Cryptography & Encryption:6G7Z1011: Lab Questions

Keith Yates

March 15, 2019

Cryptography & Encryption:6G7Z1011 : Elliptic Cryptography & Quantum Encryption

1 Cryptography & Encryption:6G7Z1011 : Elliptic Cryptography & Quantum Encryption

2 Problems & Supplementary Material:Elliptic Curves

2.1 problem:

⌜ Write a java method that finds the solutions of

$$ax^2 + bx + c = 0; \tag{1}$$

the method should take three arguments a, b and c. ⌟

2.2 problem:

⌜ Write a java method that finds the solutions of

$$ax^3 + bx^2 + cx + d = 0; \tag{2}$$

the method should take four arguments a, b, c and d. Hint
`https://en.wikipedia.org/wiki/Cubic_function#General_formula`.
⌟

2.3 problem:

⌜Find all the solutions to

$$y^2 = x^3 + 3x + 8 \mod \mathbb{F}_{13} \tag{3}$$

That is each (x, y) solution is an element of $\mathbb{F}_{13} \times \mathbb{F}_{13}$ and it satisfies eqn. 3, for example $(2, 3)$ is a solution. You should find eight answers, see §2.4 ⌟

2.4 problem:

⌜The eight solutions from §2.3 are shown in table 1, if we append an identity element 0 the nine elements can be given an abelian group structure. Formally you are creating

$$\text{Ellip}(y^2 = x^3 + 3x + 8, \mathbb{F}_{13}); \tag{4}$$

the abelian group associated with $y^2 = x^3 + 3x + 8$ and the field $\mathbb{F}_{13}$. Using the algorithm in the notes evaluate the group table.
⌟

	0	$(1,5)$	$(1,8)$	$(2,3)$	$(2,10)$	$(9,6)$	$(9,7)$	$(12,2)$	$(12,11)$
0									
$(1,5)$									
$(1,8)$									
$(2,3)$									
$(2,10)$									
$(9,6)$									
$(9,7)$									
$(12,2)$									
$(12,11)$									

Table 1: The points all lie on $y^2 = x^3 + 3x + 8$ over the field $\mathbb{F}_{13}$. Using the ideas of the lecture can you complete the table to create an abelian group of order 9?

$\times$	b	c	d	e	f	g	h	i
b								
c								
d								
e								
f								
g								
h								
i								

2.5 problem:$\mathbb{F}_{3^2}$

⌜Construct the field $\mathbb{F}_{3^2}$ The following matrices are a field of cardinality nine over $\mathbb{Z}(3)$

$$\begin{array}{lll} a = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, & b = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, & c = \begin{pmatrix} 0 & 2 \\ -2 & 0 \end{pmatrix}, \\ d = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, & e = \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}, & f = \begin{pmatrix} 1 & 2 \\ -2 & 1 \end{pmatrix}, \\ g = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}, & h = \begin{pmatrix} 2 & 1 \\ -1 & 2 \end{pmatrix}, & i = \begin{pmatrix} 2 & 2 \\ -2 & 2 \end{pmatrix}. \end{array} \tag{5}$$

⌟

2.6 problem:

⌜Continue with your assignment. ⌟