

Paper

Mock title for mock paper

Introduction

This is my mock paper to show the ease of working with pandoc [1]. This is a simple yet very powerful construct which allows you to combine markdown with L^AT_EX in one and the same file. Also shown in this file is how you can do references by specifying a .bib file in your YAML header. Some compact examples include:

(Don't forget that these are just some examples. I encourage you to read the documentation and try it yourself)

- item 1
- **References** look *like this*: [1], [2]

```
def compute(x):  
    return x**3 + 7 * x + 1
```

Let $E : y^2 = x^3 + 7x + 1$ be an elliptic curve over \mathbb{F}_{13} . Verifying that the point $(5, 3)$ is on the curve can be done as follows:

$$y^2 = x^3 + 7x + 1$$

$$5^2 = 3^3 + 7 \cdot 3 + 1$$

$$25 = 81 + 21 + 1$$

$$25 = 103$$

Adjusting for \mathbb{F}_{13}

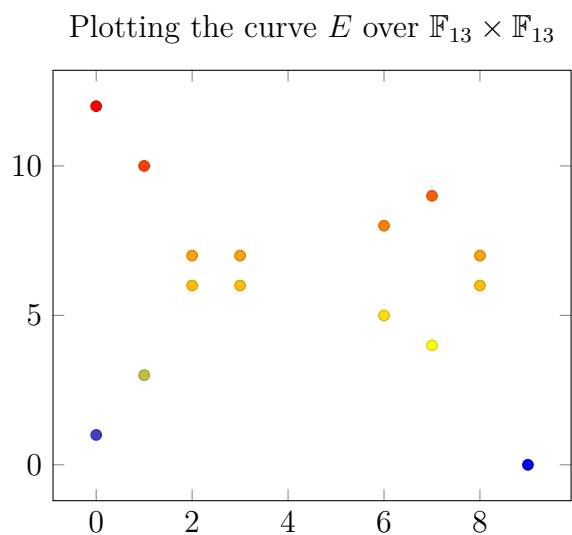
$$12 = 12$$

□

Creating a table to show *all* the points on the curve E :

x	x^2	$x^3 + 7x + 1$	y	points
0	0	1	1, 12	(0, 1), (0, 12)
1	1	9	3, 10	(1, 3), (1, 10)
2	4	10	6, 7	(2, 6), (2, 7)
3	9	10	6, 7	(3, 6), (3, 7)
4	3	2	-	-
5	12	5	-	-
6	10	12	5, 8	(6, 5), (6, 8)
7	10	3	4, 9	(7, 4), (7, 9)
8	12	10	6, 7	(8, 6), (8, 7)
9	3	0	0	(9, 0)
10	9	5	-	-
11	4	5	-	-
12	1	6	-	-

We can also plot this curve:



References

- [1] “The pandoc website.” <http://pandoc.org/>.
- [2] G. Bertoni, J. Daemen, M. Peeters, and G. Van Assche, “Keccak,” in *Advances in cryptology – eurocrypt 2013*, 2013, pp. 313–314.