MATH 178 Homework #13

Tamir Enkhjargal

May 2019

Elliptic Curve Cryptography

4.

$y^2 = x^3 - 4$ in $\mathbb{F}_2$

$0^2 = 0, \ 1^2 = 1$

x	$x^3 - 4$	$y \pm \sqrt{x^3 - 4}$
0	0	(0,0)
1	1	(1,1) (and 0)

$y^2 = x^3 - 4$ in $\mathbb{F}_3$

$0^2 = 0, \ 1^2 = 1, \ 2^2 = 1$

x	$x^3 - 4$	$y \pm \sqrt{x^3 - 4}$
0	2	-
1	0	(1,0)
2	1	(2,1), (2,2) (and 0)

$y^2 = x^3 - 4$ in $\mathbb{F}_5$

$0^2 = 0, \ 1^2 = 1, \ 2^2 = 4, \ 3^2 = 4, \ 4^2 = 1$

x	$x^3 - 4$	$y \pm \sqrt{x^3 - 4}$
0	1	(0,1), (0,4)
1	2	-
2	4	(2,2), (2,3)
3	3	-
4	1	(4,0) (and 0)

5.

```
e=[0,0,1,-1,0]
p=7
e=Mod(1,p)*e
q=[0,0]
ellpow(e,q,2)=[1,0]
ellpow(e,q,3)=[6,6]
ellpow(e,q,4)=[2,4]
ellpow(e,q,5)=[2,2]
ellpow(e,q,6)=[6,0]
ellpow(e,q,7)=[1,6]
ellpow(e,q,8)=[0,6]
ellpow(e,q,9)=[0]
```

Therefore $9q$ is the zero point.

6.

```
ee=[0,0,0,0,-4]
p=nextprime(10^25)
e=ee*Mod(1,p)
g=[2,2]
public = \r eckey.txt
ellpow(e,public,a)
```

The shared key was 5372475807523701402046910 $\equiv$ 4542 reduced mod 65536.
Using this as the key, and decrpyting the message:

```
‘tiara is a recursive acronym’
```

9.

```
f = t^16+t^6+t^2+t+1
E = [1,0,0,0,1]*Mod(Mod(1,2),f)
\r ECDHkey.txt
public = %4
private = 31415
ellpow(E,public,private)
t^14+t^13+t^12+t^9+t^6+t^2
```

Therefore, the shared key was 0111001001000100
Using this as the key, and decrpyting the message:

```
‘No dark sarcasm in the classroom’
```