# ELEMENTARY NUMBER THEORY

## MIDTERM I REVIEW

The first midterm will cover material up to (not including) Euclidean rings.

### 1. What you need to know

Definitions of the basic notions (divisibility, unit, irreducible, prime, gcd, congruence, residue class, Euler's phi function, order of a residue class; Legendre symbol, Jacobi symbol)

The basic results: primes are irreducible; in $\mathbb{Z}$, irreducibles are prime; unique factorization domain; Fermat's Little Theorem; Wilson's Theorem; Euler-Fermat; Fermat's two squares theorem; Chinese Remainder Theorem; Gauss's Lemma; quadratic reciprocity law plus supplementary laws.

### 2. What you should be able to do

Apply the Euclidean algorithm to compute gcd's and Bezout representations; use Bezout to compute the inverse of residue classes; solve systems of two linear congruences; compute Euler's phi function; apply the quadratic reciprocity law.

### 3. Proofs

You should be familiar with Euler's proof that there are infinitely many primes, and wirh the proofs of Fermat's Little Theorem and Euler-Fermat, ans Gauss's Lemma; you also should be able to explain the main steps in the proofs of the important theorems (without going into details), as well as the background of RSA.