Math 480 (Spring 2007): Homework 8

Due: Monday, May 21

There are 6 problems. Each problem is worth 6 points and parts of multipart problems are worth equal amounts. You may work with other people and use a computer, unless otherwise stated. Acknowledge those who help you.

1. Write the integer 9000000000000000001053 as a sum of two squares.
2. Evaluate the infinite continued fraction $[2, \overline{1, 3}]$. Your answer should be an explicit quadratic irrational number.
3. (a) Write down in any way (no proof required) the infinite continued fraction of the quadratic irrational number $\frac{1+\sqrt{7}}{2}$. (Your answer should look like a finite continued fraction followed by a repeating part with a bar over it.)

   (b) Prove that your answer to (a) is correct by doing algebra as in problem 2 to show that the value of the continued fraction you give is really $\frac{1+\sqrt{7}}{2}$.)
4. Find a positive integer that has at least three different representations as the sum of two squares, disregarding signs and the order of the summands.
5. Let E be the elliptic curve $y^2 = x^3 - 7x$ over the rational numbers.

   (a) There is a point $P = (a, b)$ on E with $a, b \in \mathbb{Z}$ and $|a| < 10$. Find it.

   (b) Compute $Q = P + P$ by any method.
6. Let E be the elliptic curve $y^2 = x^3 + 2x$ over the finite field $\mathbb{Z}/3\mathbb{Z}$.

   (a) Show that $\#E(\mathbb{Z}/3\mathbb{Z}) = 4$, i.e., that there are 3 solutions to $y^2 = x^3 + 2x$ with $x, y \in \mathbb{Z}/3\mathbb{Z}$. (The fourth element of $E(\mathbb{Z}/3\mathbb{Z})$ is the point at infinity.)

   (b) Determine the group structure of the group $E(\mathbb{Z}/3\mathbb{Z})$ of order 4. [Hint: It is either cyclic or the Klein four group – which one is it?]