CONJUNTOS Y NÚMEROS

Conjuntos

> Principio de inclusión-exclusión: Sean A, B dos conjuntos finitos tales que $A \cap B \neq \emptyset \Rightarrow |A \cup B| = |A| + |B| - |A \cap B|$.

Funciones

> Definición: Sea $f : X \to Y$ una función, decimos que f es **inyectiva** $\Leftrightarrow \forall x_1, x_2 \in X : x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ ($f(x_1) = f(x_2) \Rightarrow x_1 = x_2$).

> Definición: Sea $f : X \to Y$ una función, decimos que f es **sobreyectiva** $\Leftrightarrow \forall y \in Y, \exists x \in X : f(x) = y$**.**

> Definición: Sea $f : X \to Y$ una función, decimos que f es **biyectiva** $\Leftrightarrow f$ es inyectiva y sobreyectiva.

> Teorema: Sea $f : X \to Y$ un función, $\exists f^{-1} \Leftrightarrow f$ es biyectiva.

> Definición: Sea $f : X \to Y$ una función y $V \subset Y$, decimos que $f^{-1}(V) = \{x \in X : f(x) \in V\}$ es la **preimagen** de V por f .

> Principio del Palomar: Se $kn + 1$ palomas comparten n nidos, hay al menos un nido con $k + 1$ palomas.

Relación de orden

> Definición: Sea R una relación en un conjunto X, decimos que R es una **relación de orden** si cumple las propiedades:

> - Reflexiva: $\forall x \in X$ se tiene que xRx.
> - Antisimétrica: $\forall x, y \in X$ si $xRy \wedge yRx \Rightarrow x = y$.
> - Transitiva: $\forall x, y, z \in X$ si $xRy \wedge yRz \Rightarrow xRz$.

> Definición: Sea R una relación de orden en un conjunto X y $M \in X$, decimos que M es un máximo (resp. mínimo) de $X \Leftrightarrow xRM, \forall x \in X$ (resp. mRx).

> Definición: Sea R una relación de orden en un conjunto X y $M \in X$, decimos que M es un elemento maximal (resp. minimal) de $X \Leftrightarrow \forall x \in X$: $MRx \Rightarrow M = x$ (resp. $xRm \Rightarrow m = x$).

Relación de equivalencia

> Definición: Sea $\sim$ una relación en un conjunto X, decimos que $\sim$ es una **relación de equivalencia** si cumple las propiedades:
>
> - Reflexiva: $\forall x \in X$ se tiene que $x \sim x$.
> - Simétrica: $\forall x, y \in X$ si $x \sim y \Rightarrow y \sim x$.
> - Transitiva: $\forall x, y, z \in X$ si $x \sim y \wedge y \sim z \Rightarrow x \sim z$.

> Definición: Sea $\sim$ una relación de equivalencia en un conjunto X, decimos que $[x] = \{y \in X$: $x \sim y\}$ es la **clase de equivalencia** de $x \in X$.

> Definición: Sea $\sim$ una relación de equivalencia en un conjunto X, decimos que $X/\sim = \{[x]$: $x \in X\}$, el conjunto de todas las clases de equivalencia de la relación es el **conjunto cociente**.

Cardinalidad

> Definición: Sea X un conjunto, decimos que $|X|$ es el cardinal de X.

> Teorema: $|\mathbb{N} \times \mathbb{N}| = |\mathbb{N}| = \chi_0$.

> Teorema de Cantor-Schroeder-Bernstein: Sean X, Y dos conjuntos infinitos tales que $\exists$ un par de funciones $f : X \to Y$ y $g : Y \to X$ inyectivas $\Rightarrow \exists h : X \to Y$ biyectiva. Es decir, $|X| \leq |Y| \wedge |Y| \leq |X| \Rightarrow |X| = |Y|$.

> Teorema: $\mathbb{R}$ no es numerable $\Leftrightarrow |\mathbb{R}| = \chi_1 \geq \chi_0$.

> Teorema de Cantor: Sea A un conjunto tal que $A \subset U$ (conjunto universal) $\Rightarrow |A| < |P(A)|$.

Teoría de números

> Algoritmo de Euclides: Sean $a, b, c, r \in \mathbb{Z} \backslash \{0\} : a = cb + r \Rightarrow mcd(a, b) = mcd(b, r)$.

> Definición: Sean $a, b \in \mathbb{Z} \backslash \{0\} : mcd(a, b) = 1$, definimos que a y b son **coprimos**.

> Identidad de Bézout: Sean $a, b \in \mathbb{Z} \backslash \{0\}$ y $m = mcd(a, b) > 0 \Rightarrow \exists u, v \in \mathbb{Z} : m = ua + vb$.

> Lema de Euclides: Sean $a, b, c \in \mathbb{Z} : a|bc \wedge mcd(a, b) = 1 \Rightarrow a|c$.

> Definición: Sean $a, b, c \in \mathbb{Z}$ fijos, decimos que $ax + by = c$ es una ecuación diofántica, de la que solo nos interesan sus soluciones $(x, y) \in \mathbb{Z} \times \mathbb{Z}$.

> Proposición: Sean $a, b, c \in \mathbb{Z}$ con $mcd(a, b) = d$, la ecuación diofántica $ax + by = c$ tiene soluciones enteras $mcd(x, y) \Leftrightarrow d|c$.

> Teorema: Sean $a, b, c, n \in \mathbb{Z}$, $d = mcd(a, b)$ y (x_0, y_0) una solución particular de la ecuación diofántica $ax + by = c \Rightarrow$ cualquier solución de la misma es de la forma:
>
> - $x = x_0 + \frac{b}{d}n$.
> - $y = y_0 - \frac{a}{d}n$.

> Teorema Fundamental de la Aritmética: $\forall n \in \mathbb{N}, \exists$ primos $p_1, p_2, ..., p_s$ y $\alpha_1, \alpha_2, ..., \alpha_s \in \mathbb{N} : n = p_1^{\alpha_1} \cdot n = p_2^{\alpha_2} \cdot ... \cdot n = p_s^{\alpha_s}$.

> Definición: Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $n > 1$, decimos que $a \equiv b(n) \Leftrightarrow n|(b - a)$ es una congruencia módulo n.

> Teorema pequeño de Fermat: Sea p un primo y $a \in \mathbb{N} : p \nmid a \Rightarrow a^{p-1} \equiv 1(p)$.

> Corolario: $a^p \equiv a(p) \Leftrightarrow p|(a^p - a)$.

> Teorema: Sean $a, b \in \mathbb{Z}$, $n \in \mathbb{N} \backslash \{1\}$ y $mcd(a, -n) = mcd(a, n) = d$. Entonces:
>
> - Si $d \nmid b$, la ecuación $ax \equiv b(n)$ no tiene soluciones en $\mathbb{Z}_n$.
> - Si $d|b$, la ecuación $ax \equiv b(n)$ tiene exactamente d soluciones en $\mathbb{Z}_n$.

> Teorema Chino del Resto: Sean $a_1, a_2, ..., a_k \in \mathbb{Z}$ y $m_1, m_2, ..., m_k \in \mathbb{N}$, coprimos dos a dos. Entonces el sistema

> de congruencias $x \equiv a_1\,(m_1\,), x \equiv a_2\,(m_2\,), ..., x \equiv a_k\,(m_k\,)$ tiene solución única módulo $M = m_1 \cdot m_2 \cdot ... \cdot m_k$.

> Lema: Sean $x, y \in \mathbb{Z}$, $n \in \mathbb{N} \backslash \{1\}$ y la congruencia $x \equiv y(n) \Rightarrow mcd(x, n) = mcd(y, n)$.

> Definición: Sea $z = a + bi \in \mathbb{C}$, decimos que su parte real es $a = Re(z)$ y su parte imaginaria es $b = Im(z)$.

> Definición: Sea $z = a + bi \in \mathbb{C}$, decimos que su módulo es $|z| = \sqrt{x^2 + y^2}$.

> Teorema: $e^{it} = \cos t + i \sin t$.

Polinomios

> Lema de Bézout: Sea K un cuerpo, $a \in K$ y $p(x) \in K[x]$, $(x - a)|p(x) \Leftrightarrow p(a) = 0$.

> Teorema Fundamental del Álgebra: Sea $p(x) \in \mathbb{C}$ un polinomio no constante de grado $n \geq 1$, $p(x)$ tiene exactamente n raíces en $\mathbb{C}$.

> Definición: Sea $p(x) \in \mathbb{Z}[x]$, decimos que $C(p(x)) = mcd(a_0\,, a_1\,, ..., a_n)$ es el contenido de $p(x)$. Si $C(p(x)) = 1$, decimos que $p(x)$ es primitivo.

> Teorema de Gauss: Sea $p(x) \in \mathbb{Z}[x]$ un polinomio primitivo, $p(x)$ es irreducible en $\mathbb{Q} \Leftrightarrow p(x)$ es irreducible en $\mathbb{Z}[x]$.