Álgebra I

1. Conjuntos, relaciones y funciones: Conjuntos: definiciones, pertenencia, contenciones, operaciones (unión, intersección, diferencia). Leyes de De Morgan. Cardinal de conjuntos finitos. Tablas de verdad y relación con lógica proposicional. Igualdad de conjuntos (diagramas de Venn, tablas). Producto cartesiano. Conjunto de Partes (y su cardinal para cjtos finitos). Relaciones: definición, su representación como grafos. Relaciones de orden y equivalencia. Clases de equivalencia. Clausura transitiva. Funciones: Definición. Composición. Funciones inyectivas, sobreyectivas, biyectiva, inversa. Cuantificadores: noción intuitiva.

2. Números naturales e Inducción: Definición “intuitiva” de los números naturales, primeras demostraciones por inducción (simple). Sumatoria, productoria y su escritura como ciclos en un programa. Factorial y su interpretación combinatoria (biyecciones en conjuntos finitos). Número combinatorio y su interpretación combinatoria (subconjuntos en un conjunto finito), escritura como suma de dos combinatorios, definición recursiva del combinatorio. Definición de funciones recursivas en pseudocódigo (o código en algún lenguaje concreto). Definición por los axiomas de Peano de los números naturales. Ejemplos de demostración por inducción global. Ejemplos de algoritmos recursivos (sort, Hanoi, Fibonacci) y análisis de complejidad. Cálculo de a^n por distintos algoritmos (introducción intuitiva de noción de complejidad). Inducción global y principio de buena ordenación.

3. Números enteros: Enteros. Divisibilidad y primeras propiedades. Primos y Compuestos. Algoritmo de división. Aplicaciones del algoritmo de división. Escrituras en distintas bases, sistemas de numeración. Máximo común divisor. Algoritmo de Euclides (y su complejidad), escritura del máximo común divisor como combinación lineal. Numeros coprimos. Propiedades. Teorema Fundamental de la aritmética. Cantidad de primos. Criba. Aplicaciones del TFA (cantidad de divisores, cálculo de gcd y del mcm). Curiosidades de los primos. Congruencias, propiedades y aplicaciones (criterios de divisibilidad). Restos modulo m. Grupos y Anillos (comparación de Z/mZ con Z). Ecuaciones lineales diofánticas y ecuaciones de congruencia. Algoritmos. Sistemas de ecuaciones de congruencia. Teorema Chino del Resto. Pequeño Teorema de Fermat. Algoritmos probabilisticos de primalidad. de Euler-Fermat. Aplicación: Algoritmo criptográfico RSA.

4. Polinomios con coeficientes en un cuerpo: Cuerpos. Definición y ejemplos, Q, R, C, Z/pZ. Anillo de polinomios K[x]: generalidades (suma, producto, unidades), grado, divisibilidad, irreducibles y compuestos, algoritmo de división. Paralelismo

con Z: Máximo común divisor, algoritmo de Euclides, coprimos. Factorización única. Aspecto funcional: Evaluacion de polinomios (def y algoritmos). Raíces. Teorema del resto. Resolución de cuadraticas en K[X]. Multiplicidad. Equivalencias. Cota para el número de raíces con multiplicidad sobre un cuerpo. C[X]: Repaso del cuerpo C, coordenadas polares, fórmulas de Moivre. Raíces/factorizacion de X^n – z en C[x]. Grupo de raíces de la unidad. Teorema Fundamental del Algebra, irreducibles de C[X]. R[X]: Raíces complejas no reales de polinomios reales. Factorización en R[X]. Q[X]: Teorema de Gauss para calcular raíces racionales. Ejemplos de factorización en K[X] para distintos K. Criterios de irreducibilidad sobre Q y algoritmos de factorización sobre los distintos cuerpos.