Modern Computing for Mathematicians (Math 587)

Written Assignment No. 5

due May 5, 2009

1 Directions

Prepare your solutions so as to obtain both PDF and XHTML + MathML outputs. No particular computer algebra system is mandated although for this assignment the use of *Sage* is recommended. Some *Sage* code that may be useful may be found in

```
http://math.albany.edu/pers/hammond/course/mat587s2009/assgt/sage/ell.sage
http://math.albany.edu/pers/hammond/course/mat587s2009/assgt/sage/elgell.sage
```

Re-state each exercise before presenting its solution. Write each solution carefully so as to explain it to someone who does not understand how to do it.

Submit in writing:

- A printout of the PDF output.
- The URL in your website at `www.albany.edu` where your XHTML + MathML output may be found.

Note that the source for this assignment sheet is found at `amcm090505.glm`.

2 Exercises

1. The following is a sequence of 14 point pairs for the finite field $\mathbf{F}_{1867}$ on the elliptic curve $y^2 = x^3 - 7x + 10$ that represents El Gamal encryption with secret key 257 relative to that curve of a sequence of 14 points on that curve which, in turn, is the point sequence associated with a text string of length 14 by the method described in section 2 of recent course notes[1] with 10 "tries".

```
[[[147, 573], [317, 1169]], [[1341, 1033], [537, 1225]],
 [[590, 265], [531, 1155]], [[811, 693], [858, 989]],
 [[582, 819], [542, 772]], [[468, 742], [1469, 1179]],
 [[244, 1731], [1043, 1583]], [[1103, 229], [856, 409]],
 [[1167, 1146], [677, 1241]], [[1516, 1178], [825, 1473]],
 [[289, 953], [528, 280]], [[449, 500], [119, 1688]],
 [[392, 20], [475, 869]], [[944, 199], [1857, 1344]]]
```

   (a) Decrypt the sequence of point pairs to obtain the sequence of points.

[1] URI: http://math.albany.edu/pers/hammond/course/mat587s2009/eelg.xhtml

(b) What text string of length 14 underlies the sequence of points?

2. Encrypt the length 35 text string

   `\int_1^2 \frac{dt}{t} = \mbox{ln} 2`

   for the elliptic curve $y^2 = x^3 - 7x + 10$ in the field $\mathbf{F}_{1867}$ as follows:

   (a) Compute the sequence of 35 points on the curve that correspond via the method described in section 2 of the recent course notes using 10 "tries" per point.

   (b) Find the sequence of point pairs representing the El Gamal encryption of the sequence of points when the base point b and the public key c (related by the formula $c = jb$ where j, an integer, is the secret key) are given by

   $$b = [123, 22] \qquad c = [669, 795]$$

   and where the pair $[q, r]$ for a given point p in the sequence is computed using the formulae

   $$\begin{aligned} q &= kb \\ r &= p + kc \end{aligned}$$

   where, for pedagogical reasons, the number k, which usually should be a random value modulo the order of b, is instead computed as

   $$127n + 307 \text{ modulo the order of } b$$

   with n the position of the point p in the sequence of points.