Math 42: Midterm 1
Topics Covered

- Definitions (know them and be able to use them in simple proofs)
  - Divides, i.e. $a \mid b$
  - Congruence, i.e. $a \equiv b \mod c$
  - Greatest common divisor, relatively prime
  - Unit
  - $\mathbb{Z}_p$ and U_p
- Be able to compute
  - GCDs
  - solutions to linear diophantine equations ($ax + by = c$)
  - continued fractions and convergents
  - multiplicative inverses mod m
  - solutions (and number of solutions) to linear congruences $ax \equiv b \mod m$
  - $\varphi(n)$
  - powers mod m
  - solutions to systems of two congruences (i.e. find x such that $x \equiv a \mod m$ and $x \equiv b \mod n$)
- Proofs
  - Proofs covered in class are fair game
  - Proofs from the homework are fair game
  - Induction
  - One-to-one and onto functions