

Math 4400/Number Theory/Fall 2012
Stuff to Know for the Third Midterm

Definitions you need to know.

- (1) What is the Legendre symbol?
- (2) What is Euler's criterion for computing the Legendre symbol?
- (3) What is a Gaussian integer?
- (4) What is the norm of a Gaussian integer?
- (5) What is an irreducible (indecomposable) Gaussian integer?
- (6) What is Pell's Equation?

How to's.

- (1) Find a field with p^2 elements.
- (2) Compute any Legendre symbol using Quadratic Reciprocity.
- (3) Carry out Fermat's infinite descent for sums of squares.
- (4) Find the gcd of a pair of Gaussian integers.
- (5) Factor a Gaussian integer.
- (6) Given a solution to Pell's equation, find infinitely many others.

Theorems you should be able to state precisely.

- (1) Quadratic Reciprocity
- (2) Unique factorization of Gaussian integers.
- (3) Exactly which natural numbers are sums of two squares?

Stuff you should be able to prove.

- (1) Euler's criterion.
- (2) -1 is a square mod p if and only if $p = 2$ or $p \equiv 1 \pmod{4}$.
- (3) The multiplicativity of the Legendre symbol.
- (4) 2 is a square mod p if and only if $p \equiv 1$ or $7 \pmod{8}$.
- (5) Any prime $\equiv 1 \pmod{4}$ is a sum of two squares.
- (6) Any prime $\equiv 3 \pmod{4}$ is not a sum of two squares.
- (7) The unit Gaussian integers are $1, -1, i, -i$ and nothing else.