Graded Homework 6 (50 points)

Kimberly Mandery

DUE 1600 181114

Instructions: This is a graded homework assignment worth 50 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. (15 points) Suppose that the cubic polynomial $X^3 + AX + B$ factors as

$$X^3 + AX + B = (X - e_1)(X - e_2)(X - e_3).$$

Prove that $4A^3 + 27B^2 = 0$ if and only if two (or more) of e_1, e_2, and e_3 are the same. (*Hint:* Multiply out the right-hand side and compare coefficients to relate A and B to e_1, e_2, and e_3.)

Proof.
Starting with factors, we have $X^3 + AX + B$ equal to

$$(X - e_1)(X - e_2)(X - e_3).$$

Expanding we get $X^3 + AX + B$ equal to

$$X^3 - X^2(e_1 + e_2 + e_3) + X(e_1e_2 + e_1e_3 + e_2e_3) - e_1e_2e_3.$$

We can match up the left side with the right in order to find that

$$A = e_1e_2 + e_1e_3 + e_2e_3 \text{ and } B = -e_1e_2e_3.$$

Forward Approach
We can plug A and B into our equation $4A^3 + 27B^2 = 0$

$$4(e_1e_2 + e_1e_3 + e_2e_3)^3 + 27(-e_1e_2e_3)^2 = 0.$$

Expanding and simplifying, we get

$$4e_2^3e_3^3 + 12e_1e_2^2e_3^2(e_2 + e_3) + 4e_1^3(e_2 + e_3)^3 + 3e_1^2e_2e_3(4e_2^2 + 17e_2e_3 + 4e_3^2).$$

We know that as roots $-e_1 - e_2 - e_3 = 0$ so we can substitute $e_1 = -e_2 - e_3$ and obtain

$$4e_2^3e_3^3 + 12(-e_2 - e_3)e_2^2e_3^2(e_2 + e_3) + 4(-e_2 - e_3)^3(e_2 + e_3)^3 + 3(-e_2 - e_3)^2e_2e_3(4e_2^2 + 17e_2e_3 + 4e_3^2).$$

Factoring we get

$$-(e_1 - e_3)^2(2e_2 + e_3)^2(e_2 + 2e_3)^2.$$

Thus we get, respectively,

$$e_2 = e_3 \text{ and } e_2 = e_1 \text{ and } e_1 = e_3.$$

Reverse Approach
If we begin with the fact that at least two of the factors are equal (WLOG, say $e_2 = e_3$) we get

$$A = 2e_1e_2 + e_2^2 \text{ and } B = -e_1e_2^2.$$

Then our equation $4A^3 + 27B^2$ becomes

$$4(2e_1e_2 + e_2^2)^3 + 27(-e_1e_2^2)^2$$

$$4e_2^6 + 24e_1e_2^5 + 75e_1^2e_2^4 + 32e_1^3e_2^3.$$

We know that $e_1 = -2e_2$ so substituting in we have

$$4e_2^6 + 24(-2e_2)e_2^5 + 75(-2e_2)^2e_2^4 + 32(-2e_2)^3e_2^3.$$

Simplifying we get $4e_2^6 - 48e_2^6 + 300e_2^6 - 256e_2^6$ which is equal to 0, thus $4A^3 + 27B^2 = 0$.

2. (15 points) For the elliptic curve $E\colon Y^2 = X^3 + 3X + 2$ over the finite field $\mathbb{F}_7$, make a list of the set of points $E(\mathbb{F}_7)$.

Since $\mathbb{F}_7 \cong \mathbb{Z}_7$, we let $X \in \mathbb{Z}_7$ in order to find all $Y \in \mathbb{Z}_7$ satisfying E. To begin, we can compute the square of all elements in $\mathbb{Z}_7$. The following table will organize these into similar groups.

$Y^2 \equiv 0$	$Y^2 \equiv 1$	$Y^2 \equiv 2$	$Y^2 \equiv 4$
$0^2 \bmod 7 \equiv 0$	$1^2 \bmod 7 \equiv 1$	$3^2 \bmod 7 \equiv 2$	$2^2 \bmod 7 \equiv 4$
	$6^2 \bmod 7 \equiv 1$	$4^2 \bmod 7 \equiv 2$	$5^2 \bmod 7 \equiv 4$

If X=0, then $Y^2 = (0)^3 + 3(0) + 2 \Rightarrow Y^2 = 2$. This corresponds to the Y values 3 and 4, giving the equivalence points [0,3,1] and [0,4,1]. We can continue in this fashion to produce the entire list of these points $E(\mathbb{F}_7)$ being

$$\{\mathcal{O}, [0,3,1], [0,4,1], [2,3,1], [2,4,1], [4,1,1], [4,6,1], [5,3,1], [5,4,1]\}.$$

3. (20 points) Decrypt the message in runes on the cover of Tolkien's famous novel.

Because of the high prevalence of repeated segments of runes and pre-esxisting knowledge of the Tolkien universe, this decryption was straightforward. After verifying the repetition of *one ring to* verb *them*, it was a simple task of constructing the rest of the message. Thus the passage reads

One ring to rule them all.
One ring to find them.
One ring to bring them all
and in the darkness bind them.