# 1. Notación

| | |
|---|---|
| $\mathbb{N}$ | Los números naturales $\{1, 2, 3, \ldots\}$. |
| $\mathbb{Z}$ | Los enteros $\{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$. |
| $\mathbb{Q}$ | Los números racionales (fracciones). |
| $\mathbb{R}$ | Los números reales. |
| $\mathbb{P}$ | Los números primos $\{2, 3, 5, 7, 11, \ldots\}$. |
| $]a, b[$ | El intervalo $\{x \in \mathbb{R} : a < x < b\}$. |
| $[a, b]$ | El intervalo $\{x \in \mathbb{R} : a \leq x \leq b\}$. |
| $]a, b]$ | El intervalo $\{x \in \mathbb{R} : a < x \leq b\}$. |
| $[a, b[$ | El intervalo $\{x \in \mathbb{R} : a \leq x < b\}$. |
| $]a, +\infty[$ | El intervalo $\{x \in \mathbb{R} : x > a\}$. |
| $[a, +\infty[$ | El intervalo $\{x \in \mathbb{R} : x \geq a\}$. |
| $]-\infty, a[$ | El intervalo $\{x \in \mathbb{R} : x < a\}$. |
| $]-\infty, a]$ | El intervalo $\{x \in \mathbb{R} : x \leq a\}$. |
| $\lfloor x \rfloor$ | El único entero que satisface $x - 1 < \lfloor x \rfloor \leq x$. |
| $\lceil x \rceil$ | El único entero que satisface $x < \lceil x \rceil \leq x + 1$. |
| $\{x\}$ | Parte fraccionaria de $x$. |
| $x \in X$ | $x$ pertenece a $X$. |
| $A \subset B$ | $A$ esta contenido en $B$. |
| $\forall$ | Para todo. |
| $\exists$ | Existe. |
| $\exists!$ | Existe un único. |
| $\Rightarrow$ | Implica. |
| $\Longleftrightarrow$ | Si, y solo si. |
| $\therefore$ | Por lo tanto. |
| $\blacksquare$ | Lo cual queriamos demostrar. |

# 2. Preliminares

## 2.1. Paridad

Al conjunto $2\mathbb{Z} = \{\ldots, -4, -2, 0, 2, 4, \ldots\}$ se le llama el conjunto de los números pares y al conjunto $2\mathbb{Z} + 1 = \{\ldots, -3, -1, 1, 3, \ldots\}$ se le llama el conjunto de los números impares.

Las siguientes reglas[1] se cumplen para cualesquiera par e impar:

| | | | | |
|---|---|---|---|---|
| par | + | par | = | par. |
| par | + | impar | = | impar. |
| impar | + | par | = | impar. |
| impar | + | impar | = | par. |

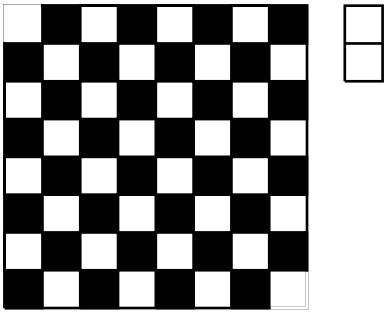
**Ejemplo 2.1.** *Demuéstre que para ninguna selección de signos en*

$$1 \pm 2 \pm \cdots \pm 10,$$

*se obtendrá una suma* 0.

*Solución: La suma* $1 + 2 + \cdots + 10 = 55$, *un entero impar. Ya que la paridad no es afectada por la elección del signo, para cualquier selección del signo* $\pm 1 \pm 2 \pm \cdots \pm 10$ *nunca será par, y en particular, nunca será* 0.

**Ejemplo 2.2.** *Dos esquinas diametralmente opuestas son cortadas de un tablero de ajedrez, que como se recordará, tiene* 64 *casillas. Demuéstre que es imposible cubrir totalmente a las* 62 *casillas restantes con* 31 *dominós.*



*Solución: Cada dominó cubre cuadrados de diferente color. Al eliminar dos casillas diametralmente opuestas, se eliminan dos casillas del mismo color. Por lo tanto quedan* 32 *casillas de un color y* 30 *del otro, con lo cual* 31 *dominós no las pueden cubrir a todas.*

[1] Estas reglas se deducirán del algoritmo de la división.

## 2.2. Principio de las Casillas

"Si $(n+1)$ objetos se deben de acomodar en $n$ casillas, entonces en alguna de las casillas hay más de un objeto".

Este resultado se conoce como *Principio de las Casillas*, también es llamado el Principio de Dirichlet, o Principio de las palomas. Peter Dirichlet fué el primero en utilizarlo en teoría de números en el siglo XIX.

Su validez es facil de ver, supongase que en cada casilla se coloca a lo más un objeto, entonces tenemos a lo más $n$ objetos acomodados, pero nosotros colocamos $n+1$, por lo tanto hay una casilla con más de un objeto.

**Ejemplo 2.3.** *En un grupo de tres personas hay dos del mismo sexo. En este caso los objetos son las personas y los sexos son las casillas.*

**Ejemplo 2.4.** *En un grupo de 13 personas hay dos que nacieron el mismo mes. En este caso los objetos son las personas y los meses son las casillas.*

**Ejemplo 2.5.** *En un grupo de 8 personas hay dos que nacieron el mismo día de la semana. En este caso los objetos son las personas y los días de la semana son las casillas.*

**Ejemplo 2.6.** *En un conjunto de $n+1$ enteros positivos, todos ellos menores o iguales a $2n$, siempre hay dos elementos de manera que uno de ellos divide al otro.*

*Solución: Podemos escribir a los $n+1$ enteros en la forma $a_1 = 2^{m_1}b_1, a_2 = 2^{m_2}b_2, \ldots, a_{n+1} = 2^{m_{n+1}}b_{n+1}$ con $b_i \geq 1$ un número impar y $m_i \geq 0$. Como $b_1, b_2, \ldots, b_{n+1}$ es un conjunto de $n+1$ números impares menores que $2n$ y entre 1 y $2n$ solamente hay $n$ impares, tenemos por el* Principio de las casillas *que hay dos de ellos iguales, digamos $b_i = b_j$. Ahora si $m_i \leq m_j$ es claro que $a_i$ divide a $a_j$, y si $m_i \geq m_j$ tenemos que $a_j$ divide a $a_i$.*

**Ejemplo 2.7.** *Sea $A$ un conjunto de 19 enteros diferentes elegidos dentro de la progresión aritmética* [2] $1, 4, 7, 10, \ldots, 100$. *Muestre que hay dos enteros*

[2] Una progresión aritmética es una sucesión de números, tal que si $a$ es el primer término, la progresión es:

$$a, a+d, a+2d, a+3d, \ldots, a+nd, \ldots$$

*diferentes en A cuya suma es* 104.

*Solución: Hay* 16 *parejas diferentes de la progresión aritmética que suman* 104*, y son: (4,100), (7,97), (10,94), (13,91), (16,88), (19,85), (22,82), (25,79), (28,76), (31,73), (34,70), (37,67), (40,64), (43,61), (46,58) y (49,55). Los números 1 y 52 no tienen pareja, dentro de la progresión, que sumen* 104*. Ahora en la progresión aritmética tenemos* 34 *números, entonces por* Principio de las casillas *tomaremos una pareja que suma* 104 *ya que solo tenemos* 18 *números que entre ellos no suman* 104.

**Ejemplo 2.8.** *Un exámen de admisión a la universidad tiene* 100 *preguntas de opción múltiple con* 4 *respuestas alternativas para cada pregunta. ¿ Cuántos alumnos se necesitan para garantizar que hay dos de ellos con las mismas respuestas en todo el exámen?*

*Solución: Como cada pregunta tiene* 4 *respuestas ,se puede contestar de* 4 *formas posibles, tenemos que habrán* $4^{100}$ *maneras diferentes de contestar el exámen, luego por el* Principio de las casillas*, bastará tener un alumno más del número de maneras diferentes de contestar el exámen. Por lo tanto se necesitan* $4^{100}+1$ *alumnos para garantizar que dos tendrán las mismas respuestas.*

## Ejercicios

**Problema 2.9.** *En un fiesta simpre hay dos personas que conocen al mismo número de personas.*

**Problema 2.10.** *¿Pueden las casillas de un tablero de* $3\times 3$*, llenarse con números del conjunto* $\{-1,0,1\}$*, de manera que la suma de los números en cada renglón, en cada columna y en cada diagonal sean diferentes?*

**Problema 2.11.** *En el espacio se dan* 9 *puntos de coordenadas enteras de manera que no hay tres de ellos colineales. Muestre que hay un punto de coordenadas enteras entre algún par de ellos.*

**Problema 2.12.** *En el espacio se dan* 19 *puntos de coordenadas enteras de manera que no hay tres de ellos colineales. Muestra que hay tres de ellos con la propiedad de que el centroide del triángulo que forman, también tiene coordenadas enteras.*

**Problema 2.13.** *Sean a, b, c y d enteros, muestre que* $(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$ *es divisible por* 12.

**Problema 2.14.** *Sean $a$, $b$, $c$ y $d$ enteros, muestre que $(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$ es divisible por 12.*

## 2.3. Principio Extremal

En muchos problemas se pide probar la existencia de un objeto que cumpla ciertas condiciones. En estos casos suele resultar útil prestar atención a los objetos que maximizan o minimizan alguna función convenientemente relacionada con la condición, y tratar de probar por absurdo(contradicción) que estos objetos cumplen la condición pedida.

**Ejemplo 2.15.** *En el parlamento unicameral de cierto país cada diputado tiene a lo sumo tres enemigos. Pruebe que es posible dividir el parlamento en dos cámaras de modo tal que cada diputado tenga, en su propia cámara, a lo sumo un enemigo.*

*Solución. Para cada partición $P$ del conjunto de todos los diputados en dos cámaras definamos el grado de conectividad $g(P)$ calculando el número de enemigos que cada diputado tiene en su propia cámara y sumando todos los valores resultantes. Esta función sólo toma valores enteros no negativos, por lo tanto debe existir una partición $P$ en dos cámaras en la cual $g$ toma su valor mínimo. Probemos ahora que en esta partición cada diputado tiene a lo sumo un enemigo en su propia cámara. En efecto, si un diputado tuviese más de un enemigo en su propia cámara, en la otra tendría a lo sumo uno (puesto que en total tiene a lo sumo tres). Entonces cambiándolo de cámara la suma $g(P)$ disminuiría al menos en una unidad, lo cual es absurdo.*

## 2.4. Contradicción

**Ejemplo 2.16.** *Sean $x, y, z, w$ enteros satisfaciendo*

$$\frac{1}{x} + \frac{1}{y} + \frac{1}{z} + \frac{1}{w} = 1.$$

*Demuéstre que al menos uno de ellos es par.*

Demostración: Supóngase que $x, y, z, w$ son impares. Luego

$$yzw + xzw + xyw + xyz = xyzw.$$

El lado izquierdo es par, por ser la suma de cuatro enteros impares. El lado derecho es impar, por ser el producto de cuatro enteros impares. Con lo cual obtenemos una contradicción.

**Ejemplo 2.17.** *Demuéstre, sin utilizar calculadora, que* $6 - \sqrt{35} < \frac{1}{10}$.

Demostración: Supóngase que $6 - \sqrt{35} \geq \frac{1}{10}$. Entonces $6 - \frac{1}{10} \geq \sqrt{35}$, o sea, $59 \geq 10\sqrt{35}$. Al elevar ambos lados al cuadrado tenemos que, $3481 \geq 3500$, lo que no tiene sentido. Entonces se concluye que $6 - \sqrt{35} < \frac{1}{10}$.

**Ejemplo 2.18.** *Si $a, b, c$ son enteros impares, demuéstre que la ecuación $ax^2 + bx + c = 0$ no posee una solución racional.*

Demostración: Si la ecuación tuviera una solución racional $\frac{p}{q}$, con $p, q$ relativamente primos, es decir $(p, q) = 1$, entonces

$$a\left(\frac{p}{q}\right)^2 + b\left(\frac{p}{q}\right) + c = 0 \Rightarrow ap^2 + bpq + cq^2 = 0.$$

Si ambos $p$ y $p$ fueran impares, entonces $ap^2 + bpq + cq^2$ sería también impar, y por lo tanto $\neq 0$. De manera semejante, si uno entre $p$ y $q$ fuese impar y el otro par, luego $ap^2 + bpq$ es par o bien $bpq + cq^2$ sería par, y $ap^2 + bpq + cq^2$ impar, otra contradicción. Luego, tal raíz racional $\frac{p}{q}$ no existe.

## 2.5. Inducción

En el principio de inducción matemática, tratamos de comprobar la veracidad de una aserción $P(n)$ estableciendo primero su validez en un caso base $k_0$ (usualmente $k_0 = 1$). Luego tratamos de establecer si la validez de $P(n-1)$ implica la validez de $P(n)$.

**Ejemplo 2.19.** *Demostrar que* $2^n > n,\ \forall n \in \mathbb{N}$.

*Solución: La aserción es cierta para* $n = 0$, *ya que* $2^0 > 0$. *Supóngase que* $2^{n-1} > n - 1$ *para* $n > 1$. *Ahora bien,*

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

*Pero* $n - 1 > 0 \implies n - 2 \geq 0$, *ya que* $n + n - 2 \geq n + 0 = n$ *y entonces,*

$$2^n > n.$$

*Esto termina la inducción.*

**Ejemplo 2.20.** *Demostrar que*

$$3^{3n+3} - 26n - 27$$

*es un múltiplo de* 169 *para todo número natural* $n$.

*Solución: Sea* $P(n)$ *la aserción "*$\exists k \in \mathbb{N}$ *con* $3^{3n+3} - 26n - 27 = 169k$.*" Demostraremos que* $P(1)$ *es cierta y que* $P(n-1) \implies P(n)$. *Para* $n = 1$ *se asevera que* $3^6 - 53 = 676 = 169 \cdot 4$ *es divisible por* 169, *lo cual es evidente.*

*Ahora bien,* $P(n-1)$ *se traduce en la existencia de un* $N \in \mathbb{N}$ *tal que* $3^{3(n-1)+3} - 26(n-1) - 27 = 169N$, *i.e., para* $n > 1$,

$$3^{3n} - 26n - 1 = 169N$$

*para algún entero* $N$. *Luego*

$$3^{3n+3} - 26n - 27 = 27 \cdot 3^{3n} - 26n - 27 = 27(3^{3n} - 26n - 1) + 676n$$

*lo que simplifica a*

$$27 \cdot 169N + 169 \cdot 4n,$$

*lo que claramente es múltiplo de* 169. *Esto termina la inducción.*

# 3. Divisibilidad y Primos

## 3.1. Divisibilidad

Definición: Un entero $b$ es divisible por un entero $a$, no cero, si existe un entero $x$ tal que $b = ax$ y se escribe $a \mid b$. En el caso en que no sea divisible por $a$ se escribe $a \nmid b$.
En ocasiones se usa la notación $a \,||\, b$, para indicar $a^k \mid b$, pero $a^{k+1} \nmid b$.

**Teorema 3.1.** *Dados $a, b, c \in \mathbb{Z}$ tenemos que:*

1. *$a \mid b$ implica $a \mid bc$ para cualquier entero $c$;*
2. *$a \mid b$ y $b \mid c$ implica $a \mid c$;*
3. *$a \mid b$ y $a \mid c$ implica $a \mid (bx + cy)$ para cualquiera enteros $x$ y $y$;*
4. *$a \mid b$ y $b \mid a$ implica $a = \pm b$;*
5. *$a \mid b$, $a > 0, b > 0$, implica $a \leq b$.*

**Teorema 3.2.** *El algoritmo de la división. Dados dos enteros cualesquiera $a$ y $b$, con $a \geq 0$, existen los enteros $q$ y $r$ tales que $b = qa + r$, $0 \leq r \leq a$. Si $a \mid b$, entonces $r$ satisface las desigualdades más fuertes $0 < r < a$.*

Definición: Si $k \mid a$ y $k \mid b$, entonces se dice que $k$ es un divisor común o un factor común de $a$ y $b$.
Se dice que $g$ es el máximo común divisor de $a$ y $b$, si $g$ es el mayor de los divisores comunes a $a$ y $b$, y se denota por $(a, b)$.

**Teorema 3.3.** *Si $g$ es el máximo común divisor de $b$ y $c$, entonces existen los enteros $x_0$ e $y_0$ tales que $g = (b, c) = bx_0 + cy_0$.*

Demostración: Considérese el conjunto $A = \{bx + cy : x, y \in \mathbb{Z}\}$, este conjunto de enteros incluye valores positivos y negativos, y también 0 seleccionando $x = y = 0$.
Escojanse $x_0$ y $y_0$ de manera que $bx_0 + cy_0$ sea el menor entero positivo $l$ en el conjunto, así que $l = bx_0 + cy_0$.
Ahora demostraremos de manera indirecta(por contradicción) que $l \mid b$, esto es, se supondrá que $l \nmid b$ y se obtendrá una contradicción.
Si $l \nmid b$, tenemos que existen enteros $q$ y $r$ tales que $b = ql + r$ con $0 < r < l$.
De aquí se tiene que $r = b - ql = b - q(bx_0 + cy_0) = b(1 - x_0) + c(-qy_0)$ $\therefore$

$r \in A$.
Esto contadice el hecho de que $l$ es el menor entero positivo en el conjunto $A = \{bx + cy : x, y \in \mathbb{Z}\}$.
$\Rightarrow b = gB$, $c = gC$ y $l = bx_0 + cy_0 = g(Bx_0 + Cy_0) \Rightarrow g \mid l \Rightarrow g \leq l \Rightarrow g = l$■
Con esto acabamos de obtener una nueva caracterización del máximo común divisor de $a$ y $b$, como el menor entero positivo en el conjunto $A = \{bx + cy : x, y \in \mathbb{Z}\}$.

**Teorema 3.4.** *Para cualquier entero positivo m, (ma,mb)=m(a,b).*

Demostración:

$$\begin{aligned}(ma, mb) &= \text{menor valor positivo de } max + mby \\ &= m\cdot\{\text{menor valor positivo de } ax + by\} \\ &= m(a, b)\blacksquare\end{aligned}$$

**Teorema 3.5.** *Si $d \mid a$ y $d \mid b$ y $d > 0$, entonces*

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{1}{d}(a, b)$$

*si $(a, b) = g$, entonces $\left(\frac{a}{g}, \frac{b}{g}\right) = 1$.*

Demostración:

$$\begin{aligned}(ma, mb) &= \text{menor valor positivo de } \tfrac{a}{d}x + \tfrac{b}{d}y \\ &= \tfrac{1}{d}\cdot\{\text{menor valor positivo de } ax + by\} \\ &= \tfrac{1}{d}(a, b)\blacksquare\end{aligned}$$

**Teorema 3.6.** *Si $(a, m) = (b, m) = 1$, entonces $(ab, m) = 1$.*

Demostración: Existen $x_0, y_0, x_1, y_1 \in \mathbb{Z}$, tales que $1 = ax_0 + my_0 = bx_1 + my_1$. Por lo tanto puede escribirse $(ax_0)(bx_1) = (1 - my_0)(1 - my_1) = 1 - my_2$, donde $y_2 = y_0 + y_1 - my_0y_1 \Rightarrow abx_0x_1 + my_2 \Rightarrow (ab, m) = 1\blacksquare$

Definición: Se dice que $a$ y $b$ son primos relativos o coprimos en el caso de que $(a, b) = 1$.

**Teorema 3.7.** *Para todo k, $(a, b) = (b, a) = (a, -b) = (a, b + ak)$.*

Demostración: Las primeras dos igualdades son consecuencias directas de la definición, ahora veamos la tercera igualdad.

$$\begin{aligned}(a, b + ak) &= \text{menor valor positivo de } ax + (b + ak)y \\ &= \{\text{menor valor positivo de } a(x + k) + by\} \\ &= \{\text{menor valor positivo de } ax' + by\}, \text{ donde } x' = x + k \\ &= (a, b)\blacksquare\end{aligned}$$

**Teorema 3.8.** *Si* $c \mid ab$ *y* $(b, c) = 1$, *entonces* $c \mid a$.

Demostración:

**Teorema 3.9 (El algoritmo euclideano).** *Dados los enteros* $b$ *y* $c > 0$, *se hace una aplicación repetida del algoritmo de la división,*

$$\begin{array}{rcll} b & = & cq_1 + r_1 & 0 < r_1 < c, \\ c & = & r_1q_2 + r_2 & 0 < r_2 < r_1, \\ r_1 & = & r_2q_3 + r_3 & 0 < r_3 < r_2, \\ & \vdots & & \vdots \\ r_{j-2} & = & r_{j-1}q_j + r_j & 0 < r_j < r_{j-1}, \\ r_{j-1} & = & r_jq_{j+1} & \end{array}$$

$\Rightarrow (b, c) = r_j$, *los valores* $x_0$ *y* $y_0$ *en* $(b, c) = bx_0 + cy_0$ *pueden obtenerse eliminando* $r_1, r_2, \ldots, r_{j-1}$ *en el conjunto de ecuaciones.*

Demostración:

Definición: Sean $a, b \in \mathbb{Z}$, el menor de los múltiplos de $a$ y $b$ recibe el nombre de mínimo común múltiplo y se denota por $[a, b]$.

**Teorema 3.10.** *Si* $m > 0$, $[ma, mb] = m[a, b]$. *También* $[a, b] \cdot (a, b) = \mid ab \mid$.

## 3.2. Primos

Definición: Se dice que un entero $p > 1$ es un número primo, o simplemente que es un primo, en caso de que no exista divisor $d$ de $p$ que satisfaga $1 < d < p$. Si un entero $a > 1$ no es un primo entonces se dice que es un número compuesto.

**Teorema 3.11.** *Si $p \mid ab$, siendo $p$ primo, entonces $p \mid a$ o bien $p \mid b$. Más generalmente, si $p \mid a_1, a_2 \cdots a_n$, entonces $p$ divide por lo menos a un factor $a_i$ del producto.*

**Teorema 3.12 (El teorema fundamental de la aritmética).** *Todo entero $n$ mayor que 1 puede expresarse como producto de primos. Y está factorización es canonica(única), salvo el orden de los primos.*

Ejercicio: Demuestra que si $n$ es un entero positivo compuesto entonces tiene un divisor primo $p$ en el rango $1 < p \leq \sqrt{n}$. (Sugerencia: si $n = ab$ y $a > \sqrt{n}$, entonces $b < \sqrt{n}$).

**Teorema 3.13 (Euclides).** *El número de primos es infinito.*

Demostración: Sean $2, 3, 5, \ldots, p$ todos los primos entre 2 y un primo $p$, vamos a demostrar la existencia de un primo nuevo, mayor que $p$. Sea $N = (2 \cdot 3 \cdot 5 \cdot \ldots \cdot p) + 1$. Si $N$ no es primo es divisible entre un primo. Pero N no es divisible entre ninguno de los primos $2, 3, 5, \ldots, p$ (dividiendo a $N$ por cualquiera de estos números da residuo 1), así que si $N$ no es primo es divisible por un primo entre $p$ y $N$. De cualquier modo obtenemos un primo mayor que $p$ con lo cual tenemos una cantidad infinita de primos ■

**Teorema 3.14.** *Dado cualquier entero positivo $k$, existen $k$ enteros compuestos consecutivos.*

**Teorema 3.15.** *$\sqrt{2}$ es irracional.*

Demostración: Si $\sqrt{2}$ fuera racional, entonces podríamos escribir $\sqrt{2} = \frac{m}{n}$, con $m$ y $n$ enteros positivos, y también suponer que son primos relativos, $(m, n) = 1$. Así que $2n^2 = m^2$ y $2 \mid m^2$. Como 2 es un primo, tenemos que $2 \mid m$, así que $m = 2k$, donde $k$ es un entero positivo. Obtenemos entonces

$$2n^2 = (2k)^2 = 4k^2 \Rightarrow n^2 = 2k^2.$$

Ahora tenemos $2 \mid n^2 \Rightarrow 2 \mid n$, así que 2 es un divisor común de $m$ y $n$, contradiciendo la suposición original. Por lo tanto $\sqrt{2}$ es irracional ■

# 4. Congruencias

Definición: Sea $m$ un entero diferente de cero, $a, b \in \mathbb{Z}$. Entonces $a \equiv b\ (modm) \Leftrightarrow m \mid (b-a)$, $a$ congruente con $b$ modulo $m$ si, y solo si $m$ divide a $b-a$. Si $b-a$ no es divisible por $m$ se dice que $a$ no es congruente con $b$ modulo $m$ y en este caso se escribe $a \neq b\ (modm)$.

**Teorema 4.1.** *Supóngase que $a, b, c, d, x, y,$ denotan enteros. Entonces:*

*a)* $a \equiv b(modm)$, $b \equiv a(modm)$ *y* $b - a \equiv 0(modm)$ *son proposiciones equivalentes.*

*b) Si* $a \equiv b(modm)$ *y* $b \equiv c(modm)$, *entonces* $a \equiv c(modm)$.

*c) Si* $a \equiv b(modm)$ *y* $c \equiv d(modm)$, *entonces* $ax + cy \equiv bx + dy(modm)$

*d) Si* $a \equiv b(modm)$ *y* $c \equiv d(modm)$, *entonces* $ac \equiv bd(modm)$

*e) Si* $a \equiv b(modm)$ *y* $d \mid m$, *entonces* $a \equiv b(modd)$

**Teorema 4.2.** *Supógase que $f$ denota un polinomio con coeficientes enteros. Si* $a \equiv b(modm)$ *entonces* $f(a) \equiv f(b)(modm)$.

**Teorema 4.3.** *Supóngase que $a, x, y, m$ denotan enteros. Entonces:*

*a)* $ax \equiv ay(modm)$ *si y solamente si* $x \equiv y \left(mod \frac{m}{(a,b)}\right)$.

*b) Si* $ax \equiv ay(modm)$ *y* $(a, m) = 1$, *entonces* $x \equiv y(modm)$.

*c)* $x \equiv y(modm_i)$ *para* $i = 1, 2, \ldots, r$ *si y solamente si* $x \equiv y(mod[m_1, m_2, \ldots, m_r])$.

Definición: Si $x \equiv y(modm)$ entonces $y$ recibe el nombre de residuo de $x$ módulo $m$. Un conjunto $x_1, x_2, \ldots, x_m$ es un sistema completo de residuos $x$ módulo $m$ si para todo entero $y$ existe uno y solamente un $x_j$ tal que $y \equiv x_j(modm)$.

**Teorema 4.4.** *Si* $x \equiv y(modm)$ *entonces* $(x, m) = (y, m)$.

Definición: Un sistema reducido de residuos módulo $m$ es un conjunto de enteros $r_i$ tales que $(r_i, m) = 1$, $r_i \neq r_j(modm)$ si $i \neq j$ y tales que todo $x$ primo para $m$ es congruente módulo $m$ para algún miembro $r_i$ del conjunto.

**Teorema 4.5.** *El número $\phi(m)$ es el número de enteros positivos menores o iguales a $m$ que son relativamente primos para $m$.*

**Teorema 4.6.** *Sea* $(a, m) = 1$. *Sea $r_1, r_2, \ldots, r_n$ un sistema completo, o bien, reducido, de residuos módulo $m$. Entonces $ar_1, ar_2, \ldots, ar_n$ es un sistema completo, o bien, reducido, respectivamente, de residuos módulo $m$.*

**Teorema 4.7 (Teorema de Fermat).** *Considérese que $p$ denota un primo. Si* $p \nmid a$ *entonces* $a^{p-1} \equiv 1(modp)$. *Para todo entero $a$,* $a^p \equiv a(modp)$.

**Teorema 4.8 (Generalización de Euler del teorema de Fermat).** *Si* $(a, m) = 1$ *entonces*

$$a^{\phi(m)} \equiv 1(modm).$$

**Corolario 4.9.** *Si* $(a, b) = 1$ *entonces* $ax \equiv b(modm)$ *tiene una solución* $x = x_1$. *Todas las soluciones están dadas por* $x = x_1 + jm$ *donde* $j = 0, \pm 1, \pm 2, \ldots$.

**Teorema 4.10 (Teorema de Wilson).** *Si* $p$ *es un primo, entonces* $(p-1)! \equiv -1(modp)$.

## 4.1. Solución de congruencias

Definición: Considérese que $r_1, r_2, \ldots, r_m$ denota un sistema completo de residuos módulo $m$. El número de soluciones de $f(x) \equiv 0(modm)$ es el número de los $r_i$ tales que $f(x_i) \equiv 0(modm)$.