10

Homework 9 Cryptography

Rick Staals
0716184

Erwin van Duijnhoven
0719562

November 27, 2013

Exercise 1

Prove that for (x_1, y_1) and (x_2, y_2) on the circle $x^2 + y^2 = 1$ also their sum $(x_1, y_1) + (x_2, y_2) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2)$ is on the circle.

4/4

Answer 1

Let $C = \{(x, y)|x^2+y^2 = 1\}$. With the sum of two elements $(x_1, y_1), (x_2, y_2) \in C$ defined as

$$(x_1, y_1) + (x_2, y_2) = (x_1y_2 + y_1x_2, y_1y_2 - x_1x_2),$$

w We need to prove that $(x_1y_2+y_1x_2, y_1y_2-x_1x_2) =: (\tilde{x}, \tilde{y}) \in C$. For this compute $\tilde{x}^2 + \tilde{y}^2$

$$\begin{aligned}
&\tilde{x}^2 + \tilde{y}^2 \\
&= (x_1y_2 + y_1x_2)^2 + (y_1y_2 - x_1x_2)^2 \\
&= x_1^2y_2^2 + y_1^2x_2^2 + y_1^2y_2^2 + x_1^2x_2^2 + 2x_1y_2y_1x_2 - 2y_1y_2x_1x_2 \\
&= x_1^2y_2^2 + y_1^2x_2^2 + y_1^2y_2^2 + x_1^2x_2^2 \\
&= x_1^2(y_2^2 + x_2^2) + y_1^2(y_2^2 + x_2^2) = (x_1^2+y_1^2)(x_2^2+y_2^2) \\
&= x_1^2 + y_1^2 = 1
\end{aligned}$$

Exercise 2

Find all points (x_1, y_1) on the Edwards curve $x^2 + y^2 = 1 - 5x^2y^2$ over $\mathbb{F}_{13}$. Verify that $P = (6, 3)$ and $Q = (3, 7)$ are on the curve. Compute $R = 2P + Q$.

6/6

Answer 2

Let $D = \{(x, y)|x^2 + y^2 = 1 - 5x^2y^2\}$ over $\mathbb{F}_{13}$ with the sum of two elements $(x_1, y_1), (x_2, y_2) \in D$ defined in class as

$$(x_1, y_1) + (x_2, y_2) = \left(\frac{x_1y_2 + y_1x_2}{1 - 5x_1y_1x_2y_2}, \frac{y_1y_2 - x_1x_2}{1 + 5x_1y_1x_2y_2}\right)$$

Since it is symmetric in two ways we know that for every element $(x, y) \in D$ also $(-x, y), (x, -y)$ & $(-x, -y) \in D$ and $(x, y) \in D \Leftrightarrow (y, x) \in D$

$x \backslash y$	0	1	2	3	4	5	6
0	0	**1**	4	9	3	12	10
1		7	12	3	6	8	9
2			10	11	2	9	6
3				7	4	2	**1**
4					12	0	7
5						3	11
6							0

Table 1: The results of $x^2 + y^2 + 5x^2y^2 \mod 13$

With the symmetric conditions we get the following elements to be points on the Edwards curve.

$$\{(0,1);(0,12);(1,0);(12,0);(3,6);(10,6);(3,7);(10,7);(6,3);(7,3);(6,10);(7,10)\}$$

Now with $P = (6,3)$ and $Q = (3,7)$ we want to compute $R = 2P + Q$ using the defined sum function.

$$2P + Q = P + P + Q$$

$$P + P = (6,3) + (6,3) = (\tfrac{36}{-1619}, \tfrac{12}{1621}) \equiv (\tfrac{10}{6}, \tfrac{12}{9}) \equiv (10 \cdot 11, 12 \cdot 3) \equiv (6,10) \mod 13$$

$$P + P + Q \equiv (6,10) + (3,7) \equiv (\tfrac{72}{-6299}, \tfrac{52}{6301}) \equiv (\tfrac{7}{6}, 0) \equiv (7 \cdot 11, 0) \equiv (12,0) \mod 13$$

Therefore $R = (12,0)$