**TESTING**

The Majority of the testing in my program was testing the return value’s of the important functions such as those who calculated the point of the parent elliptic group which is the first step to generate a keypair.

This consisted of using various reference websites to verify my programs results. The one that I used the most was an interactive graph created by Andrea Corbellini

<https://cdn.rawgit.com/andreacorbellini/ecc/920b29a/interactive/modk-mul.html>

This graph calculated the order of the elliptical group, the subgroup of a given point, scalar multiplication of a point and point addition. This tool helped me to realize when my values were correct. The problem arose when the values continued to get higher. The website is unable to deal with primes over 10000 and crashed when attempted. This created a problem as I was no longer able to verify my answer when is that of a high degree.

An example an output from my program I was able to check the parent group order by visiting the website

ECC ENCRYPTION KEY GENERATION

(1) Key Generation

(2) Remnants of Schoof

(3) Print Keys to File (only if ran keygen)

(4) Quit

1

Prime p = 13

a = 2

b = 3

Parent group order N = 18

Random subgroup order n = 3

Cofactor N / n = 6

Random point on curve: X = 3 Y = 6

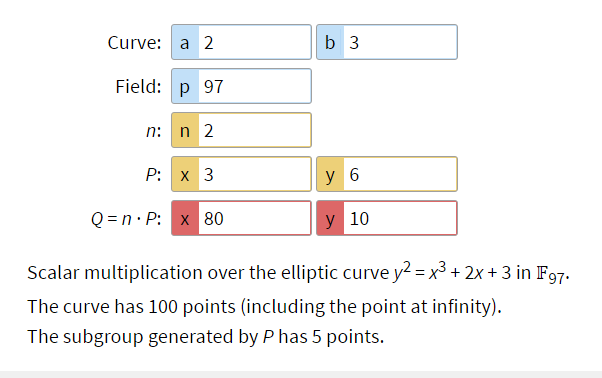
Private is d in which H = dG

Private Key = 2

Public Key is point H

X = 3

Y = 7



An answer that I discovered but was not able to utilise was CAS or computer algebra systems. There are some programs that have functions created specifically for checking the order of an elliptic curve of a large field. With this software it would have allowed me to continue verifying my answers as I tested the limits of the inputs. The reason why I was not able to use CAS was because I was unable to access one. Mathematica is a based off of a monthly subscription service.