Math 42: Final Exam
Topics Covered

1 Types of Problems

- Solving linear diophantine equations
  - Finding all solutions in $\mathbb{Z}$
  - Finding solutions in $\mathbb{N}$
  - Solving LDE's in $\mathbb{Z}[i]$
- Finding GCD's
  - In $\mathbb{Z}$ and in $\mathbb{Z}[i]$
- Continued Fractions
  - Compute continued fractions of rational numbers
  - Compute continued fractions of square roots
  - Given an infinite continued fraction, find a closed form (i.e. $\frac{a+\sqrt{d}}{b}$)
  - Computing convergents
- Solving linear congruences $ax \equiv b \mod m$
  - Give the number of solutions without solving
- Computing $\varphi(n)$
- Computing powers mod m
  - Euler's theorem ($a^{\varphi(m)} \equiv 1 \mod m$)
  - Fermat's little theorem ($a^{p-1} \equiv 1 \mod p$, p prime)
  - Successive squaring
- Chinese remainder theorem
  - Solving systems of congruences
  - Solving equations mod m by first solving mod factors of m
- Generators and Logarithms
  - Finding generators
  - Making a log table and using it to solve problems
- Factorization in $\mathbb{Z}[i]$
  - Using factorization in $\mathbb{Z}[i]$ to express integers as the sum of two squares

  - Which primes of $\mathbb{Z}$ are still prime in $\mathbb{Z}[i]$ and which can factor?

- Legendre Symbols
  - Computing Legendre symbols using Euler's Criterion and Gauss's Lemma
  - Computing Legendre symbols using Quadratic Reciprocity
  - Using Legendre symbol rules (e.g. multiplicativity)
  - Using Legendre symbols to determine numbers of solutions to quadratic equations mod m
  - Determining, using quadratic reciprocity, for which primes p a given prime q is a square (e.g. When is 3 a square mod p?)

- Pell's Equation
  - Finding multiple solutions to $x^2 - dy^2 = 1$
  - Connection to units in $\mathbb{Z}[\sqrt{d}]$

- Unique Prime Factorization
  - Know examples of systems that have UPF and systems that don't
  - Be able to explain why two factorizations are really "the same" or really "different"

2 Definitions

- Divides, i.e. $a \mid b$
- Congruence, i.e. $a \equiv b \mod c$
- Unit (in $\mathbb{Z}$, $\mathbb{Z}_m$, $\mathbb{Z}[i]$, $\mathbb{Z}[\sqrt{d}]$)
- $\mathbb{Z}_p$ and U_p
- One-to-one and Onto functions
- Ring (e.g. $\mathbb{Z}$)
- Norm and conjugate in $\mathbb{Z}[i]$ and in $\mathbb{Z}[\sqrt{d}]$
- Generator, order
- Legendre symbol

3 Proofs

- Induction
- Contradiction
- Euclid-type proofs for infinitude of primes
- Proofs from class are fair game
- Proofs from homework are especially fair game