Math 42: Midterm 2
Topics Covered

I RSA Cryptography (there won't be ugly or impossible computations)

II Chinese Remainder Theorem

III Generators and orders of elements in U_m

IV Squares mod p

  i. Legendre symbol

  ii. Euler's criterion

  iii. $\left(\frac{-1}{p}\right)$

V $\mathbb{Z}[i]$

VI Sums of squares

- Definitions (know them and be able to use them)
  - Generator
  - Order
  - Legendre symbol
  - $\mathbb{Z}[i]$: norm, unit, complex conjugate
- Be able to compute
  - solutions to systems of congruences (Chinese remainder theorem)
  - solutions to congruences using logarithms
  - Legendre symbols, using Euler's criterion and rules of the Legendre symbol
  - factorizations in $\mathbb{Z}[i]$
  - norms in $\mathbb{Z}[i]$ and sums of squares (i.e. given an integer n, determine whether it can be written as a sum of squares, and if so, find a and b such that $a^2 + b^2 = n$)
- Proofs
  - Proofs covered in class are fair game
  - Proofs from the homework are fair game