Math 324 Spring 2017
Homework 3
Due: February 15, 2017

---

1. (a) Determine (with proof) all primes p so that $\left(\frac{3}{p}\right) = 1$.

   (b) Determine (with proof) all odd primes so that 6 a quadratic residue modulo p.

2. Prove that an even integer is a difference of squares if and only if it is divisible by 4.

3. Show that if p is a prime and p is at least 7, then there are always two consecutive quadratic residues of p.

4. (a) Prove or disprove that the sum of the quadratic residues mod p is divisible by p if $p > 3$.

   (b) Determine (with proof) $\sum_{a=1}^{p-1} \left(\frac{a}{p}\right)$.

5. Use the fact that $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic to show that $\left(\frac{-3}{p}\right) = 1$ when $p \equiv 1 \bmod 3$. (Hint: Prove there exists an element $d \in U(\mathbb{Z}/p\mathbb{Z})$ of order 3, then show $(2d+1)^2 \equiv -3 \bmod p$.)

6. Let $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ be an ascending chain of ideals in an integral domain D. Prove that $\bigcup_{n=1}^{\infty} I_n$ is an ideal in D.

7. In an integral domain D, the *radical of an ideal* I is $\mathrm{rad}(I) = \{d \in D \mid d^n \in I \text{ for some } n \in \mathbb{N}\}$.
   Prove that:
   (a) $\mathrm{rad}(I)$ is an ideal.
   (b) $\mathrm{rad}(IJ) = \mathrm{rad}(I) \cap \mathrm{rad}(J) = \mathrm{rad}(I \cap J)$.
   (c) $\mathrm{rad}(\mathrm{rad}(I)) = \mathrm{rad}(I)$.

8. *Magma*: Write a short program to find the smallest prime which can be simultaneously written in the forms x^2+y^2, x^2+2y^2, x^2+3y^2, $\ldots$, x^2+10y^2. The command `NthPrime(i)` will give you the ith prime. So `NthPrime(1)` gives 2, `NthPrime(2)` gives 3, and `NthPrime(27)` gives 103.

   Suggestion: Before you start writing Magma code, think about the theory we have learned about primes of these forms. If you have never thought about computer programs much before, I'm happy to have a brainstorming session with you to help guide some of your thinking on how to execute this search. Also, you may want to start experimenting with typing code in another program and importing it into Magma. There is information to our Magma guide about this.