# Crypto Homework 6

Noah Wong

November 2018

1.) 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.

Expanding out the right side of the factors we get,

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

Thus in the form of a cubic polynomial we have,

$$B = -e_1e_2e_3,$$
$$A = (e_1e_2 + e_2e_3 + e_1e_3)$$
$$0 = e_1 + e_2 + e_3.$$

($\implies$): First we will show that if $4A^3 + 27B^2 = 0$ then two (or more) of $e_1, e_2$ and $e_3$ are the same. Now having $A$ and $B$ in terms of our factors $e_1, e_2$ and $e_3$ we can plug these into $4A^3 + 27B^2 = 0$ to get,

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

Using Wolfram Mathematica to simplify our equations equations we get,

$$4e_1^3e_2^3 + 12e_1^3e_2^2e3 + 12e_1^2e_2^3e_3 + 12e_1^3e_2e_3^2 + 51e_1^2e_2^2e_3^2 + 12e_1e_2^3e_3^2 + 4e_1^3e_3^3 + 12e_1^2e_2e_3^3 + 12e_1e_2^2e_3^3 + 4e_2^3e_3^3.$$

Then we can substitute $e_1 = -e_2 - e_3$ since $0 = e_1 + e_2 + e_3$. Using Mathematica again to avoid unnecessary computation we get,

$$-4e_2^6 - 12e_2^5e_3 + 3e_2^4e_3^2 + 26e_2^3e_3^3 + 3e_2^2e_3^4 - 12e_2e_3^5 - 4e_3^6.$$

This factors into

$$(e_2 - e_3)^2(2e_2 + e_3)^2(e_2 + 2e_3)^2 = 0.$$

Thus there are three cases, one if $e_2 - e_3 = 0$, then $e_2 = e_3$ and we are done. Two, if $2e_2 + e_3 = 0$ then $2e_2 = -e_3$ and putting this back into the equation for $e_1$ gives us $e_1 = -e_2 + 2e_2 = e_2$, so $e_1 = e_2$. Three, if $e_2 + 2e_3 = 0$ then $e_2 = -2e_3$ and putting this back into the equation for $e_1 = -e_2 - e_3$ gives us $e_1 = 2e_3 - e_3$ thus $e_1 = e_3$.

($\impliedby$): Now we will show that if two (or more) of $e_1, e_2$ and $e_3$ are the same, then $4A^3 + 27B^2 = 0$. Without loss of generality assume that $e_1 = e_2 = e$, then $e_3 = -2e$. Then $A = e^2 - 4e^2 = -3e^2$ and $B = -2e^3$. Thus for $4A^3 + 27B^2$ we are given,

$$4(-3e^2)^3 + 27(-2e^3)^2,$$
$$4(-27e^6) + 27(4e^6) = 0.$$

Thus if two (or more) of $e_1, e_2$ and $e_3$ are the same, then $4A^3 + 27B^2 = 0$.

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

First we will examine the squares in $\mathbb{F}_7$ to cross-check later.

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

Now looking at the seven possibilites for $X$ and finding which values work for $Y$.

$$X = 0 \quad 0^3 + 3(0) + 2 = Y \quad 2 = Y^2 \quad Y = 3, 4 \quad (0, 3)\ (0, 4)$$
$$X = 1 \quad 1^3 + 3(1) + 2 = Y \quad 6 = Y^2 \quad Y = \emptyset \quad \text{Nothing}$$
$$X = 2 \quad 2^3 + 3(2) + 2 = Y \quad 2 = Y^2 \quad Y = 3, 4 \quad (2, 3)\ (2, 4)$$
$$X = 3 \quad 3^3 + 3(3) + 2 = Y \quad 3 = Y2 \quad Y = \emptyset \quad \text{Nothing}$$
$$X = 4 \quad 4^3 + 3(4) + 2 = Y \quad 1 = Y^2 \quad Y = 1, 6 \quad (4, 1)\ (4, 6)$$
$$X = 5 \quad 5^3 + 3(5) + 2 = Y \quad 2 = Y^2 \quad Y = 3, 4 \quad (5, 3)\ (5, 4)$$
$$X = 6 \quad 6^3 + 3(6) + 2 = Y \quad 5 = Y^2 \quad Y = \emptyset \quad \text{Nothing}$$

So the points of $E : (\mathbb{F}_7)$ are $\mathcal{O}$, $[0, 3, 1]$, $[0, 4, 1]$, $[2, 3, 1]$, $[2, 4, 1]$, $[4, 1, 1]$, $[4, 6, 1]$, $[5, 3, 1]$, $[5, 4, 1]$, where $\mathbb{O}$ is the point at infinity.

3.) Decrypt the message in runes on the cover of Tolkien's famous novel as depicted on the next page.

The message comes in 4 parts one along each side of the cover. Starting at the top and going clockwise, he message in runes is,

ᚠᚾᛖ · ᚱᛁᚾᚷ · ᛏᚠ · ᚱᚢᛚᛖ · ᚦᛖᛗ · ᚠᛚᛚ
ᚠᚾᛖ · ᚱᛁᚾᚷ · ᛏᚠ · ᛒᚱᛁᛝ · ᚦᛖᛗ · ᚠᛚᛚ · ᚠᚾᛞ
ᚠᚾᛖ · ᚱᛁᚾᚷ · ᛏᚠ · ᚠᛁᚾᛞ · ᚦᛖᛗ
ᛁᚾ · ᚦᛖ · ᛞᚨᚱᚴᚾᛖᛋᛋ · ᛒᛁᛞ · ᚦᛖᛗ

We can see a pattern arising, the first three lines all start with the same 9 symbols (ᚠᚾᛖ · ᚱᛁᚾᚷ · ᛏᚠ). Assuming that the dots denote word breaks I made an educated guess from my experience with the lord of the rings books and movies (as well as having a roommate in college write his thesis on the books) that this message came from the famous poem about the rings of power. The poem is about the rings in Tolkien's fantasy world with the most famous stanza at the end about the hobbit's ring, this starts "one ring to ..." and repeats "one ring to" three times throughout the stanza. From this we can decode the rest of the message either rune by rune or from the poem in question. It goes,

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

From here we can see that the second and third lines should be switched leaving us with the famously quoteable,

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

We can see now that rune correspond to sounds rather than letters, for example ᚦ corresponds to ”th”. The remaining runes correspond to individual letters like *textarao* correspond to ”o”. I was also assisted by the rune package I used ”allrunes” since often the letter used in the Latex code was very similar if not exactly the corresponding English equivalent. I found the information on writing runes in Latex code here: (`ftp://ftp.dante.de/tex-archive/fonts/allrunes/allrunes.pdf`).