

Math 303 Midterm Study Guide

1. Basic Concepts

Module I. Computers, Codes, and Pails of Water

Binary Numbers

Krypto

Nim

Tic-tac-toe Code

Pails of Water Problem

Clock Arithmetic

Division Algorithm

Mod n tables

Secret Codes

Module II. An Elementary Approach to Primes

Divisibility

Primes and Composites

Sieve of Eratosthenes

Factoring into Primes

Fundamental Theorem of Arithmetic

Applications to GCD and LCM

Katie's Theorem

Ruth-Aaron Numbers

Prime Deserts

Euler's Theorem

Primes of Special type

2. Definitions

Prime

Composite

Unit

$\text{POW}(a, b)$

$a \bmod n$

Greatest common divisor $\text{GCD}(a, b)$

Relatively prime

The Division Algorithm. Given integers a and $d > 0$, there are unique numbers q (the quotient) and r (the remainder) such that $a = qd + r$, $0 \leq r < d$.

Least common multiple $\text{LCM}[a, b]$

Prime desert

Twin primes

3. Theorems

Sieve Bound Theorem. Every composite number n has a prime factor $< \sqrt{n}$.

Basic Divisibility Theorems such as

Addition Theorem. If d divides a and d divides b , then d divides $a + b$

The Refrigerator Theorem. If d divides ab and $\text{GCD}(d, a) = 1$, then d divides b .

The All-or-Nothing Theorem. If p is a prime, then p divides a or $\text{GCD}(a, p) = 1$.

Splitting Theorem. If a prime p divides ab , then p divides a or p divides b .

Fundamental Theorem of Arithmetic. Every positive integer > 1 can be written uniquely as a product of primes, except for the order of the primes.

Prime Desert Theorem. For any n , you can find n consecutive composites.

Euclid's Theorem: There are infinitely many primes.

4. Algorithms

Convert binary to decimal, and decimal to binary.

Solve the pails of water problem

Find GCD of two numbers

Find LCM of two numbers

Find remainders when working mod n

Basic Divisibility Tests for divisors 2, 3, 4, 5, 6, 8, 9, 10

The $p = 31$ code

Encoding messages

Decoding messages

Given the encoding number, find the decoding number

Find GCD and LCM of a and b using their prime factorization

Find GCD and LCM of a and b without using their prime factorization