MATH 674.3 Winter 2014

Written Assignment 5

Instructions: Solutions must be provided in one of the following formats.

- **LaTeX (preferred). Download the template to make this easier.**
- **Word or your choice of software, with proper math formatting and converted into a single .pdf file.**
- **Hand-written solutions, written legibly with HB2 pencil on un-lined paper, and scanned into a single .pdf file.**

1. [2 marks]
When elliptic curves are used for cryptography, why are elliptic curves over finite fields better than elliptic curves over the real numbers?

2. [8 marks]
An elliptic curve $y^2 = x^3 + ax + b \pmod{29}$ includes points $P = (7, 15)$ and $Q = (16, 13)$.

   (a) Determine with justification the equation of the curve.

   (b) Determine with justification all values of x for which there is no point (x, y) on the curve.

3. [5 marks]
Sometimes students wonder why the geometric construction $P + Q$ requires the reflection step. Suppose instead that we used a simpler no-reflection definition to add elliptic curve points, letting $R = P + Q$ where P, Q, R are collinear points on an elliptic curve (i.e. removing the reflection step from the definition of addition).

   (a) Show that with a *no-reflection* definition of addition, we could get $2P = \mathcal{O}$ for every choice of P.

   (b) What advantage does the actual definition of addition (that is, with the reflection step) have over the *no-reflection* definition of $R = P + Q$?

4. [8 marks]
For this question, you may work by hand or use the applet Elliptic Curves Applet: over Z_p in the Content for Module 5. Computations are over the elliptic curve $y^2 = x^3 + 11x + 6$ over $\mathbb{Z}_{23}$. To support your answer, you can quote calculations without great detail. For example, you could say that $2(2, 6) = (19, 17)$, without detailing the calculations of m, x, y.
Tip: *Organize your work to avoid unnecessary repetition.*

   Given a positive integer k, define a set of points $S(k)$ on the elliptic curve as follows:
   $P \in S(k)$ **IF AND ONLY IF** $[(2^k)P = \mathcal{O}$ AND $(2^{k-1})P \neq \mathcal{O}]$.

   (a) Determine with justification all points in $S(1)$.

   (b) Determine with justification all points in $S(2)$.

   (c) Determine with justification the largest value of k for which $S(k)$ is not empty, and the corresponding points in $S(k)$.

5. [13 marks]
Finding $\frac{1}{2}R$ *with Bisection Method*: Let $R = (3, 3.742)$ on the elliptic curve $y^2 = x^3 - 6x + 5$ over the real numbers. *Goal:* Using a bisection method, we will determine a point P_n on the curve so that $2P_n \approx R$ or $P_n \approx \frac{1}{2}R$.

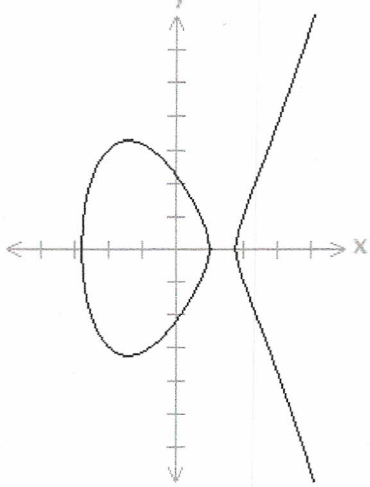
Round and show all numbers to 3 decimal places.
Method: In parts (a)-(c), we determine suitable starting points P_1 and P_2.

(a) If $P_1 = (0.400, y_1)$ and $P_2 = (0.750, y_2)$ lie on the curve, determine the possible values for y_1 and y_2.

(b) For each possibility in (a), determine the corresponding coordinates of $2P_1$ and $2P_2$.

(c) From (a) and (b), select the values of y_1, y_2 so that $P_1 = (0.400, y_1)$, $P_2 = (0.750, y_2)$ lie on the curve, and so that $2P_1$, $2P_2$ and R lie in the same quadrant of the xy plane and on the same piece of the elliptic curve.

On the elliptic curve to the right, graph R, P_1 and its geometric construction of $2P_1$, and P_2 and its geometric construction of $2P_2$.



(d) Beginning with P_1 and P_2 from (c), list a sequence of points $P_1, P_2, P_3, ..., P_n$, all in the same quadrant of the xy plane, so that each successive x_{2P_i} gets closer and closer to x_R; that is, $|x_{2P_{i+1}} - x_R| \leq |x_{2P_i} - x_R|$ for most (but not necessarily all) $i \geq 2$.
The last point in your sequence, P_n, should satisfy $|x_{2P_n} - x_R| \leq 0.005$ so that $2P_n \approx R$.

i	3	4	...
k	2		
j	1		
$x_{P_i} = \frac{x_{P_j} + x_{P_k}}{2}$			
y_{P_i}			
m			
x_{2P_i}			
y_{2P_i}			
$\lvert x_{2P_i} - x_R \rvert$			

Bisection Method: To create each successive point P_i in the sequence, find two previous points P_j and P_k as late as possible in the sequence such that $x_{2P_j} < x_R < x_{2P_k}$. Then define x_{P_i} as the average of x_{P_j} and x_{P_k}, and calculate the corresponding values of y_{P_i}, m, x_{2P_i}, y_{2P_i} and $|x_{2P_i} - x_R|$. Report your results in a table like that to the right, including as many columns as necessary. Computations may be done in a spreadsheet such as Excel. You may include a screenshot of your work.