# MATH 540: STUDY GUIDE FOR EXAM 2

The following is a list of topics and types of problmems you should know for Exam 2. The exam will consist of true-false questions, short answer questions (including definitions), calculations, and one proof.

**1.** Chinese Remainder Theorem. Know how to find solutions to a given system of linear congruences.

**2.** Euler $\phi$-function. Know its definitions, its various properties and how they are used to calculate specific values of $\phi(n)$, for $n \in \mathbb{Z}$.

**3.** Know how to use Euler's Theorem: For $n \geq 1$ and $a \in \mathbb{Z}$ with $\text{GCD}(a, n) = 1$, $a^{\phi(n)} \equiv 1 \pmod{n}$.

**4.** Know Euler's product formula and how to verify it in specific cases.

**5.** Roots modulo $n$. For a polynomial with integer coefficients, know the basic properties of roots modulo $n$, for $n \geq 1$. Know the basic properties of roots modulo $n$ of polynomials of the form $X^d - 1$. In particular, know the order of an element $a$ modulo $n$, if $\text{GCD}(a, n) = 1$ and primtive roots modulo $n$.

**6.** Quadratic polynomials modulo $p$, $p$ prime. Know when roots to quadratic polynomials exist modulo $p$, and how to find them if $p \equiv 3 \pmod{4}$.

**7.** Quadratic residues.

(a) Know the basic properties of the Legendre symbol and how to use those properties to calculate $(\frac{a}{b})$.
(b) Know Euler's Criterion and how to use it.
(c) Know the Quadratic Reciprocity laws and how to use them to calculate various values of the Legendre symbol.
(d) Know Gauss's Lemma and how to verify it with specific examples.

**8.** Be able to reproduce the proof of any one of the following three theorems:

(i) If $p$ is prime and $n \geq 1$, then $\phi(p^n) = p^n - p^{n-1}$.
(ii) If $\text{GCD}(a, n) = 1$ and $a^r \equiv 1 \pmod{n}$, then $r$ is divisible by the order of $a$ mod $n$.
(iii) Euler's Criterion: If $p$ is an odd prime, and $\text{GCD}(a, p) = 1$, then $a$ is a quadratic residue modulo $p$ if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.