Graded Homework 7 (40 points)
DUE 1600 19 November 2018

Instructions: This is a graded homework assignment worth 40 points. Solutions must be organized, neat in appearance, and must clearly indicate the answer to each problem. Be sure to show your work where appropriate.

1. (20 points) Let E be the elliptic curve

$$E\colon y^2 = x^3 + x + 1$$

and let $P = (4, 2)$ and $Q = (0, 1)$ be the points on E modulo 5. Solve the elliptic curve discrete logarithm problem for P and Q, that is, find a positive integer n such that $Q = nP$.

Using the algorithm described in class we will evaluate nP for $n = 1, 2, \cdots$, until we get Q,

$$P \oplus P = (4, 2) \oplus (4, 2)$$

$$\lambda = \frac{3(4)^2 + 1}{2(2)} \equiv \frac{49}{4} \equiv \frac{4}{4} \equiv 1 \pmod 5$$

$$x_3 \equiv 1^2 - 4 - 4 \equiv 1 - 4 - 4 \equiv -7 \equiv 3 \pmod 5$$

$$y_3 \equiv 1(4 - 3) - 2 \equiv -1 \equiv 4 \pmod 5$$

$$2P = [3, 4, 1]$$

Next for $3P$, we will evaluate $3P = P \oplus 2P$

$$P \oplus 2P = (4, 2) \oplus (3, 4)$$

$$\lambda = \frac{4 - 2}{3 - 4} \equiv \frac{2}{4} \equiv 2 \cdot 4 \equiv 3 \pmod 5$$

$$x_3 \equiv 3^2 - 4 - 3 \equiv 2 \pmod 5$$

$$y_3 \equiv 3(4 - 2) - 2 \equiv 4 \pmod 5$$

$$3P = [2, 4, 1]$$

So $n \neq 3$, thus we must strive on. For $4P$ we calculate $2P \oplus 2P$.

$$2P \oplus 2P = (3, 4) \oplus (3, 4)$$

$$\lambda = \frac{3(3)^2 + 1}{2(4)} \equiv \frac{28}{8} \equiv \frac{3}{3} \equiv 1 \pmod 5$$

$$x_3 \equiv 1^2 - 3 - 3 \equiv 0 \pmod 5$$

$$y_3 \equiv 1(3-0) - 4 \equiv 4 \pmod 5$$
$$4P = [0, 4, 1]$$

Again we fall short, for $5P = 3P \oplus 2P$ we get,

$$3P \oplus 2P = (2, 4) \oplus (3, 4)$$
$$\lambda = \frac{4-4}{3-2} \equiv \frac{0}{1} \equiv 0 \pmod 5$$
$$x_3 \equiv 0^2 - 2 - 3 \equiv 0 \pmod 5$$
$$y_3 \equiv 0(2-0) - 4 \equiv 1 \pmod 5$$
$$5P = [0, 1, 1]$$

Hurray! $n = 5$, so $5P = Q$.

2. (20 points) Use the double-and-add algorithm (Table 6.3) to compute nP in $E(\mathbb{F}_p)$ for the following curves and points.

$$E\colon Y^2 = x^3 + 23X + 13, \qquad p = 83, \qquad P = (24, 14), \qquad n = 19.$$

Using the double-and-add algorithm we need to split n into binary, $n = 16 + 2 + 1$. So we need to compute $19P = 16P + 2P + P$. Before we do we need to calculate the second powers of P, we start with $2P$. For all the inverses I used wolfram alpha to compute them.

$$P \oplus P = (24, 14) \oplus (24, 14)$$
$$\lambda \equiv \frac{3(24)^2 + 23}{2(14)} \equiv \frac{8}{28} \equiv 8 \cdot 3 \equiv 24 \pmod{83}$$
$$x_3 \equiv 24^2 - 24 - 24 \equiv 30 \pmod{83}$$
$$y_3 \equiv 24(24 - 30) - 14 \equiv 8 \pmod{83}$$
$$2P = [30, 8, 1]$$

$$2P \oplus 2P = (30, 8) \oplus (30, 8)$$
$$\lambda \equiv \frac{3(30)^2 + 23}{2(8)} \equiv \frac{67}{16} \equiv 67 \cdot 26 \equiv 82 \pmod{83}$$
$$x_3 \equiv 82^2 - 30 - 30 \equiv 24 \pmod{83}$$
$$y_3 \equiv 82(30 - 24) - 8 \equiv 69 \pmod{83}$$
$$4P = [24, 69, 1]$$

$$4P \oplus 4P = (24, 69) \oplus (24, 69)$$
$$\lambda \equiv \frac{3(24)^2 + 23}{2(69)} \equiv \frac{8}{55} \equiv 8 \cdot 80 \equiv 59 \pmod{83}$$
$$x_3 \equiv 59^2 - 24 - 24 \equiv 30 \pmod{83}$$
$$y_3 \equiv 59(24 - 30) - 69 \equiv 75 \pmod{83}$$
$$8P = [30, 75, 1]$$

$$8P \oplus 8P = (30, 75) \oplus (30, 75)$$
$$\lambda \equiv \frac{3(30)^2 + 23}{2(75)} \equiv \frac{67}{67} \equiv 1 \pmod{83}$$
$$x_3 \equiv 1^2 - 30 - 30 \equiv 24 \pmod{83}$$
$$y_3 \equiv 1(30 - 24) - 75 \equiv 14 \pmod{83}$$
$$16P = [24, 14, 1]$$

We can see here that $16P = P$ this allows us to rearrange our first equation as $19P = P \oplus 2P \oplus P = 4P$, thus we have already calculated $4P = [24, 69, 1]$ so $19P = [24, 69, 1]$.