Math 400 Fall 2018
Cryptology HW 7 Solutions
Due Thursday, October 18

Problems 2 and 3 will be worth 20 points each.

1. The group S_3 is the set $\{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$, where e is the identity and multiplication obeys the following rules: $\sigma^3 = e = \tau^2, \tau\sigma = \sigma^2\tau$.

   (a) What are σ^{-1} and τ^{-1}? That is, tell me which of the six elements in the set I gave you is σ^{-1} and which is τ^{-1}.

   (b) Compute $\tau\sigma^2, \tau(\sigma\tau), (\sigma\tau)(\sigma\tau)$, an $(\sigma\tau)(\sigma^2\tau)$. (Again, your answer for each part should be one of the six elements I gave you.)

   Solution:

   (a) $\sigma^{-1} = \sigma^2$ and $\tau^{-1} = \tau$.

   (b)

$$\begin{aligned}
\tau\sigma^2 &= \sigma^2\tau\sigma = \sigma^4\tau = \sigma\tau \\
\tau\sigma\tau &= \sigma^2\tau\tau = \sigma^2 \\
\sigma\tau\sigma\tau &= \sigma\sigma^2\tau\tau = \sigma^3\tau^2 = ee = e \\
\sigma\tau\sigma^2\tau &= \sigma\sigma\tau\tau = \sigma^2.
\end{aligned}$$

2. Let $E : y^2 = x^3 - 2x + 4$, and let $P = (0, 2)$ and $Q = (3, -5)$.

   (a) Check that $P, Q \in E(\mathbb{Q})$.

   (b) Compute Δ to confirm that this is an elliptic curve.

   (c) Compute $P \oplus Q$.

   (d) Compute $P \oplus P$ and $Q \oplus Q$.

   (e) Compute $3P = P \oplus P \oplus P$ and $3Q = Q \oplus Q \oplus Q$.

   Solution:

   (a) $0^3 - 2 \cdot 0 + 4 = 4 = 2^2$ and $3^3 - 2 \cdot 3 + 4 = 25 = 5^2$ so these are on the curve.

   (b) $\Delta = 4A^3 + 27B^2 = 4 \cdot (-2)^3 + 27 \cdot 4^2 = -32 + 432 = 400 \neq 0$ so this is an elliptic curve.

(c) The line through P and Q is given by $y = \frac{-5-2}{3-0}(x-0)+2 = -\frac{7}{3}x+2$.
We plug this into the cubic and get

$$\begin{aligned}(2-7x/3)^2 &= x^3-2x+4\\ 4-28x/3+49x^2/9 &= x^3-2x+4\\ 0 &= x^3-49x^2/9+22x/3\end{aligned}$$

and we know that $-49/9 = -x_1-x_2-x_3 = -0-3-x_3$ so $-22/9 = x_3$ and $x_3 = 22/9$.
Plugging this back into the equation for the line, we get $y_3 = -154/27+2 = -100/27$, so $P \oplus Q = (22/9, 100/27)$.

(d) We have $2yy' = 3x^2-2$, so at the point P we have $2\cdot 2\cdot y' = 3\cdot 0^2-2$ or $y' = -1/2$. Thus the tangent line is $y = -x/2+2$.
Plugging this into the cubic gives

$$\begin{aligned}(-x/2+2)^2 &= x^3-2x+4\\ x^2/4-2x+4 &= x^3-2x+4\\ 0 &= x^3-x^2/4\end{aligned}$$

and we have $-1/4 = -x_1-x_2-x_3 = -0-0-x_3$ so $x_3 = 1/4$.
Plugging this into the line gives $y_3 = -1/8+2 = 15/8$. Thus we have $P\oplus P = (1/4, -15/8)$
Similarly, at the point Q we have $2\cdot(-5)\cdot y' = 3\cdot 3^2-2$ or $-10y' = 25$, so $y' = -5/2$. Thus the tangent line is $y = -5/2(x-3)-5 = -5x/2+5/2$.
Plugging this into the cubic gives

$$\begin{aligned}(-5x/2+5/2)^2 &= x^3-2x+4\\ 25x^2/4-25x/2+25/4 &= x^3-2x+4\\ 0 &= x^3-25x^2/4+21x/2-9/4\end{aligned}$$

and we have $-25/4 = -x_1-x_2-x_3 = -3-3-x_3$ so $-1/4 = -x_3$ and $x_3 = 1/4$.
Plugging this into the line gives $y_3 = -5/8+5/2 = 15/8$, so $Q\oplus Q = (1/4, -15/8)$.

(e) We have $3Q = (-237/121, -845/1331)$ and $3P = (240, 3718)$.
In particular, $3P = (1/4, -15/8)\oplus(0,2)$. The line connecting these two points is $y = \frac{2+15/8}{0-1/4}(x-0)+2 = -31x/2+2$.
Plugging this into the cubic gives

$$\begin{aligned}(2-31x/2)^2 &= x^3-2x+4\\ 4-62x+961x^2/4 &= x^3-2x+4\\ 0 &= x^3-961x^2/4+60x\end{aligned}$$

and we have $-961/4 = -x_1-x_2-x_3 = -0-1/4-x_3$ so $x_3 = 960/4 = 240$.
Plugging this back into the line gives $y_3 = -31(240)/2+2 = -3718$, so $3P = (240, 3718)$.

Similarly, $3Q = (1/4, -15/8) \oplus (3, -5)$. The line connecting these two points is $y = \frac{-5+15/8}{3-1/4}(x-3) - 5 = \frac{-25/8}{11/4}(x-3) - 5 = \frac{-25}{22}(x-3) - 5 = \frac{-25}{22}x - \frac{35}{22}$.
Plugging this into the cubic gives

$$\begin{aligned}(-25x/22 - 35/22)^2 &= x^3 - 2x + 4\\ 1225/484 + 875x/242 + 625x^2/484 &= x^3 - 2x + 4\\ 0 &= x^3 - 625x^2/484 - 1359x/242 + 711/484\end{aligned}$$

and we have $-625/484 = -x_1 - x_2 - x_3 = -3 - 1/4 - x_3$ so $x_3 = -237/121$.
Plugging this back into the line gives $y_3 = (-25/22)(-237/121) - 35/22 = 845/1331$. So $3Q = (-237/121, -845/1331)$.

3. Let $E : y^2 = x^3 + 17$. Let $P = (-1, 4)$ and let $Q = (2, 5)$.

   (a) Confirm that $P, Q \in E(\mathbb{Q})$.

   (b) Compute Δ to confirm that this is an elliptic curve.

   (c) Compute $P \oplus Q$ and $P - Q$.

   (d) Compute $2P = P \oplus P$ and $2Q = Q \oplus Q$.

   Solution:

   (a) $(-1)^3 + 17 = 15 = 4^2$ so $P \in E(\mathbb{Q})$, and $2^3 + 17 = 25 = 5^2$ so $Q \in E(\mathbb{Q})$.

   (b) $\Delta = 4A^3 + 27B^2 = 27 \cdot 17^2 = 7803 \neq 0$ so this is an elliptic curve.

   (c) The line through P and Q is given by $y = \frac{5-4}{2+1}(x+1) + 4 = x/3 + 13/3$.
   Plugging this into the cubic gives

$$\begin{aligned}(x/3 + 13/3)^2 &= x^3 + 17\\ x^2/9 + 26x/9 + 169/9 &= x^3 + 17\\ 0 &= x^3 - x^2/9 + -26x/9 - 16/9\end{aligned}$$

   so we have $-1/9 = -x_1 - x_2 - x_3 = 1 - 2 - x_3$ and thus $x_3 = -8/9$.
   Plugging this back into the line gives us $y_3 = -8/27 + 13/3 = 109/27$, so $P \oplus Q = (-8/9, -109/27)$.
   $-Q = (2, -5)$, so the line through P and $-Q$ is $y = \frac{-5-4}{2+1}(x+1) + 4 = -3x + 1$.
   Plugging this into the cubic gives

$$\begin{aligned}(1 - 3x)^2 &= x^3 + 17\\ 1 - 6x + 9x^2 &= x^3 + 17\\ 0 &= x^3 - 9x^2 + 6x + 16\end{aligned}$$

   so we have $-9 = -x_1 - x_2 - x_3 = 1 - 2 - x_3$ and thus $x_3 = 8$.
   Plugging this back into the line gives us $y_3 = -24 + 1 = -23$, so $P - Q = (8, 23)$.

   (d) The derivative of the cubic is $2yy' = 3x^2$. So the derivative at P is $2 \cdot 4 \cdot y' = 3(-1)^2$ so we have $y' = 3/8$ and the equation for the tangent line is $y = 3/8(x+1) + 4 = 3x/8 + 35/8$.

Plugging this into the cubic gives

$$\begin{aligned}(3x/8 + 35/8)^2 &= x^3 + 17\\ 9x^2/64 + 105x/32 + 1225/64 &= x^3 + 17\\ 0 &= x^3 - 9x^2/64 - 105x/32 - 137/64\end{aligned}$$

so we have $-9/64 = -x_1 - x_2 - x_3 = 1 + 1 - x_3$ and so we have $x_3 = 137/64$.

Plugging this back into the line gives us $y_3 = 3 \cdot 137/8 \cdot 64 + 35/8 = 2651/512$, so $2P = (137/64, -2651/512)$.

The derivative at Q is given by $2 \cdot 5y' = 3 \cdot 2^2$ and thus $y' = 6/5$. Thus the equation for the tangent line is $y = 6/5(x - 2) + 5 = 6x/5 + 13/5$.

Plugging this into the cubic gives

$$\begin{aligned}(6x/5 + 13/5)^2 &= x^3 + 17\\ 36x^2/25 + 156x/25 + 169/25 &= x^3 + 17\\ 0 &= x^3 - 36x^2/25 - 156x/25 + 256/25\end{aligned}$$

so we have $36/25 = -2 - 2 - x_3$ and thus $x_3 = -64/25$.

Plugging this into the line gives $y_3 = 6/5(-64/25) + 13/5 = -59/125$ so $2Q = (-64/25, 59/125)$.

4. Consider the following curves:

   (i) $y^2 = x^3 - 7x + 3$

   (ii) $y^2 = x^3 - 7x + 9$

   (iii) $y^2 = x^3 - 7x - 12$

   (iv) $y^2 = x^3 - 3x + 2$

   (v) $y^2 = x^3$.

   (a) Compute the discriminant of each curve. Which of these are elliptic curves?

   (b) Sketch a graph of each curve (you may use a computer for this step). How can you visually tell which of these curves was an elliptic curve?

   Solution:

   (a) The discriminants are:

      (i) -1129

      (ii) 815

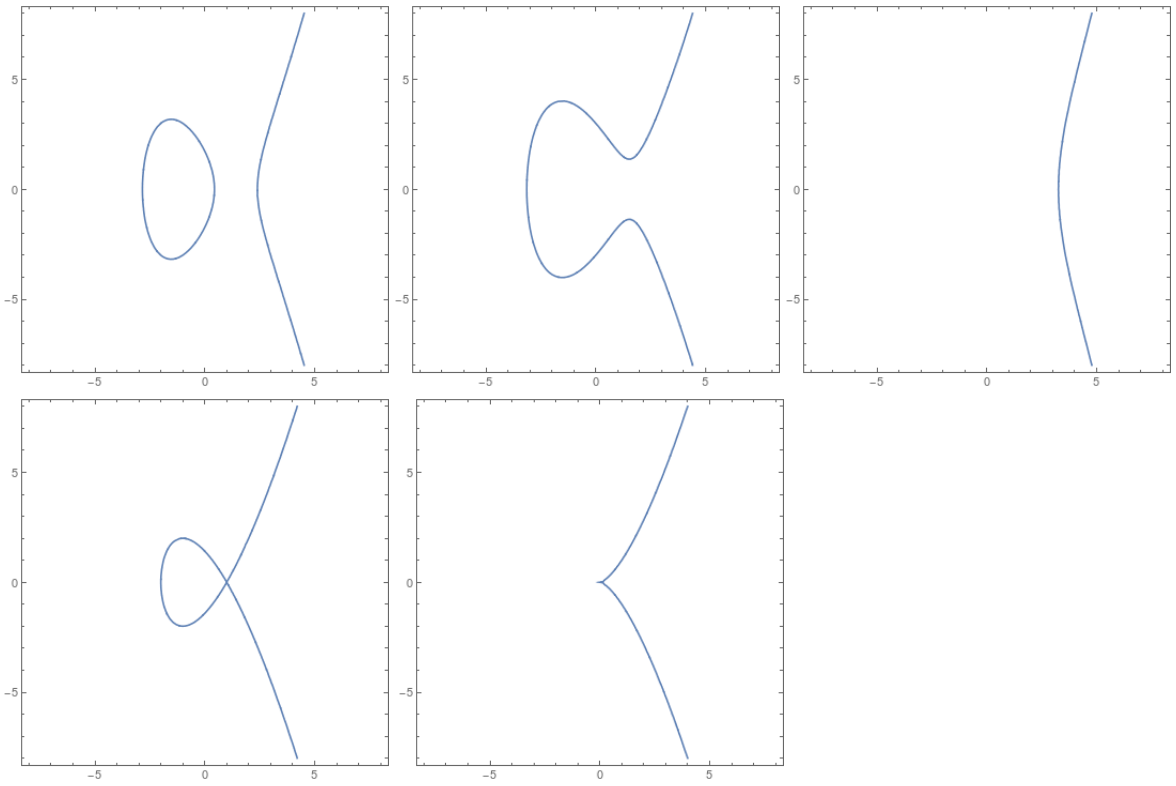
      (iii) 2516

      (iv) 0

      (v) 0

      So the first three are elliptic curves, and the last two are not.

(b)



We see the first three are smooth curves, and thus are reasonable elliptic curves. The fourth has a self-intersection and the fifth has a cusp, so are not differentiable everywhere, and so the elliptic curve addition isn't always well-defined.