiv x_0 \; mod \; m$, entonces x_1 también será solución de la ecuación. Así pues, si (2.1) posee solución, entonces posee infinitas. Sin embargo sólo nos interesan aquellas soluciones que no sean congruentes entre si.

Volviendo a la ecuación anterior, podemos expresarla como

$$a \cdot x - m \cdot y = b \tag{2.2}$$

donde y es un entero a determinar.

Una ecuación del tipo (2.2) se denomina **ecuación lineal diofántica** en las variables x e y. Se supone que las soluciones de esta ecuación son números enteros.

Diofantos de Alejandría fue uno de los grandes matemáticos griegos y escribió sus obras a mediados del siglo 3 d.c. La más importante es la *Aritmética*, que consistía en el estudio de resolución de ecuaciones, como por ejemplo la ecuación $Ax^2 + C = y^2$.

Ejemplo:
Resolver

$$7 \cdot x + 15 \cdot y = 12$$

Solución:

Usaremos el método de Euler, que consiste en despejar una de las incógnitas con menor coeficiente, en función de la otra.

Esto nos conduce a establecer una ecuación diofántica con coeficientes menores.

Se tiene entonces

$$x = \frac{12 - 15 \cdot y}{7} = 1 - 2 \cdot y + \frac{5 - y}{7}$$

Si se requiere que x e y sean enteros, se debe tener

$$z = \frac{5 - y}{7} \quad \textit{entero.}$$

Luego

$$y = 5 - 7 \cdot z$$

Dándole valores enteros arbitrarios a z, podemos obtener valores enteros de x e y, que cumplen la ecuación original. Expresando x e y en función de z se deduce

$$x = -9 + 15 \cdot z$$

$$y = 5 - 7 \cdot z.$$

Siendo z cualquier entero. Por ejemplo, haciendo $z = 0$ se tiene $x = -9$, $y = 5$, lo cual nos da una solución a la ecuación.

Como veremos enseguida, la ecuación lineal diofántica siempre se puede resolver si se cumplen ciertas condiciones sobre los coeficientes a, b y c.

Teorema 2.6.1 *La ecuación*

$$ax + by = c \tag{2.3}$$

tiene solución si y sólo si $d \mid c$, *donde* $d = (a, b)$.

Demostración:

Notemos en primer lugar que $d \mid a$, y $d \mid b$. Por lo tanto, si la ecuación (2.3) tiene solución (x, y) se tiene que $d \mid ax + by$, y luego $d \mid c$.

Recíprocamente, supongase que $d \mid c$. Dividiendo entre d la ecuación original, nos da

$$a'x + b'y = c' \tag{2.4}$$

donde $a' = a/d$, $b' = b/d$ y $c' = c/d$. Es claro que si (2.4) tiene solución, entonces (2.3) también posee solución y viceversa. Luego ambas ecuaciones son equivalentes.

Notemos que $(a', b') = 1$, y por lo tanto existen enteros x'_0 e y'_0 tales que

$$a'x'_0 + b'y'_0 = 1$$

Luego es fácil verificar que $x_0 = c'x'_0$ e $y_0 = c'y'_0$ son soluciones de (2.4) y por ende soluciones de (2.3).

Teorema 2.6.2 *Si la ecuación lineal diofántica (2.3) posee solución y* (x_0, y_0) *es una solución particular, entonces toda otra solución* (x, y) *es de la forma*

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t$$

donde t *es cualquier entero.*

Demostración:

En primer lugar, probaremos que x e y son solución. En efecto

$$a(x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + by_0 = c$$

Por otro lado si (x, y) es cualquier solución de (2.3), también lo será de (2.4) y en consecuencia

$$a'(x - x_0) + b'(y - y_0) = c' - c' = 0$$

de donde

$$a'(x - x_0) = -b'(y - y_0)$$

De acá se deduce $a' \mid b'(y - y_0)$ y por lo tanto $a' \mid (y - y_0)$. Luego $y = y_0 + a't$, donde t es un entero. Igualmente, se verifica $x = x_0 + b's$, con s entero.

Probaremos que $s = -t$, para lo cual sustituimos la solucion (x, y) en (2.4)

$$a'(x_0 + b's) + b'(y_0 + a't) = c'$$

$$a'x_0 + b'y_0 + a'b'(s + t) = c'$$

como (x_0, y_0) es solución de (2.4) se tiene $a'x_0 + b'y_0 = c'$, y por lo tanto

$$c' + a'b'(s + t) = c'$$

o sea

$$a'b'(s + t) = 0$$

de donde $s = -t$. Con esto termina la demostración.

♠

Teorema 2.6.3 *La ecuación lineal de congruencia*

$$ax \equiv b \ mod \ m \tag{2.5}$$

posee solución si y sólo si $d \mid b$, donde $d = (a, m)$. Si x_0 es una solución particular de (2.5), entonces la solución general viene dada por

$$x \equiv x_0 \ mod \ \frac{m}{d}.$$

Demostración:

Podemos expresar la ecuación anterior como

$$ax - my = b \tag{2.6}$$

De acuerdo al teorema anterior, sabemos que (2.6) posee solución y además la solución general para la x viene expresada mediante:

$$x = x_0 + \frac{m}{d}t.$$

Para finalizar la demostración, observemos que las d soluciones

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

son todas distintas módulo m. ♠

Ejemplo:
Resolver

$$30x \equiv 15 \ mod \ 21$$

Solución:

Obsérvese que $(30, 21) = 3$, y 3 divide a 15. Luego la ecuación tiene solución. El número de soluciones módulo 21 será igual a $(21, 30) = 3$.

Con la finalidad de hallar una solución particular, procederemos a dividir entre 3 la ecuación. Luego

$$10x \equiv 5 \ mod \ 21$$

esto es

$$3x \equiv 5 \ mod \ 7$$

Por simple inspección, calculamos una solución $x \equiv 4 \ mod \ 7$. Luego las tres soluciones distintas módulo 21 son: 4, 11 y 18.

Ejemplo:

Resolver

$$238x + 125y = 31$$

Solución:

En este ejemplo se puede reducir el tamaño de los coeficientes, mediante un cambio de variables. Podemos reescribir la ecuación anterior

$$125(y + 2x) - 12(x + 2) = 7$$

Empleamos ahora el siguiente cambio de variables

$$X = x + 2, \quad Y = y + 2x$$

Luego la ecuación original se transforma en

$$125Y - 12X = 7$$

Resolviendo tenemos

$$X = \frac{125Y - 7}{12} = 10Y + \frac{5Y - 7}{12}$$

Nuevamente, haciendo el cambio de variable

$$z = \frac{5Y - 7}{12}$$

de donde

$$Y = \frac{12z + 7}{5} = 2z + 1 + \frac{2z + 2}{5}$$

Luego $\dfrac{2z + 2}{5}$ es un entero y por lo tanto hacemos $z = -1$.

De aquí obtenemos los resultados

$$Y = -1, \quad X = -11$$

volviendo al cambio de variables

$$y = 15, \quad x = -13$$

Luego la solución de la ecuación original viene expresada por

$$x = -13 + 125t, \quad y = 15 - 238t$$

Estudiemos ahora el problema de resolver una ecuación de congruencia con más de una indeterminada.

Ejemplo:
Resolver

$$3x + 4y \equiv 11 \ mod \ 14 \tag{2.7}$$

En primer lugar, observamos que $14 = 7 \cdot 2$. Luego es posible trabajar con módulos 7 ó 2, para hallar soluciones de (2.7). Escogemos el 2 por ser menor. Luego tomando la misma ecuación módulo 2 se obtiene

$$3x + 4y \equiv 11 \ mod \ 2$$

o sea

$$3x \equiv 1 \ mod \ 2$$

De esta ecuación provienen 7 soluciones distintas módulo 14 para x, las cuales son: 1, 3, 5, 7, 9, 11 y 13. Al sustituir cada una de éstas en la ecuación original, se obtendrán las correspondientes soluciones para la y.

Por ejemplo, si se considera $x \equiv 1 \ mod \ 14$, se tendrá

$$3x + 4y \equiv 11 \ mod \ 14$$

o bien

$$4y \equiv 8 \ mod \ 14$$

Notemos que $(14, 2) = 2$, luego podemos simplificar:

$$2y \equiv 4 \ mod \ 7$$

Luego las soluciones de y módulo 14 son 2 y 9.

Usaremos pares ordenados para indicar las soluciones de la ecuación (2.7), donde la primera componente indica la x y la segunda indica la y. De esta forma, se obtienen las soluciones $(1, 2)$ y $(1, 9)$.

Las restantes soluciones son:

$$(3,4),\ (3,11),\ (5,6),\ (5,13),\ (7,1),\ (7,8),$$
$$(9,3),\ (9,10),\ (11,5),\ (11,12),\ (13,7),\ (13,14).$$

Teorema 2.6.4 *La congruencia*

$$a_1x_1 + a_2x_2 + \ldots + a_nx_n \equiv c\ mod\ m$$

es soluble si y sólo si $d \mid c$, *donde* $d = (a_1, a_2, \ldots, a_n, m)$.

El número de soluciones distintas módulo m *es* dm^{n-1}.

Demostración:

Haremos la demostración para el caso $n = 2$. El caso general se deduce de este caso particular y del principio de inducción.

Consideremos entonces

$$a_1x + a_2y \equiv c\ mod\ m \tag{2.8}$$

donde $(a_1, a_2, m) = d$ y $d \mid c$.

Es fácil ver que la condición $d \mid c$ es necesaria para la existencia de la solución. Probaremos que esta condición es también suficiente.

A tal efecto, sea $(a_2, m) = d'$. Luego de (2.8) obtenemos

$$a_1x \equiv c\ mod\ d' \tag{2.9}$$

Notemos que $(d', a_1) = ((a_2, m), a_1) = d$, y $d \mid c$. Luego (2.9) posee d soluciones distintas módulo d', de acuerdo al teorema 2.6.3. Estas d soluciones, generan $d \cdot m/d'$ soluciones distintas módulo m para x.

Para cada solución x, se reemplaza su valor en la ecuación (2.8) para obtener

$$a_2 y \equiv c - a_1 x \ mod \ m$$

Teniendo en cuenta que: $(m, a_2) = d'$, y además: $d' \mid c - a_1 x$, se deduce entonces que la ecuación anterior posee d' soluciones distintas para y módulo m.

Contando el número de soluciones de (2.8), se tendrá la ecuación

$$S = S_x \times \ S_y$$

donde S = número de soluciones de (2.8), S_x = número de soluciones para x y S_y = número de soluciones para y. Luego

$$S = d \ \frac{m}{d'} \ d' = d.m$$

2.7 Teorema Chino del Resto

El problema de resolver la congruencia

$$ax \equiv b \ mod \ m \tag{2.10}$$

puede ser bastante laborioso si m es grande, debido al número de calculos requeridos, cuando esta se resuelve usando el método de la sección anterior. Si m se factoriza como un producto de enteros $m_1.m_2 \ldots m_n$ entonces la ecuación anterior es equivalente a las ecuaciones

$$ax \equiv b \ mod \ m_i, \qquad 1 \leq i \leq n$$

Teorema 2.7.1 *Sean $m_1, m_2, \ldots, m_n$ enteros positivos. Entonces el sistema*

$$\begin{cases} ax & \equiv & b \ mod \ m_1 \\ & \vdots & \\ ax & \equiv & b \ mod \ m_n \end{cases}$$

es equivalente a la ecuación

$$ax \equiv b \ mod \ [m_1, m_2, \ldots, m_n]$$

Demostración:

Notemos que para todo i, se tiene $m_i \mid ax - b$, por hipótesis, luego $ax - b$, es múltiplo común de los m_i y por lo tanto $[m_1, \ldots, m_n]$ divide a $ax - b$. Luego

$$ax \equiv b \ mod \ [m_1, \ldots, m_n].$$

Recíprocamente, es fácil ver que toda solución de la ecuación satisface el sistema, con lo cual se da fin a la prueba.

♠

Observación: Si los m_i son primos relativos por pareja, esto es,

$$(m_i, m_j) = 1$$

para todo par de enteros $i \neq j$,

entonces se tiene

$$[m_1, \ldots, m_n] = m_1 \ldots m_n.$$

Así pues, tenemos el siguiente resultado

Teorema 2.7.2 *Si m se factoriza*

$$m = p_1^{\alpha_1}.p_2^{\alpha_2} \ldots p_n^{\alpha_n}$$

entonces la ecuación $ax \equiv b \ mod \ m$ es equivalente al sistema de n ecuaciones

$$ax \equiv b \ mod \ p_i^{\alpha_i}, \quad 1 \leq i \leq n$$

Ejemplo:
Resolver

$$7x \equiv 6 \ mod \ 100$$

Solución:

Descomponiendo a 100 como producto de primos, nos da $100 = 2^2 5^2$, luego la ecuación es equivalente al sistema

$$7x \equiv 6 \ mod \ 25$$

$$3x \equiv 2 \ mod \ 4$$

La primera ecuación tiene solución

$$x \equiv 8 \ mod \ 25,$$

o sea $x = 8, 33, 58, 83, \ldots$.

La segunda ecuación tiene solución

$$x \equiv 2 \ mod \ 4,$$

esto es $x = 2, 6, 10, 14, 18, 22, 26, 30, 34, 38, 42, 46, 50, 54, 58, 62, \ldots$.

Luego la solución común viene expresada por

$$x \equiv 58 \ mod \ 100$$

Ejemplo:

Ahora planteamos un problema de la antigua China, que data del año 1275 d.c.

"Hallar un número tal que, al ser dividido por siete da uno como residuo, al ser dividido por ocho da dos como residuo y al ser dividido por nueve da tres como residuo".

Solución:

Podemos plantear el problema en términos de congruencias de la siguiente manera; sea x el número buscado, entonces

$$\begin{cases} x & \equiv & 1 \ mod \ 7 \\ x & \equiv & 2 \ mod \ 8 \\ x & \equiv & 3 \ mod \ 9 \end{cases}$$

De la primera ecuación obtenemos

$$x = 1 + 7k$$

Sustituyendo en la segunda ecuación

$$1 + 7k \equiv 2 \ mod \ 8$$

de donde

$$7k \equiv 1 \ mod \ 8$$

Luego

$$k \equiv 7 \ mod \ 8,$$

y por lo tanto $k = 7 + 8l$. Sustituyendo en la expresión de x nos da: $x = 50 + 56l$. Este último valor de x lo sustituimos en la tercera ecuación para obtener

$$50 + 56l \equiv 3 \ mod \ 9$$

y después de reducir módulo 9 nos queda: $l = 8 + 9j$.

Finalmente, si se remplaza el valor de l en la expresión de x produce

$$x = 50 + 56(8 + 9j) = 498 + 504j$$

de donde se concluye

$$x \equiv 498 \ mod \ 504$$

Proposición 2.7.1 *Sean m_1 y m_2 enteros primos relativos. Entonces existen enteros x_0 y x_1 tales que*

$$\begin{array}{ll} x_0 \equiv 1 \ mod \ m_1 & x_0 \equiv 0 \ mod \ m_2 \\ x_1 \equiv 0 \ mod \ m_1 & x_1 \equiv 1 \ mod \ m_2 \end{array} \tag{2.11}$$

Demostración:

Sabemos que existen enteros s y t tales que

$$s \cdot m_1 + t \cdot m_2 = 1$$

Luego $s \cdot m_1 \equiv 1 \ mod \ m_2$ y $s \cdot m_1 \equiv 0 \ mod \ m_1$. Similarmente $t \cdot m_2 \equiv 1 \ mod \ m_1$ y $t \cdot m_2 \equiv 0 \ mod \ m_2$. Tomar entonces $x_0 = t \cdot m_2$ y $x_1 = s \cdot m_1$.

♠

Proposición 2.7.2 *Sean m_1 y m_2 enteros primos relativos. Entonces dados dos enteros cualesquiera a y b, existe un entero x que satisface*

$$x \equiv a \ mod \ m_1$$

$$x \equiv b \ mod \ m_2$$

Demostración:

Tomar $x = a \cdot x_0 + b \cdot x_1$, donde x_0 y x_1 satisfacen la condición (2.11)

♠

Teorema 2.7.3 *(Teorema Chino del Resto)*
Sean $m_1, \ldots, m_n$ enteros positivos, primos relativos por parejas. Entonces si $a_1, \ldots, a_n$ son enteros cualesquiera, el sistema

$$\begin{cases} x & \equiv a_1 \mod m_1 \\ & \vdots \\ x & \equiv a_n \mod m_n \end{cases}$$

posee solución. Además si $m = m_1 \cdots m_n$, cualquier par de soluciones son congruentes módulo m.

Demostración:

Usaremos inducción sobre n. Para $n = 1$ el teorema es cierto. Supongase que el sistema

$$\begin{cases} x & \equiv a_1 \mod m_1 \\ & \vdots \\ x & \equiv a_{n-1} \mod m_{n-1} \end{cases}$$

posee solución única x_0 módulo $m' = m_1 \cdot m_2 \cdots m_{n-1}$.

Entonces el sistema original se puede reducir a resolver

$$x \equiv x_0 \mod m'$$

$$x \equiv a_n \mod m_n$$

Tenemos entonces que $(m_n, m') = (m_n, m_1 \ldots . m_{n-1}) = 1$. Luego podemos aplicar la proposición anterior para hallar la solución buscada, la cual será única módulo $m_1 \cdots m_n$, por hipótesis de inducción.

Aplicación del teorema chino en cronología

Una de las medidas más usadas en la cronología histórica es la de los **días julianos**. Los días julianos tienen la misma duración que los días

solares, sin embargo éstos se cuentan a partir del primero de enero del 4713 a.c., el cual es el día juliano 1, y de allí en adelante se enumeran los días en sucesión creciente.

Este sistema fue ideado por **Joseph Justus Scaliger** de Leyden, y apareció por primera vez en su obra "*De emendatione temporum*" (París 1583).

Estos días julianos se agrupan en períodos de 7980 años. Cada uno de estos períodos se denomina **Ciclo Juliano o Período Juliano**. La razón para elegir semejante número, la veremos a continuación.

Tenemos que $7980 = 28 \times 19 \times 15$ y cada uno de estos factores tiene un significado muy especial dentro de los calendarios de distintas cronologías

El número 28 corresponde al llamado **Ciclo Solar** de 28 años. Este es el ciclo más pequeño en el cual los días de la semana y las fechas del calendario se repiten. El primer año de un ciclo solar es aquel, en donde el día primero de enero es lunes. Por ejemplo, el año 1560 tiene año solar 1.

El número 19 corresponde al **Ciclo Metónico o Ciclo Lunar**, el cual dura 19 años. Este es el menor ciclo en el cual las fases de la luna se repiten en las mismas fechas del calendario. Este proviene del astrónomo griego Meton (siglo V a.c.), quién descubrió que 19 años solares corresponden exactamente a 235 lunaciones o meses lunares. Los años del ciclo metónico se llaman **Años Dorados**. Este sistema fue introducido por el Emperador Dionisio Exigus en el año 533 d.c. y este año tiene año dorado 1.

Finalmente, el número 15 corresponde a otro ciclo, el cual no tiene nada que ver con astronomía. Se trata del ciclo de recolección de impuestos en la antigua Roma que constaba de 15 años y se llama la **indicción**. Este ciclo fue introducido por el Emperador Constantino en el año 313 d.c. correspondiendo a este año el primer año de dicho ciclo.

La idea de Scaliger era usar un sistema de cronología que incluyera todos estos ciclos. Esto permitiría calcular fácilmente una fecha determinada al pasar de un sistema a otro. El problema entonces era

escoger una fecha apropiada para iniciar la cuenta de los años julianos. Se necesitaba un año x de la historia, tal que en ese año se diera inicio a los tres ciclos. Esto es, x debe tener

$$\begin{array}{c}\text{Año solar} = 1\\ \text{Año dorado} = 1\\ \text{Año de indicción} = 1\end{array}$$

Usando congruencias, se debe tener el sistema

$$\begin{cases} x \equiv 1560 \mod 28 \\ x \equiv 532 \mod 19 \\ x \equiv 313 \mod 15 \end{cases}$$

Reduciendo esto se tiene

$$\begin{cases} x \equiv 20 \mod 28 \\ x \equiv 0 \mod 19 \\ x \equiv 13 \mod 15 \end{cases}$$

Nótese que (28, 27) = 1, (28,15) = 1 y (15,19) = 1. Luego por el Teorema Chino del Resto, el sistema anterior posee solución.

A fin de determinar el valor de x, comenzaremos por usar la primera ecuación. Luego

$$x = 20 + 28k \quad \text{con } k \text{ entero.}$$

Usando la segunda ecuación nos queda

$$20 + 28k \equiv 0 \mod 19$$

$$1 + 9k \equiv 0 \mod 19$$

$$9k \equiv 18 \mod 19$$

de donde

$$k \equiv 2 \mod 19$$

Luego

$$k = 2 + 19s$$

y por lo tanto volviendo a x en la última ecuación tenemos

$$76 + 532s \equiv 13 \ mod \ 15$$

$$1 + 7s \equiv 13 \ mod \ 15$$

luego, $7s \equiv 12 \ mod \ 15$, de donde $s \equiv 6 \ mod \ 15$. Por lo tanto $s = 6+15t$.

Nuevamente, si reemplazamos este valor en la expresión para x nos da

$$x = 76 + 532(6 + 15t) = 326 + 7980t$$

Luego la solución viene dada por

$$x \equiv 3268 \ mod \ 7980$$

Sin embargo, descartamos el año 3268 por ser del futuro y buscamos el año y en que se inició el período juliano anterior. Esto es

$$y = 3268 - 7980 = -4712$$

En el calendario gregoriano, el año -4712 corresponde al 4713 a.c. (no hay año 0) y éste se toma como el año 1 juliano.

Ejemplo: Conociendo el año juliano de un año cualquiera, podemos calcular su año solar, dorado y de indicción; basta tomar los restos de la división del número entre 28, 19 y 15 respectivamente. Por ejemplo para buscar el año juliano de 1993, el cual llamaremos x, hacemos

$$x = 4713 + 1993 = 6706$$

Luego dividimos a 6706 entre 28, 19 y 15 respectivamente para obtener los restos que nos dan toda la información. Por lo tanto

Año solar de 1993 = 14
Año dorado de 1993 = 18
Año de indicción de 1993 = 1

Ejercicios

1) Resolver

$$238x + 133y = 31$$

2) Resolver

$$15x + 30y = 720$$

3) Resolver

$$7x + 11y = 150$$

4) Resolver las ecuaciones de congruencia.
   a) $12x \equiv 7 \ mod\ 17$
   b) $11x \equiv 7 \ mod\ 84$
   c) $18x \equiv 1 \ mod\ 25$

5) Resuelva el sistema

$$\begin{cases} x & \equiv 1 & mod\ 2 \\ x & \equiv 2 & mod\ 3 \\ x & \equiv 3 & mod\ 5 \\ x & \equiv 5 & mod\ 7 \end{cases}$$

6) Resuelva la congruencia

$$2x + 3y \equiv 15 \ mod\ 16$$

7) Hacer una tabla en donde aparezcan los años solares, dorados y de indicción para el período comprendido entre 1800 y 1850.

8) Demostrar que si x_0 es un entero y $d|m$, entonces los d enteros

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

son todos diferentes módulo m.

9) Un comerciante compró un lote de juguetes de dos tipos distintos por Bs. 50.000. El primer tipo cuesta Bs. 1.950 por unidad, y el segundo tipo cuesta Bs. 770. ¿Qué cantidad de juguetes de cada tipo compró el comerciante?.

10) Resolver

$$1050x + 6y + 462z \equiv 6 \ mod \ 12$$

11) En X se celebraron eleciones para elegir el Presidente en 1994. En 1992 se realizaron elecciones para elegir gobernadores. Si el período de mando de los presidente es de 5 años, y el de los gobernadores de 8, entonces determine en qué año coincidirán ambas elecciones.