Math 7770 Spring 2011 Final
Due: May 2, 2011 by 6:30 PM

You are to work alone on this assignment. You may consult our textbook, your notes from the course, old homeworks and their solutions, or your pets. You may also ask me for clarification on any problem. You are not to consult other textbooks, the internet, other professors, friends, family, etc. Make sure in your solutions you **completely** explain your answers and justify anything we have not already proven in class or on a homework.

Please solve 6 of the following problems.

1. Determine all quadratic imaginary fields that have an algebraic integer with norm 2.

2. Let F be a field.
   (a) Prove that for a polynomial $f \in F[x]$, $f(a) = 0$ if and only if $(x - a) \mid f(x)$.
   (b) Prove that any polynomial $f \in F[x]$ of degree d has no more than d zeroes.

3. (a) Determine the quartic (fourth power) residues for the moduli 11, 13, 17, and 19. (Don't forget that $(-a)^2 = a^2$ for any $a \in \mathbb{Z}$.)
   (b) Prove that modulo primes $p \equiv 3 \bmod 4$ all quadratic residues are also quartic residues but modulo primes $p \equiv 1 \bmod 4$ only half of the quadratic residues are quartic residues.

4. Show that the Diophantine equation $x^4 - y^4 = z^2$ has no non-zero solution. (Hint: Descent.)

5. Let $K = \mathbb{Q}(\sqrt{m})$.
   (a) Factor 2 into irreducibles in $\mathcal{O}_K$ for each $m = -11, 5, 3$, and -7.
   (b) Prove that if $m < -7$ and $\mathcal{O}_K$ is a unique factorization domain, then $-m$ is congruent to 3 mod 8. (Hint: Think about 2.)

6. (a) Show that if p is an odd rational prime then $\left(\frac{-2}{p}\right) = 1$ if and only if $p \equiv 1$ or $3 \bmod 8$.
   (b) Use $\mathbb{Z}[\sqrt{-2}]$ to show that the rational prime p can be written as $p = x^2 + 2y^2$ if and only if $p \equiv 1$ or $3 \bmod 8$.

7. (a) Find all singular points on the curve $y^2 - 2y - x^3 + 12x - 15 = 0$.
   (b) Let E be the elliptic curve $y^2 = x^3 + 1$ defined over the field $\mathbb{Z}/5\mathbb{Z}$. List the points on E.

8. This problem explains why during the elliptic curve section we did not work with all cubic equations but only those of the form $y^2 = x^3 + Ax + B$. Continued on next page ...

The curve $G(x, y) = 0$ is said to be obtained from $F(x, y) = 0$ through a **linear change of variables** if $G(x, y) = F(c_1(x, y), c_2(x, y))$ where c_1 and c_2 are linear functions in the variable x and y. (For example $c_1(x, y)$ could be $\frac{1}{2}y + 3x - 1$.) Consider all coefficients to be in $\mathbb{Q}$.

(a) Show that by making an appropriate linear change of variables to a curve of the form

$$F(x, y) = y^2 + a_4xy + a_3y - x^3 - a_2x^2 - a_1x - a_0 = 0$$

with $a_i \in \mathbb{Q}$, one can obtain a curve of the form

$$G(x, y) = y^2 - x^3 - b_2x^2 - b_1x - b_0 = 0$$

with $b_i \in \mathbb{Q}$ too. (Hint: Complete the square on the variable y.)

(b) Show that by making an appropriate linear change of variables to a curve of the form

$$G(x, y) = y^2 - x^3 - b_2x^2 - b_1x - b_0 = 0$$

with $b_i \in \mathbb{Q}$, one can obtain a curve of the form

$$H(x, y) = y^2 - x^3 - Ax - B = 0$$

with A, $B \in \mathbb{Q}$. (Hint: Can you get rid of the x^2 term in $G(x, y)$ by replacing x with a linear equation?)