Math 40520 Theory of Number
Homework 6

Due Wednesday, 2015-10-14, in class

Do 3 of the following problems.

1. Let $p \equiv 5 \pmod 8$ be a prime number. You may assume that 2 is not a perfect square mod p. Suppose a is a perfect square mod p, not divisible by p.
   (a) Show that $2^{(p-1)/2} \equiv -1 \pmod p$.
   (b) If $\alpha = a^{(p-1)/4} \equiv \pm 1 \pmod p$.
   (c) Show that $x^2 \equiv a \pmod p$ has the solutions
   $$x \equiv \begin{cases} \pm a^{(p+3)/8} \pmod p & \text{if } \alpha = 1 \\ \pm 2^{(p-1)/4} a^{(p+3)/8} \pmod p & \text{if } \alpha = -1 \end{cases}.$$
2. The number $g = 2$ is a primitive root modulo the prime $p = 101$. Send me the number 11 encrypted with Elgamal.
3. Devise a zero-knowledge proof conversation based on RSA.
4. Let p be a prime $p \equiv 2 \pmod 3$. Show that if m, n are integers such that $p \mid m^2 + mn + n^2$ then $p \mid m$ and $p \mid n$.
5. Show that -3 is a perfect square modulo a prime $p \neq 3$ if and only if $p \equiv 1 \pmod 3$. [Hint: Use the fact that $\mathbb{Z}_p^\times$ is cyclic.]
6. Exercise 3.2 on page 67 in the textbook.
7. Exercise 3.3 on page 67 in the textbook.
8. Exercise 3.6 on page 68 in the textbook.