Tema 3: Ecuaciones diofánticas, congruencias y criterios de divisibilidad

J. Sendra, E. Martín, A. Méndez y C. Ortiz

Marzo 2011

Índice

Guía del tema

Asignatura:	Matemática Discreta
Titulo de la Unidad:	Ecuaciones diofánticas, congruencias y criterios de divisibilidad
Semanas de impartición en el cuatrimestre:	Del 21 de marzo al 1 de abril

Requisitos para seguir con aprovechamiento el tema

- Manejar con soltura el algoritmo de la división.
- Conocer y manejar relaciones de equivalencia.
- Atención y paciencia para asimilar los resultados.
- Conocer y utilizar el principio de inducción matemática.

Objetivos

Objetivo general: Conocer y manejar ecuaciones diofánticas, congruencias y sistemas de numeración

Objetivos Específicos:

- Manejar los restos de las divisiones.
- Conocer y resolver las ecuaciones diofánticas.
- Manejar el concepto de congruencia.
- Aplicar propiedades básicas de las congruencias.
- Conocer el Teorema Pequeño de Fermat.
- Calcular el inverso de un número en $\mathbf{Z}_m$.
- Resolver Ecuaciones con congruencias.
- Entender el Teorema de los restos chinos y saber aplicar el método para resolver un sistema de congruencias.
- Conocer los comandos más básicos de Maple en relación con congruencias.
- Deducir criterios de divisibilidad a partir de resultados generales,
- Aplicar los resultados para conocer los divisores de un número entero no negativo.

Contenidos teóricos

- Ecuaciones Diofánticas
- Congruencias
- Sistemas de numeración y criterios de divisibilidad

Evaluación Se entregarán los ejercicios propuestos antes de la fecha límite **11 de abril de 2011**

1. Ecuaciones Diofánticas

Se llama ecuaciones diofánticas a una amplia clase de ecuaciones algebraicas con más de una indeterminada en $\mathbf{Z}$ y $\mathbf{Q}$. En primer lugar, se estudian las ecuaciones lineales diofánticas de la forma $ax + by = n$. A continuación, se analiza la ecuación diofántica de la forma $x^2 - y^2 = n$ con $n > 0$, así como la ecuación, también llamada pitagórica, de la forma $x^2 + y^2 = z^2$. Se termina la sección enunciando la famosa conjetura de Fermat.

Teorema 1.1. *Sean a, b y $n \in \mathbf{Z}$. La ecuación lineal $ax + by = n$ tiene solución entera x_0, y_0 si y sólo si $d = mcd(a, b)$ divide a n.*

Demostración. Si la ecuación tiene soluciones enteras x_0, y_0 entonces $ax_0 + by_0 = n$. Ahora bien, como $d \mid ax_0$ y $d \mid by_0$ se tiene que $d \mid n$. Supongamos ahora que $d \mid n$, es decir existe $r \in \mathbf{Z}$ tal que $n = dr$. Si $n = 0$ entonces $x_0 = 0$ e $y_0 = 0$ es una solución trivial de la ecuación. Si $n \neq 0$ entonces $d \neq 0$ y existen $u, v \in \mathbf{Z}$ tales que $au + bv = d$. Multiplicando por r ambos lados de esta ecuación se tiene $a(ur) + b(vr) = dr = n$, de donde se deduce que $x_0 = ur$, $y_0 = vr$ es una solución de la ecuación $ax_0 + by_0 = n$. □

Algoritmo para encontrar una solución.

Sea la ecuación diofántica $ax + by = n$. En primer lugar se calcula el $mcd(a, b)$ mediante el algoritmo de Euclides:

$$\begin{aligned} a &= bq_1 + r_1 \\ b &= r_1 q_2 + r_2 \\ &\vdots \\ r_{t-2} &= r_{t-1} q_t + r_t \\ r_{t-1} &= r_t q_{t+1} \end{aligned}$$

donde $r_t = mcd(a, b) = d$. Por tanto despejando de la penúltima ecuación se tiene:

$$r_{t-2} - r_{t-1} q_t = d$$

y substituyendo el valor de r_{t-1} de la ecuación anterior a ésta, se obtiene:

$$r_{t-2} - (r_{t-3} - r_{t-2} q_{t-1}) q_t = d$$

que es equivalente a:

$$-r_{t-3} q_t + r_{t-2}(1 + q_t q_{t-1}) = d.$$

Siguiendo este proceso de substitución ascendiendo por las igualdades, se obtiene

$$aq_1^* + bq_2^* = d$$

donde q_1^*, q_2^* son expresiones en función de $q_1, \cdots, q_t$. Por tanto, una solución de la ecuación diofántica es:

$$x_0 = \frac{nq_1^*}{d}, \quad y_0 = \frac{nq_2^*}{d}.$$

EJEMPLO 1.1. Se quiere encontrar una solución entera de la ecuación diofántica:

$$525x + 100y = 50.$$

En primer lugar observamos que mediante el algoritmo de Euclides:

$$525 = 100 \cdot 5 + 25$$

$$100 = 4 \cdot 25$$

por tanto $mcd(525, 100) = 25$ y además como $25 \mid 50$, se tiene que la ecuación diofántica tiene soluciones enteras.

Despejando de la primera ecuación se tiene:

$$525 + (-5)100 = 25$$

y en este caso obtenemos:

$$x_0 = \frac{1 \cdot 50}{25} = 2, \quad y_0 = \frac{-5 \cdot 50}{25} = -10$$

que es una solución entera de la ecuación diofántica. □

Proposición 1.1. *Sean a, b y $n \in \mathbf{Z}$. Si x_0, y_0 es una solución particular de la ecuación diofántica $ax+by = n$, entonces todas las soluciones enteras de la ecuación son de la forma*

$$x = x_0 + (b/d)t, \quad y = y_0 - (a/d)t, \quad t \in \mathbf{Z}$$

donde $d = mcd(a, b)$.

Demostración. Para los detalles sobre la demostración ver [3] Proposición 2.2.6. □

EJEMPLO 1.2. Se quiere encontrar las soluciones enteras de la ecuación diofántica del ejemplo anterior:

$$20x + 50y = 430.$$

Sabemos que $x_0 = 2$ $y_0 = -10$ es una solución particular, por tanto aplicando la proposición anterior se tiene que todas las soluciones son de la forma:

$x = 2 + (100/25)t = 2 + 4t, \quad y = -10 - (525/25)t = -10 - 21t, \quad t \in \mathbf{Z}.$ □

Ejercicio 1. Nos preguntamos si será posible llenar exactamente un depósito de 25 litros con recipientes de 6 y 8 litros.

A continuación se estudia la resolución en $\mathbf{Z}$ de las ecuaciones diofánticas de la forma $x^2 - y^2 = n$.

Teorema 1.2. *La ecuación diofántica $x^2 - y^2 = n$ con $n > 0$, tiene solución $\Leftrightarrow$ n se puede factorizar como producto de dos números de la misma paridad, es decir ambos pares o ambos impares. Si existen, las soluciones son de la forma:*

$$x = \frac{a+b}{2}, \quad y = \frac{a-b}{2}$$

donde a y b recorren todos los pares de números de la misma paridad y tales que $n = ab$.

Demostración. Para los detalles sobre la demostración ver [1] Teorema 1-4.7. □

Ejemplo 1.3. Encontrar todas las soluciones positivas de $x^2 - y^2 = 40$.

Como $40 = 2^3 5$, se tiene que 40 puede expresarse como el producto de dos números de la misma paridad como $40 = 10 \cdot 4 = 20 \cdot 2$. Por tanto, si $a = 10$ y $b = 4$ se tiene

$$x = \frac{14}{2} = 7, \quad y = \frac{6}{2} = 3$$

y si $a = 20$ y $b = 2$ se tiene

$$x = \frac{22}{2} = 11, \quad y = \frac{18}{2} = 9.$$

Por tanto, las soluciones buscadas son $\{7, 3\}$ y $\{11, 9\}$. □

Como aplicación del resultado anterior, Fermat estableció un algoritmo para estudiar si un número natural impar es compuesto.

Algoritmo de factorización de Fermat.

Sea n un número natural impar, esto es $n = a \cdot b$ con a y b impares. Por el Teorema 1.2 se puede expresar:

$$(\frac{a+b}{2})^2 - (\frac{a-b}{2})^2 = n.$$

Por tanto, el problema se traduce en resolver la ecuación: $x^2 - y^2 = n$ o equivalentemente, $x^2 - n = y^2$. Para ello, primero se determina el mínimo entero positivo q que satisfaga $q^2 \geq n$ y estudiamos si alguno de los siguientes números:

$$q^2 - n, (q+1)^2 - n, (q+2)^2 - n, \cdots$$

es un cuadrado. Obsérvese que este proceso es finito pues:

$$(\frac{n+1}{2})^2 - n = (\frac{n-1}{2})^2.$$

De todo ello se deduce que los únicos valores que hay que estudiar son los m tales que:

$$q \leq m \leq \frac{n+1}{2}.$$

Concluyendo, que si para ninguno de estos valores de m, el valor de $m^2 - n$ es un cuadrado, entonces el número n es primo.

EJEMPLO 1.4. Veamos si el número 22733 es un número compuesto. En primer lugar se obtiene que el menor q tal que $q^2 \geq 22733$ es $q = 151$. Por tanto, habrá que estudiar si alguno de los números m comprendidos entre:

$$151 \leq m \leq \frac{(22733+1)}{2} = 11367.$$

verifican si $m^2 - 22733$ es un cuadrado.

$$151^2 - 22733 = 22801 - 22733 = 68$$

$$152^2 - 22733 = 23104 - 22733 = 371$$

$$153^2 - 22733 = 23409 - 22733 = 676 = 26^2.$$

De donde se concluye que $22733 = 179 \cdot 127$. □

Analizamos ahora la ecuación diofántica de la forma:

$$x^2 + y^2 = z^2$$

con $x, y, z \in \mathbf{Z}$, también llamada ecuación pitagórica. Obsérvese que este problema es equivalente a encontrar todos los triángulos rectángulos con lados de longitud entera.

Teorema 1.3. *Las soluciones de la ecuación pitagórica $x^2 + y^2 = z^2$ que satisfacen las condiciones:*

$$mcd(x, y, z) = 1, \;\; 2 \mid x, \;\; x, y, z \in \mathbf{Z}$$

vienen dadas por las fórmulas:

$$x = 2st, \;\; y = s^2 - t^2, \;\; z = s^2 + t^2$$

para s, t con $s > t$ tales que $mcd(s, t) = 1$ y s y t tienen distinta paridad.

Demostración. Para los detalles sobre la demostración ver [1] Teorema 1-4.11. □

Conjetura de Fermat. La ecuación $x^n + y^n = z^n$ no tiene soluciones con $x, y, z \in \mathbf{N}$ cuando $n \geq 3$.

Desde mediados del siglo XVII la conjetura de Fermat ha constituido un problema del que se han ocupado numerosos matemáticos, algunos de gran renombre como por ejemplo Euler, Gauss, Legendre, Cauchy, Lamé o Dirichlet y se propusieron premios para quien demostrase su veracidad, o falsedad. En 1995 Andrew Wiles demostró un resultado, con un pequeño error detectado por Richard Taylor, mediante el que la conjetura de Fermat quedaba demostrada.

2. Congruencias

Definición 2.1. *Si m es un número entero positivo, se dice que dos números enteros a, b son **congruentes módulo** m si existe $k \in \mathbf{Z}$ tal que $a - b = km$. Simbólicamente se denota $a \equiv b \; mod(m)$.*

Observación 2.1. Siguiendo la definición anterior se tiene que

$$a \equiv b \ mod(m) \Leftrightarrow m \mid (a-b).$$

El lenguaje de congruencias fue introducido por K. Gauss a los 24 años en su libro Disquisitiones Arithmeticae, y hoy seguimos utilizándolo en la vida cotidiana. La esfera de un reloj funciona con congruencias módulo 12, los cuentakilómetros de los coches lo hacen módulo 100000 y los meses se representan módulo 12.

Ejemplo 2.1.

$$0 \equiv 8 \ \ mod(4)$$
$$-6 \equiv 4 \ \ mod(2)$$
$$18 \equiv 3 \ \ mod(5)$$

Proposición 2.1. *La relación de congruencia módulo m en $\mathbf{Z}$, es de equivalencia y divide a $\mathbf{Z}$ en clases de equivalencia de manera que dos diferentes de ellas son disjuntas.*

Demostración. Para los detalles sobre la demostración ver [3] Proposición 2.4.1. □

Proposición 2.2. *Fijado $m > 0$, cada número entero $a \in \mathbf{Z}$ es congruente módulo m con uno de los enteros $0, 1, 2 \cdots, m-1$.*

Demostración. Dividiendo a entre m, se tiene que existen q y r únicos tales que $a = qm + r$ con $0 \leq r < m$. De donde se deduce que $a \equiv r \ \ mod(m)$. □

Observación 2.2. La congruencia módulo m divide a $\mathbf{Z}$ en m clases de equivalencia que son [0],[1],[2],..,[$m-1$], cuyo conjunto cociente viene dado por

$$\mathbf{Z}_m = \{[0], [1], \cdots, [m-1]\}$$

Ejemplo 2.2. Las clases de equivalencia en $\mathbf{Z}$ módulo 3 son [0],[1], y [2]:

$$[0] = \{a \in \mathbf{Z} \setminus a \equiv 0 \ \ mod(3)\} = \{a \in \mathbf{Z} \setminus a = k \cdot 3, k \in \mathbf{Z}\} = \{\cdots, -6, -3, 0, 3, 6, \cdots\}$$

De forma análoga:

$$[1] = \{a \in \mathbf{Z} \setminus a \equiv 1 \ \ mod(3)\} = \{a \in \mathbf{Z} \setminus a = 1 + k \cdot 3, k \in \mathbf{Z}\} = \{\cdots, -5, -2, 1, 4, 7, \cdots\}$$

$$[2] = \{a \in \mathbf{Z} \setminus a \equiv 2 \ \ mod(3)\} = \{a \in \mathbf{Z} \setminus a = 1 + k \cdot 3, k \in \mathbf{Z}\} = \{\cdots, -4, -1, 2, 5, 8, \cdots\}$$

Teorema 2.1. *Sea m entero positivo y $a, a', b, b' \in \mathbf{Z}$.*

a) Si $a \equiv a' \ \ mod(m)$ y $b \equiv b' \ \ mod(m)$ entonces $a + b \equiv a' + b' \ \ mod(m)$.

b) Si $a \equiv a' \ \ mod(m)$ y $b \equiv b' \ \ mod(m)$ entonces $ab \equiv a'b' \ \ mod(m)$.

c) Si $a \equiv a' \ \ mod(m)$ *y* $h \neq 0$ *número entero, entonces* $ah \equiv a'h \ \ mod(m)$.

d) Si $h \mid a$, $h \mid a'$, $mcd(h, m) = 1$ *y* $a \equiv a' \ \ mod(m)$, *entonces* $\frac{a}{h} \equiv \frac{a'}{h} \ \ mod(m)$.

Demostración. Se deja como ejercicio al lector. □

EJEMPLO 2.3. Como $9 \equiv 1 \ \ mod(8)$, aplicando c) del teorema anterior se tiene que

$$9 \cdot 9 \equiv 1 \cdot 9 \ \ mod(8) \equiv 1 \ \ mod(8)$$

así sucesivamente

$$3^{400} = (3^2)^{200} \equiv 1^{200} \ \ mod(8) \equiv 1 \ \ mod(8).$$

Las congruencias tienen varias aplicaciones en matemáticas, una de ellas es la obtención de los criterios de divisibilidad que se estudiarán en la siguiente sección. Otra aplicación de las congruencias es el siguiente resultado.

Teorema 2.2. El Teorema Pequeño de Fermat. *Sea* p *un número primo y* a *un número natural tal que* p *no divide a* a. *Entonces,* $a^{p-1} \equiv 1 \ \ mod(p)$.

Demostración. Para los detalles sobre la demostración ver [3] Teorema 2.4.7. □

Proposición 2.3. *Sea* $a \equiv b \ \ mod(m_1)$, $a \equiv b \ \ mod(m_2), \cdots, a \equiv b \ \ mod(m_k)$ *donde* a *y* b *son números enteros y* $m_1, m_2, \cdots, m_k$ *son enteros positivos. Entonces*

$$a \equiv b \ \ mod(m.c.m(m_1, m_2, \cdots, m_k)).$$

Demostración. Para los detalles sobre la demostración ver [3] Proposición 2.4.8. □

Corolario 2.1. *Sea* $a \equiv b \ \ mod(m_1)$, $a \equiv b \ \ mod(m_2), \cdots, a \equiv b \ \ mod(m_k)$ *donde* a *y* b *son números enteros y* $m_1, m_2, \cdots, m_k$ *son enteros positivos primos dos a dos. Entonces*

$$a \equiv b \ \ mod(m_1 \cdot m_2 \cdots m_k).$$

Cálculo del Inverso en $\mathbf{Z}_p$.

Todo elemento $[a] \in \mathbf{Z}_p$ tiene su opuesto respecto a la suma, $[p - a]$, y si p es primo, y $[a] \neq [0]$, tiene inverso multiplicativo y es único. A continuación, se exponen dos métodos distintos para calcular el elemento inverso.

- El primero se basa en el Teorema Pequeño de Fermat anteriormente estudiado y que escribimos de la forma:

$$[a]^{p-1} = [1].$$

Esto es:

$$[a]^{p-2} \cdot [a] = [a]^{p-1} = [1] \Rightarrow [a]^{-1} = [a]^{p-2}.$$

- El segundo método se basa en el Teorema de Bezout (véase Teorema 5.1.1 en [9]) que afirma que dados $a, b \in \mathbf{Z}$ no nulos, existen $u, v \in \mathbf{Z}$ tales que $ua + vb = mcd(a, b)$. Por tanto, si $[a] \in \mathbf{Z}_p$, con $0 < a < p - 1$ entonces existen $u, v \in \mathbf{Z}$ tales que $ua + vp = 1$. Tomando clases de equivalencia se tiene: $[u][a] = [1] - [p] = [1]$, de donde se deduce que:

$$[a]^{-1} = [u].$$

Computacionalmente, el segundo método es más apropiado que el primero, la idea básica para calcular $[a]^{-1} = [u]$ es seguir el proceso explicado en la sección 1 en el algoritmo para encontrar una solución de una ecuación diofántica, utilizando el algoritmo de Euclides. (Ver Capitulo 4 en [9]). Nótese que es equivalente a encontrar una solución de la ecuación diofántica $ax + py = 1$.

Ejemplo 2.4. Calcular el inverso de [7] en $\mathbf{Z}_{31}$. Aplicando el algoritmo de Euclides de la división se tiene:

$$31 = 4 \cdot 7 + 3$$

$$7 = 2 \cdot 3 + 1$$

Despejando los restos de las dos igualdades se tiene:

$$31 - 4 \cdot 7 = 3$$

$$7 - 2 \cdot 3 = 1$$

Ahora substituyendo el valor del resto de la primera en la segunda igualdad se tiene:

$$1 = 7 - 2 \cdot 3 = 7 - 2 \cdot (31 - 4 \cdot 7) = 9 \cdot 7 - 2 \cdot 31.$$

De donde se deduce que el inverso es $[7]^{-1} = [9]$. □

Observación 2.3. El comando "igcdex" de Maple devuelve el mcd de dos números enteros a y b, tal que $g = mcd(a, b)$ con $g = sa + tb$.

```
> igcdex(7,31,s,t);

                                1

> s;t;

                                9
                               -2
```

Ecuaciones con congruencias.

Se considera la ecuación $ax \equiv b \mod(m)$ con a, b números enteros y m entero positivo. Esta ecuación se satisface cuando existe $y \in \mathbf{Z}$ tal que:

$$ax - b = ym.$$

Es decir, si (x, y) es una solución de la ecuación diofántica $ax - b = ym$, x es una solución de $ax \equiv b \mod(m)$.

EJEMPLO 2.5. Queremos encontrar las soluciones enteras de $4x \equiv 2 \mod(6)$. Si x es una solución entera de esta ecuación, existe un número entero y tal que $4x - 2 = 6y$, esto es $4x - 6y = 2$. Ahora bien, como $mcd(4, 6) = 2$ divide a 2, por el Teorema 1.1 se tiene que la ecuación diofántica tiene solución entera. Además, por la Proposición 1.1, la ecuación tiene infinitas soluciones que pueden expresarse de la forma:

$$x = x_0 + (b/2)t, \;\; y = y_0 - (a/2)t, \;\; t \in \mathbf{Z}$$

siendo (x_0, y_0) una solución particular. Por ello, en primer lugar calculamos (x_0, y_0) utilizando el algoritmo de Euclides. Obsérvese que como $6 = 1 \cdot 4 + 2$ se tiene despejando que $(-1) \cdot 4 - (-1) \cdot 6 = 2$, de donde se deduce que $x_0 = -1, y_0 = -1$ es una solución particular. Por tanto, las soluciones de $4x \equiv 2 \mod(6)$ son de la forma $x = -1 - 3t, \;\; t \in \mathbf{Z}$. Nótese que todas estas soluciones pertenecen sólo a dos clases de equivalencia: si t es par $x \equiv -1 \mod(6)$ y si t es impar $x \equiv 2 \mod(6)$. □

Teorema 2.3. *Sean a y b dos números enteros y m un entero positivo con $mcd(a, m) = d$. Si d no divide a b, la ecuación $ax \equiv b \mod(m)$ no tiene solución. Si d divide a b, la ecuación $ax \equiv b \mod(m)$ tiene exactamente d soluciones no congruentes entre sí módulo m.*

Observación 2.4. Las d soluciones no congruentes entre sí módulo m a las que se refiere el Teorema anterior se pueden expresar de la forma:

$$x = x_0 - (m/d)n, \quad n = 0, 1, 2, 3, \cdots, d - 1.$$

Un antiguo problema Chino.

Encontrar un número que dividido entre 3 *dé como resto* 1*, dividido entre* 5 *dé como resto* 2 *y que dividido entre* 7 *dé como resto* 3*.*

Esto es, se trata de resolver el sistema:

$$\begin{cases} x \equiv 1 \mod(3) \\ x \equiv 2 \mod(5) \\ x \equiv 3 \mod(7). \end{cases}$$

Este tipo de problemas, han dado lugar al siguiente teorema.

Teorema 2.4. El Teorema de los Restos Chinos. Sun Tsu, siglo I. *Sean $m_1, m_2, \cdot m_s$ enteros primos entre sí. Entonces el sistema de congruencias:*

$$\begin{cases} x \equiv a_1 \mod(m_1) \\ x \equiv a_2 \mod(m_2) \\ \vdots \\ x \equiv a_s \mod(m_s). \end{cases}$$

tiene una única solución entera en cada uno de los intervalos

$$[u, u + m_1 \cdots m_s) \ \ con \ \ u \in \mathbf{Z}.$$

Demostración. Para los detalles sobre la demostración ver [9] Capítulo 4, Sección 4.3.1. □

Observación 2.5.

- De la demostración se deduce que si $k \neq j$ entonces $mcd(m_k, m_j) = 1$ y por el Teorema de Bezout se tiene que existen enteros $u_{k,j}, u_{j,k}$ tales que $u_{k,j}m_k + u_{j,k}m_j = 1$, y por tanto la solución mencionada es de la forma:

$$a = a_1(u_{2,1} \cdot m_2 \cdots u_{s,1} \cdot m_s) + a_2(u_{1,2} \cdot m_1 u_{3,2} \cdot m_3 \cdots u_{s,2} \cdot m_s) + \cdots + a_s(u_{1,s} \cdot m_1 \cdots u_{s-1,s} \cdot m_{s-1}).$$

- Para resolver un sistema con más de dos ecuaciones de congruencias se procede como sigue: primero se resuelve el sistema formado por las dos primeras

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

en cada $[u, u+m_1 \cdot m_2)$ y denotemos por A la solución encontrada. A continuación se resuelve, de la misma forma, el sistema

$$\begin{cases} x \equiv A \mod(m_1 \cdot m_2) \\ x \equiv a_3 \mod(m_3) \end{cases}$$

en cada $[u, u+m_1 \cdot m_2 \cdot m_3)$. Finalmente, se repite el proceso hasta terminar con las ecuaciones del sistema inicial. (Para más detalle ver [9], Capítulo 4, Sección 4.3.1.)

Ejemplo 2.6. Resolver el sistema:

$$\begin{cases} x \equiv 1 \mod(3) \\ x \equiv 2 \mod(5) \\ x \equiv 3 \mod(7). \end{cases}$$

En primer lugar se resuelve el sistema formado por las dos primera ecuaciones:

$$\begin{cases} x \equiv 1 \mod(3) \\ x \equiv 2 \mod(5) \end{cases}$$

En este caso $m_1 = 3$ y $m_2 = 5$, y aplicando el algoritmo de Euclides se tiene que el sistema:

$$\begin{cases} 5 = 1 \cdot 3 + 2 \\ 3 = 1 \cdot 2 + 1 \end{cases}$$

tiene solución única en $[0, 0 + 3 \cdot 5) = [0, 15)$. Para calcular esta solución, despejamos los restos en las dos igualdades

$$\begin{cases} 5 - 1 \cdot 3 = 2 \\ 3 - 1 \cdot 2 = 1. \end{cases}$$

Ahora, substituyendo $r_1 = 2$ en la segunda igualdad se tiene $2 \cdot 3 - 1 \cdot 5 = 1$, y por tanto $u = 2$ y $v = -1$. Siguiendo la observación anterior se tiene que la solución es de la forma

$$a = a_1 v m_2 + a_2 u m_1 = 1 \cdot (-1) \cdot 5 + 2 \cdot 2 \cdot 3 = 7.$$

A continuación, se resuelve el sistema de congruencias:

$$\begin{cases} x \equiv 7 \ \ mod(15) \\ x \equiv 3 \ \ mod(7). \end{cases}$$

Siguiendo el mismo procedimiento encontramos la solución en el intervalo $[0, 0 + 15 \cdot 7) = [0, 105)$:

$$15 = 7 \cdot 2 + 1.$$

de donde se deduce que $15 - 7 \cdot 2 = 1$ y por tanto $u = 1$ y $v = -2$. Por tanto, la solución es

$$a = a_1 v m_2 + a_2 u m_1 = 7 \cdot (-2) \cdot 7 + 3 \cdot 1 \cdot 15 = -53.$$

Obsérvese que como la solución ha de estar en $[0, 105)$, se tiene que la solución es $105 - 58 = 52$. Compruébese que efectivamente $x = 52$ es una solución del problema inicial. □

En Maple podemos utilizar el comando "chrem(L1,L2)" con $L1 := [a_1, \cdots, a_s]$ y $L2 := [m_1, \cdots, m_s]$, calcula la solución única del sistema de congruencias en el intervalo $[0, m_1 \cdots m_s)$. Veamos un ejemplo en Maple.

```
> chrem([1,2,3],[3,5,7]);
>
                              52
```

3. Sistemas de Numeración y criterios de divisibilidad

El sistema de numeración utilizado habitualmente para escribir números enteros agrupa de 10 en 10 unidades de un orden para formar una unidad de un orden superior. Por ejemplo, el número 3501213 se puede escribir como potencias de 10 de la forma

$$3501213 = 3 \cdot 10^6 + 5 \cdot 10^5 + 0 \cdot 10^4 + 1 \cdot 10^3 + 2 \cdot 10^2 + 1 \cdot 10^1 + 3 \cdot 10^0$$

Históricamente se han utilizado otros sistemas de numeración, así la forma de contabilizar las horas en el reloj es una consecuencia del sistema de potencias de 60 usado en la antigüedad. En la actualidad los ordenadores utilizan sistemas de numeración de potencias de 2, por ejemplo 16, o 32.

Un número entero cualquiera se puede representar como una combinación lineal de potencias de un número natural (Tª. 3.1), por ejemplo 21 en potencias de 2 es $1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2 + 1 \cdot 2^0$ y en potencias de 5 es $4 \cdot 5 + 1$.

Observación 3.1. En general, dado un número natural b y si el número n se puede representar en combinaciones lineales de potencias de b como $n = a_k \cdot b^k + a_{k-1} \cdot b^{k-1} + \ldots + a_1 \cdot b + a_0 \cdot b^0 = \sum_{i=0}^{k} a_i \cdot b^i$, escribiremos $n = (a_k \ a_{k-1} \ \ldots a_1 \ a_0)_b$.

Si el número b es mayor que 9 los símbolos para valores superiores a 9 se representan por letras mayúsculas A para 10, B para 11, C para 12 y así sucesivamente, con lo que $(A2C3)_{16} = 10 \cdot 16^3 + 2 \cdot 16^2 + 12 \cdot 16 + 3 = 41667$.

Teorema 3.1. *Sea un número natural, b, fijo al que llamaremos base. Entonces, para cualquier número entero n existen $a_k, \ldots, a_0 \in \mathbb{Z}$, con $0 \leq a_i < b \quad \forall i = 0, \ldots, k$ tal que $n = a_k \cdot b^k + \ldots + a_0 \cdot b^0$.*

Demostración. Sin pérdida de generalidad supondremos que n es positivo. Por el algoritmo de la división $n = c_1 \cdot b + a_0$, con $0 \leq a_0 < b$. Aplicando otra vez el mismo algoritmo $c_1 = c_2 \cdot b + a_1$, con $0 \leq a_1 < b$. Continuando con el proceso obtenemos una secuencia $n > c_1 > \ldots$. Puesto que todo subconjunto no vacío de números naturales tiene un elemento menor que los demás (Principio de la Buena Ordenación) existe un primer elemento $c_k \neq 0$, tal que $c_k = 0 \cdot b + a_k$, con $0 \leq a_k < b$. Entonces,

$$n = c_1 \cdot b + a_0 = (c_2 \cdot b + a_1) \cdot b + a_0 = c_2 \cdot b^2 + a_1 \cdot b + a_0 = (c_3 \cdot b + a_2) \cdot b^2 + a_1 \cdot b + a_0 =$$

$$= c_3 \cdot b^3 + a_2 \cdot b^2 + a_1 \cdot b + a_0 = \ldots = a_k \cdot b^k + \ldots + a_2 \cdot b^2 + a_1 \cdot b + a_0$$

Supongamos $n = a_k \cdot b^k + \ldots + a_1 \cdot b + a_0 = \alpha_k \cdot b^k + \ldots + \alpha_1 \cdot b + \alpha_0$, sin pérdida de generalidad podemos suponer que el número de sumandos es el mismo, ya que en otro caso se completa con términos nulos. Restando ambas expresiones obtenemos

$$0 = (a_k - \alpha_k) \cdot b^k + \ldots + (a_1 - \alpha_1) \cdot b + a_0 - \alpha_0 \Rightarrow \alpha_0 - a_0 = (a_k - \alpha_k) \cdot b^k + \ldots + (a_1 - \alpha_1) \cdot b$$

b divide a todos los términos del miembro de la dcha. de la última igualdad por lo que debe dividir a $\alpha_0 - a_0$, es decir $b | \alpha_0 - a_0$, y puesto que $0 \leq |\alpha_0 - a_0| < b$, se debe cumplir que $\alpha_0 - a_0 = 0$, por lo que $\alpha_0 = a_0$. Reordenando la última expresión, dividiendo por b y repitiendo el proceso obtenemos $a_i = \alpha_i$ para todos los $i = 0, \ 1, \ldots, k$. □

El teorema previo nos asegura que dada cualquier base, b,todo número entero positivo admite una representación única como combinación lineal de potencias de b, donde los coeficientes son todos inferiores a b.

Ejemplo 3.1.

1. Para escribir el número 1864 en base 13, dividimos sucesivamente por 13 y consideramos los restos,

$$1864 = 11 \cdot 13^2 + 0 \cdot 13 + 5 = (\mathrm{C05})_{13}$$

2. Para resolver la ecuación $(225)_7 = (x)_4$ consideramos el número en base 10 y, después expresamos el resultado en base 4.

$$(225)_7 = 2 \cdot 7^2 + 2 \cdot 7 + 5 = 117 = 4^3 + 3 \cdot 4^2 + 4 + 1 = (1311)_4 \Rightarrow x = 1311$$

Corolario 3.1. *Sea n un número entero y b un número natural. El número $n = \sum_{i=0} a_i \cdot 10^i$ es divisible por $b \iff \sum_{i=0} a_i \cdot r_i$ es divisible por b, siendo r_i el resto de dividir 10^i por b ($10^i \equiv r_i \mod (b)$). Otra forma de expresarlo es diciendo que $\sum_{i=0} a_i \cdot r_i$ es congruente con $0 \mod (b)$*

Demostración. Supondremos que n es positivo y que su representación en base 10 es

$$n = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \ldots + a_1 \cdot 10 + a_0 = \sum_{i=0}^{k} a_i \cdot 10^i, \quad \text{con } 0 \leq a_i < 10 \quad \forall i = 0, \ldots, k$$

Si r_i el resto de dividir 10^i por b, para $i = 0, \ldots, k$, se tiene que $10^0 \equiv r_0 \mod (b) \equiv 1 \mod (b)$;

$10^1 \equiv r_1 \mod (b), \ldots, 10^k \equiv r_k \mod (b)$. Entonces, utilizando que

$a \equiv b \mod (m) \Rightarrow \lambda{\cdot}a \equiv \lambda{\cdot}b \mod (m)$ y $a \equiv b \mod (m)$ y $c \equiv d \mod (m) \Rightarrow (a{+}c) \equiv (b{+}d) \mod (m)$

se tiene

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \equiv \sum_{i=0}^{k} a_i \cdot r_i \mod (b) \equiv \left(\sum_{i=0}^{k} a_i \cdot r_i \right) \mod (b)$$

Entonces, n es divisible por $b \iff n \equiv 0 \mod (b) \iff \sum_{i=0}^{k} a_i \cdot r_i$ es divisible por b. □

Ejemplo 3.2. En los dos siguientes ejemplos obtendremos criterios particulares para división por 3 y 7.

1. Puesto que $10^1 \equiv 1 \mod (3) \Rightarrow 10^h \equiv 1^h \mod (3)$. Entonces,

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \text{ es divisible por } b \iff a_0 \cdot 1 + \ldots + a_k \cdot 1 \text{ es divisible por } b$$

   Es decir, un número entero es divisible por 3 si la suma de sus dígitos es divisible por 3.

2. Para establecer el criterio de divisibilidad por 7 nótese que:

$$1 \equiv 1 \mod (7); \qquad 10^3 \equiv 6 \mod (7) \equiv -1 \mod (7)$$
$$10 \equiv 3 \mod (7); \qquad 10^4 \equiv 4 \mod (7) \equiv -3 \mod (7)$$
$$10^2 \equiv 2 \mod (7); \qquad 10^5 \equiv 5 \mod (7) \equiv -2 \mod (7)$$

Además, $10^6 \equiv 1 \mod (7)$, por lo que para un valor $k > 6$ cualquiera se verifica

$$10^k = 10^{6l+r}, \text{ con } 0 \leq r < 6 \Rightarrow 10^k \equiv 1 \cdot 10^r \mod (7)$$

con lo que se van repitiendo en el mismo orden los restos. Así, el criterio de divisibilidad por 7 es

$$n \sum_{i=0}^{k} a_i \cdot 10^i \text{ es divisible por } 7 \Longleftrightarrow a_0 + 3a_1 + 2a_2 - a_3 - 3a_4 - 2a_5 + \ldots \text{ es divisible por } 7$$

Si dado un entero positivo b y consideramos el vector $V_b^* = (l_0,\ l_1,\ \ldots, l_n, \ldots)$, llamado *adjunto de* b, formado por los enteros más próximos a cero que es solución de $x \equiv 10^n \mod (b)$, con $n \in \mathbb{N}$, el criterio general de divisibilidad podemos expresarle como

$$n = \sum_{i=0}^{k} a_i \cdot 10^i \text{ es divisible por } b \Longleftrightarrow a_0 l_0 + \ldots + a_k l_k \text{ es divisible por } b \Longleftrightarrow V_n \cdot V_b^* \text{ es divisible por } b$$

siendo $V_n = (a_0,\ a_1, \ldots, a_n,\ 0, \ldots)$.

A la vista de los casos anteriores $V_3^* = (1,\ 1, \ldots) = (\bar{1})$, donde $\bar{1}$ significa que 1 se repite indefinidamente (es el periodo de 3). Se puede demostrar que todo número entero positivo tiene vector adjunto periódico, y, en particular $V_7^* = (\overline{1,\ 3,\ 2,\ -1,\ -3,\ -2})$.