Math 4981 Final Solutions

Instructor: Jay Daigle

May 4, 2021

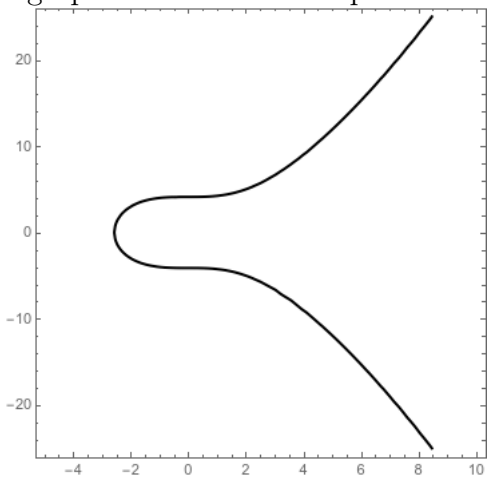
1. This test is due Tuesday, May 4, at midnight. Logistically, this will work just like the homework: download it, write up your answers, and upload them to Blackboard for me to grade.
2. You will have three hours for this test, though I don't expect you to need all of them. Please write down your start and end times on the test and include that in your upload. You may not spend more than three hours on the test unless you have a specific accommodation.
3. You may consult the course notes during this test, or any notes you have made for yourself.
4. If you have questions, I will be online and responsive during the official time slot 10:20–12:20. If you want to take the test at a time you know I'll be able to answer any questions quickly, I encourage you to use one of those time slots.
5. You may use a four-function calculator, but nothing more sophisticated. (You can use something like google or wolfram alpha, but only to do basic arithmetic!) Show all your work and explain all calculations you do.
6. Each problem is worth 20 points The maximum score for this test is 120 points.

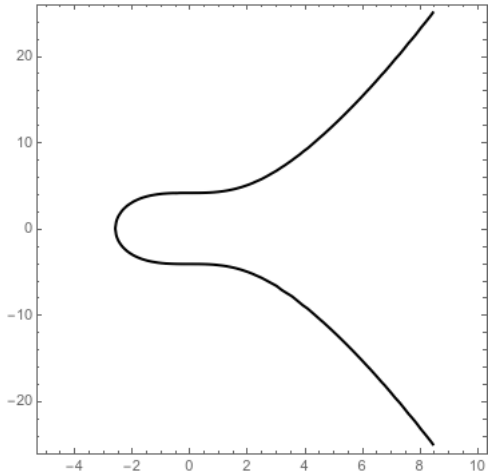
Name:

Time Started:

Time Completed:

Problem 1. Let $E : y^2 = x^3 + 17$, $P = (-2, 3)$, and $Q = (2, 5)$. Compute $2P - Q$ *geometrically*, explicitly giving an equation for each line involved, and sketching these lines on the graphs below or on a separate sheet.





Solution:

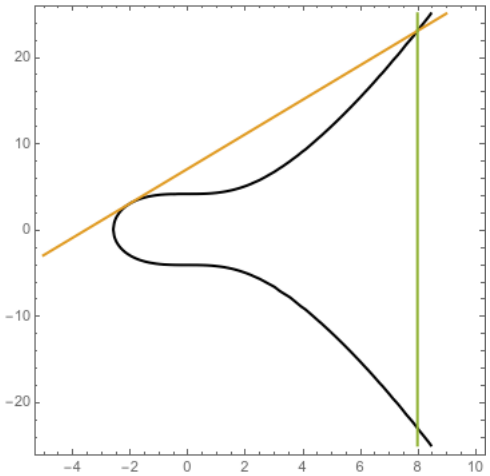
First we compute $2P$. We have $2yy' = 3x^2$, so at the point P we have $2 \cdot 3 \cdot y' = 3 \cdot 2^2$ and thus $y' = 2$. Then the equation of the tangent line is

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

and we get the cubic equation

$$\begin{aligned} (2x + 7)^2 &= x^3 + 17 \\ 4x^2 + 28x + 49 &= x^3 + 17 \\ 0 &= x^3 - 4x^2 - 28x - 32. \end{aligned}$$

We have $-4 = 2 + 2 - x_3$ so $x_3 = 8$; plugging this back into our equation gives $y = 23$, and flipping across the x axis gives us that $2P = (8, -23)$.



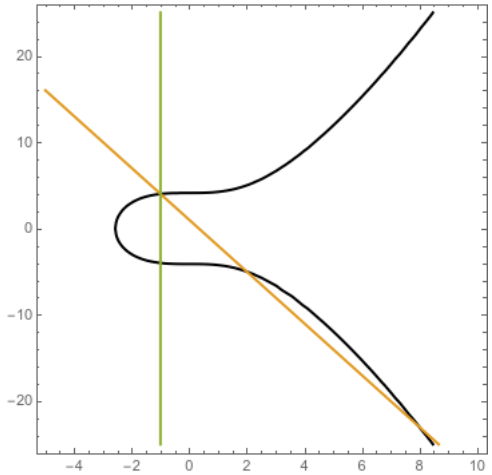
Now we compute $2P - Q$. The point $-Q = (2, -5)$, and the line between $2P$ and $-Q$ has slope $\frac{-5-(-23)}{2-8} = -3$, and thus has equation

$$y + 5 = -3(x - 2)$$

and we get the cubic equation

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

We have $-9 = -2-8-x_3$ and thus $x_3 = -1$. Plugging this back into our equation gives $y = 4$, and flipping across the x axis gives is $2P - Q = (-1, -4)$.



(We could also do this the other way. $P - Q = (4, 9)$, and then we can add P to $(4, 9)$ to get $(-1, -4)$. This way seems more natural to me, though.)

Problem 2. Suppose Alice and Bob want to communicate using a Elliptic Curve Diffie-Hellman scheme. They have chosen the curve $E : y^2 = x^3 + x + 3$, the field $\mathbb{F}_{23}$, and the point $P = (0, 7)$.

(a) If Alice chooses $n_A = 5$, what is her public key?

(b) If Bob's private key is $n_B = 3$, what does he compute as the shared secret?

Solution:

(a)

$$2P = (2,6) \qquad \lambda = \frac{3\cdot 0+1}{2\cdot 7} = \frac{1}{14} = 5$$
$$x = 5^2 - 0 - 0 = 2$$
$$y = 5(0-2) - 7 = -17 = 6$$

$$4P = (5,8) \qquad \lambda = \frac{3\cdot 2^2+1}{2\cdot 6} = \frac{13}{12} = 2\cdot 13 = 3$$
$$x = 3^2 - 2 - 2 = 5$$
$$y = 3(2-5) - 6 = 8$$

$$5P = (5,8) \oplus (0,7) = (7,10) \qquad \lambda = \frac{8-7}{5-0} = \frac{1}{5} = 14$$
$$x = 14^2 - 5 - 0 = 7$$
$$y = 14(5-7) - 8 = -36 = 10.$$

$5P = (7, 10)$.

(b) $2Q_A = (15, 9)$.

$3Q_A = (10, 22)$.

Problem 3. Set

$$U = \frac{1}{2}\begin{bmatrix} 1 & i & 1 & i \\ i & 1 & i & 1 \\ 1 & i & -1 & -i \\ i & 1 & -i & -1 \end{bmatrix}$$

$$|\Psi\rangle = \frac{1+i}{5}|00\rangle + \frac{2-i}{5}|01\rangle + \frac{2+3i}{5}|10\rangle + \frac{-2+i}{5}|11\rangle.$$

(a) Confirm that U is a unitary matrix.

(b) Confirm that $|\Psi\rangle$ is a valid state of a quantum computer.

(c) Compute $U|\Psi\rangle$. What is the probability of measuring each possible state?

Solution:

(a)

$$\begin{aligned} UU^\dagger &= \frac{1}{4}\begin{bmatrix} 1 & i & 1 & i \\ i & 1 & i & 1 \\ 1 & i & -1 & -i \\ i & 1 & -i & -1 \end{bmatrix}\begin{bmatrix} 1 & -i & 1 & -i \\ -i & 1 & -i & 1 \\ 1 & -i & -1 & i \\ -i & 1 & i & -1 \end{bmatrix} \\ &= \frac{1}{4}\begin{bmatrix} 4 & 0 & 0 & 0 \\ 0 & 4 & 0 & 0 \\ 0 & 0 & 4 & 0 \\ 0 & 0 & 0 & 4 \end{bmatrix}. \end{aligned}$$

(b)

$$\begin{aligned} \||\Psi\rangle\|^2 &= \left|\frac{1+i}{5}\right|^2 + \left|\frac{2-i}{5}\right|^2 + \left|\frac{2+3i}{5}\right|^2 + \left|\frac{-2+i}{5}\right|^2 \\ &= \frac{2}{25} + \frac{5}{25} + \frac{13}{25} + \frac{5}{25} = 1 \\ \||\Psi\rangle\| &= \sqrt{1} = 1. \end{aligned}$$

(c)

$$U|\Psi\rangle = \frac{1}{10}\begin{bmatrix} 1 & i & 1 & i \\ i & 1 & i & 1 \\ 1 & i & -1 & -i \\ i & 1 & -i & -1 \end{bmatrix}\begin{bmatrix} 1+i \\ 2-i \\ 2+3i \\ -2+i \end{bmatrix}$$
$$= \frac{1}{10}\begin{bmatrix} 1+i+2i+1+2+3i-2i-1 \\ i-1+2-i+2i-3-2+i \\ 1+i+2i+1-2-3i+2i+1 \\ i-1+2-i-2i+3+2-i \end{bmatrix}$$
$$= \frac{1}{10}\begin{bmatrix} 3+4i \\ -4+3i \\ 1+2i \\ 6-3i \end{bmatrix} = \begin{bmatrix} 3/10+2/5i \\ -2/5+3/10i \\ 1/10+1/5i \\ 3/5-3/10i \end{bmatrix}$$

and we get

$$P(|00\rangle) = \frac{9+16}{100} = \frac{1}{4}$$
$$P(|01\rangle) = \frac{16+9}{100} = \frac{1}{4}$$
$$P(|10\rangle) = \frac{1+4}{100} = \frac{1}{20}$$
$$P(|11\rangle) = \frac{36+9}{100} = \frac{9}{20}$$

Problem 4. (a) Let

$$|\Psi\rangle = \frac{i}{4}|00\rangle + \frac{-3+i}{4}|01\rangle + \frac{2i}{4}|10\rangle + \frac{-1}{4}|11\rangle.$$

Compute $U_{FT}|\Psi\rangle$.

(b) Suppose we wish to use Knapsack cryptography with the public key

$$\mathbf{M} = (51, 84, 170, 186, , 253, 284).$$

Encrypt the plaintext $(1, 0, 0, 0, 1, 1)$. Decrypt the ciphertext $S = 554$.
Solution:

(a) We (still) know that

$$\begin{aligned}
U_{FT}|00\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 0\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{1}{2}|11\rangle \\
U_{FT}|01\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 1\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{i}{2}|01\rangle + \frac{-1}{2}|10\rangle + \frac{-i}{2}|11\rangle \\
U_{FT}|10\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 2\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{-1}{2}|01\rangle + \frac{1}{2}|10\rangle + \frac{-1}{2}|11\rangle \\
U_{FT}|00\rangle &= \frac{1}{2}\sum_{y=0}^{3}\exp(2\pi i\cdot 3\cdot y/4)|y\rangle_2 \\
&= \frac{1}{2}|00\rangle + \frac{-i}{2}|01\rangle + \frac{-1}{2}|10\rangle + \frac{i}{2}|11\rangle
\end{aligned}$$

and so

$$\begin{aligned}
U_{FT}|\Psi\rangle &= \frac{i}{4}U_{FT}|00\rangle + \frac{-3+i}{4}U_{FT}|01\rangle + \frac{2i}{4}U_{FT}|10\rangle + \frac{-1}{4}U_{FT}|11\rangle \\
&= \frac{i}{8}|00\rangle + \frac{i}{8}|01\rangle + \frac{i}{8}|10\rangle + \frac{i}{8}|11\rangle \\
&\quad + \frac{-3+i}{8}|00\rangle + \frac{-1-3i}{8}|01\rangle + \frac{3-i}{8}|10\rangle + \frac{1+3i}{8}|11\rangle \\
&\quad + \frac{2i}{8}|00\rangle + \frac{-2i}{8}|01\rangle + \frac{2i}{8}|10\rangle + \frac{-2i}{8}|11\rangle \\
&\quad + \frac{-1}{8}|00\rangle + \frac{i}{8}|01\rangle + \frac{1}{8}|10\rangle + \frac{-i}{8}|11\rangle \\
&= \frac{-4+4i}{8}|00\rangle + \frac{-1-3i}{8}|01\rangle + \frac{4+2i}{8}|10\rangle + \frac{1+i}{8}|11\rangle.
\end{aligned}$$

(b) To encrypt we get $51 + 253 + 284 = 588$. To decrypt we see that $S = 84 + 186 + 284$ and thus we get the plaintext $(0, 1, 0, 1, 0, 1)$.

Problem 5. Take $n = 4, q = 41$, and set $R_q = \mathbb{Z}/41\mathbb{Z}[x]/\langle x^4+1\rangle$. We set $a(x) = 3x^3+5x-8$. We can use the New Hope algorithm to generate a shared secret with another person.

(a) Suppose we generate random elements $s_0(x) = x^3 + 2x$ and $s_1(x) = x^2 - x$. What public key do we generate?

(b) If we receive the encapsulated ciphertext

$$c = \Big(5x^3 - 2, (1, 0, 1, 0)\Big)$$

what shared secret do we decapsulate (using the same s_0 and s_1 as the previous part)?

(c) In a separate interaction, suppose we receive the public key $b(x) = 5x^2-12$, and we want to generate a shared secret. We generate the random polynomials $e_0(x) = x^3+1, e_1(x) = 2x^2 + x, e_2(x) = -x + 2$. What is our shared secret, and what do we transmit?

Solution:

(a) $b(x) = s_1a + s_0 = 6x^3 + 28x^2 + 7x + 3 = 6x^3 - 13x^2 + 7x + 3.$

(b) We compute

$$\begin{aligned} w &= us_1 = -2x^2 - 3x + 5 \\ \mu &= \mathrm{rec}(w, v') = \mathrm{rec}\Big(- 2x^2 - 3x + 5, (1, 0, 1, 0)\Big) \\ &= (0, 0, 0, 0). \end{aligned}$$

(c) We have

$$\begin{aligned} I_0 &= [0, 10] \\ I_1' &= [11, 20] \\ I_0' &= [21, 30] = [-21, -11] \\ I_1 &= [31, 40] = [-10, -1] \end{aligned}$$

so we compute

$$\begin{aligned} u &= e_0a + e_1 = -5x^3 - x^2 + 6x - 13 \\ v &= e_0b + e_2 = -12x^3 + 5x^2 - 6x - 10 \\ \lfloor v \rceil_2 &= (1, 0, 0, 0) \\ \langle v \rangle_2 &= (0, 0, 1, 1). \end{aligned}$$

Our shared secret is $\mu = \lfloor v \rceil_2 = (1, 0, 0, 0)$, and we transmit

$$(u, \langle v \rangle_2) = \Big(- 5x^3 - x^2 + 6x - 13, (0, 0, 1, 1)\Big)$$

Problem 6. Take $n = 4, q = 17$, and set $R_q = \mathbb{Z}/17\mathbb{Z}[x]/\langle x^4 + 1\rangle$. We set the key to be $s(x) = -x^3 + 9x^2 - 5$. We can use the somewhat homomorphic algorithm to symmetrically encrypt and decrypt messages.

(a) Use the polynomials $a = 2x^2 + 4x$ and $e = x^2 + 1$ to encrypt the message $m = x^3 + x + 1$.

(b) If we have the ciphertexts

$$\vec{c} = (x^3 + 5x - 2, 3x^2 - 5x + 7)$$
$$\vec{c}' = (4x^2 + 7x - 5, 5x^3 + x)$$

compute the ciphertext for $\vec{c} \cdot \vec{c}'$.

(c) If we receive the ciphertext

$$\Big(x^2 + 1, 3x^3 - x + 1, 5x^2 + 5x\Big)$$

what bit-string does it decrypt to?

Solution:

(a) We have $c_1 = -a = -2x^2 - 4x$, and $c_0 = as + 2e + m = 3x^3 + 9x^2 + 6$.

(b) We rewrite as polynomials, and then

$$\begin{aligned}\vec{c} \cdot \vec{c}' &= \big((x^3 + 5x - 2) + v(3x^2 - 5x + 7)\big)\big((4x^2 + 7x - 5) + v(5x^3 + x)\big) \\ &= (3 + 8x + 10x^2 + 15x^3) + v(12 + 4x + 12x^2 + 8x^3) + v^2(8 + 9x + 12x^2 + 4x^3)\end{aligned}$$

(c) We decrypt by plugging in s to our polynomial, so we get

$$\begin{aligned}\langle \vec{c}, s\rangle &= (x^2 + 1) + (3x^3 - x + 1)(-x^3 + 9x^2 - 5) + (5x^2 + 5x)(-x^3 + 9x^2 - 5)^2 \\ &= x^3 - 7x^2 + 5x - 8 \equiv x^3 + x^2 + x\end{aligned}$$

so we get the message $(1, 1, 1, 0)$.