Modern Computing for Mathematicians (Math 587)

Written Assignment No. 3

due March 19, 2009

Use LaTeX to typeset your response to this assignment. Submit your printout at the class meeting on March 19. Be sure to explain what you have done to answer these questions.

1. Determine the isomorphism class of the finite abelian group of points on the elliptic curve $y^2 = x^3 - 6x^2 + 11x - 6$

   (a) in the field $\mathbf{Z}/31\mathbf{Z}$.

   (b) in the field $\mathbf{Z}/41\mathbf{Z}$.

2. Recall that ASCII codes corresponding to the characters used in normal English text strings are values from 1 to 126. The elliptic curve E given by the equation $y^2 = x^3 - 7x + 10$ has 127 points in the finite field $\mathbf{F}_{109} = \mathbf{Z}/109\mathbf{Z}$. Hence, its set of 126 affine points, with coordinates represented by least non-negative residues, may be matched lexicographically with the integers from 1 to 126 and, thereby, with the characters used in normal English text strings.

   A message that has been converted in the way above to a sequence of points in $E(\mathbf{F}_{109})$ has been further scrambled using the bijection of the set $E(\mathbf{F}_{109})$ defined in the arithmetic of points on the elliptic curve by

   $$f: \quad P \longmapsto 29P + [92, 11] \quad .$$

   (a) Find an integer k and a point A in $E(\mathbf{F}_{109})$ such that the map

   $$g: \quad Q \longmapsto kQ + A$$

   inverts f.

   (b) What is the text of the message if the sequence of scrambled points in $E(\mathbf{F}_{109})$ is that found in `code/messagecoded`.