Definición. Una **ecuación lineal diofántica** es una ecuación del tipo $ax + by = c$ con a, b y c números enteros y en la que se pretende que las soluciones para x e y sean también números enteros.

Proposición. Sean a, b y c números enteros y sea $d = (a, b)$. La ecuación lineal diofántica $ax + by = c$ tiene solución si y sólo si d divide a c.

Proposición. Sean a y b dos números enteros y sea $d = (a, b)$. Entonces a/d y b/d son primos relativos.

Proposición. Sean a, b y c números enteros, $d = (a, b)$, y x_0, y_0 una solución particular de la ecuación lineal diofántica $ax + by = c$. Entonces todas las soluciones de dicha ecuación son de la forma $x = x_0 + (b/d)n$, $y = y_0 - (a/d)n$ con n cualquier número entero.

El teorema fundamental de la Aritmética

Proposición. Sean a y b dos números enteros no nulos y p un número primo. Supongamos que p divide al producto ab. Entonces p divide a uno de los dos números enteros a o b.

Teorema. Todo número entero es producto de factores primos de forma única salvo en el orden de los mismos.

(Sistemas de numeración) Sea b un número entero mayor o igual que 2. Entonces cualquier $n \leq 0$ puede escribirse de forma única como $n = a_0 + a_1 b + a_2 b^2 + \cdots + a_j b^j$ donde $0 \leq a_i < b$ para $i = 0, \cdots, j$ y $a_j \neq 0$.

Congruencias

Definición. Sea m un número entero positivo mayor que 1. Se dice que dos números enteros a y b son **congruentes módulo** m si existe otro entero k tal que $a - b = km$, es decir, si m divide a $a - b$. En caso de ser así, esto se denotara por $a \equiv_m b$ o por $a = b(mod\ m)$.

Proposición. Sea m un número entero positivo mayor que 1. La relación de congruencia módulo m en $\mathbb{Z}$ es una relación de equivalencia.

Definición. El conjunto cociente de $\mathbb{Z}$ sobre la relación de equivalencia de congruencia módulo m se denomina conjunto de los números enteros módulo m y se denota por $\mathbb{Z}_m$.

Teorema. $\mathbb{Z}_m$ es el conjunto formado por las clases de equivalencia de los posibles restos de dividir un número entero entre m.

Proposición. Sea m un número entero positivo mayor que 1 y $a,\ b,\ c$ y d números enteros cualesquiera. Entonces:

i) Si $a \equiv_m c$ y $b \equiv_m d$, entonces $a + b \equiv_m c + d$.

ii) Si $a \equiv_m c$ y $b \equiv_m d$, entonces $ab \equiv_m cd$.

Proposición. La suma y el producto en $\mathbb{Z}_m$ se definen como $[a] + [b] = [a + b]$ y $[a][b] = [ab]$ respectivamente. Estas operaciones verifican las propiedades asociativa y conmutativa, siendo el elemento neutro de la suma $[0]$ y del producto $[1]$. Todo elemento $[n]$ de $\mathbb{Z}_m$ tiene elemento opuesto $[m - n]$. Todo elemento $[n]$ tal que $(n, m) = 1$ tiene elemento inverso.

Ecuaciones y sistemas en congruencias

Teorema. Sean m un número entero positivo mayor que 1 y a y b dos números enteros cualesquiera y consideremos $d = (a, m)$. Si d no divide a b entonces la ecuación $ax \equiv_m b$ no tiene solución. Si por el contrario d divide a b entonces $ax \equiv_m b$ tiene d soluciones no congruentes módulo m.

Lema. Sea a y b números enteros tales que $a \equiv_{m_1} b,\ a \equiv_{m_2} b, \cdots, a \equiv_{m_k} b$. Entonces $a \equiv_M b$ donde M es el mínimo común múltiplo de los m_i.

Corolario. Sean a y b números enteros tales que $a \equiv_{m_1} b, a \equiv_{m_2} b, \cdots, a \equiv_{m_k} b$. Si los módulos de las congruencias son primos relativos dos a dos, entonces $a \equiv_{m_1 m_2 \cdots m_k} b$.

Teorema chino del resto Sean m y m' dos números enteros mayores que 1. Si $(m, m') = 1$, el sistema en congruencias $x \equiv_m u$ $x \equiv_{m'} v$ tiene solución única módulo mm'.

Teorema chino del resto generalizado Sean $m_1,\ m_2, \cdots, m_n$ números enteros mayores que 1 y primos relativos dos a dos. Entonces el sistema de congruencias $x \equiv_{m_1} u_1,\ x \equiv_{m_2} u_2, \cdots, x \equiv_{m_n} u_n$ tiene solución única módulo $m = m_1 m_2 \cdots m_n$.

Algoritmo de Gauss. La solución x del teorema chino del resto puede calcularse como $x = \Sigma_{i=1}^{n} u_i N_i M_i \, mod \, m$ donde $N_i = m/m_i$ y $M_i = N_i^{-1} \, mod \, m_i$.

Corolario. Sean $m_1,\ m_2, \cdots, m_n$ números enteros mayores que 1 y $a_1, a_2, \cdots, a_n$ y $u_1,\ u_2, \cdots, u_n$ números enteros cualesquiera. Consideremos el sistema de congruencias $a_1 x \equiv_{m_1} u_1,\ a_2 x \equiv_{m_2} u_2, \cdots, a_n x \equiv_{m_n} u_n$ Si los m_i son primos relativos dos a dos y $(a_i, m_i) = 1$ para todo $i = 1, \cdots, n$, entonces el sistema tiene solución, que es única módulo $m_1 m_2 \cdots m_n$.