Week 8: Elliptic Curve Cryptography

Jay Daigle

Occidental College

October 19, 2017

$\mathbb{F}_{13}$

$\mathbb{F}_{13}$

$$\begin{array}{cccccc} 1^2 \equiv 1 & 2^2 \equiv 4 & 3^3 \equiv 9 & 4^3 \equiv 3 & 5^2 \equiv 12 & 6^2 \equiv 10 \\ 7^2 \equiv 10 & 8^2 \equiv 12 & 9^2 \equiv 3 & 10^2 \equiv 9 & 11^2 \equiv 4 & 12^2 \equiv 1 \end{array}$$

$\mathbb{F}_{13}$

$$\begin{array}{cccccc} 1^2 \equiv 1 & 2^2 \equiv 4 & 3^3 \equiv 9 & 4^3 \equiv 3 & 5^2 \equiv 12 & 6^2 \equiv 10 \\ 7^2 \equiv 10 & 8^2 \equiv 12 & 9^2 \equiv 3 & 10^2 \equiv 9 & 11^2 \equiv 4 & 12^2 \equiv 1 \end{array}$$

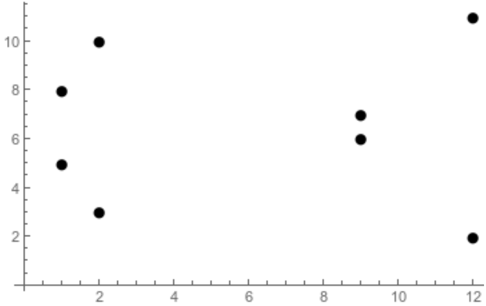
$$E : y^2 = x^3 + 3x + 8 \text{ over } \mathbb{F}_{13}$$

$\mathbb{F}_{13}$

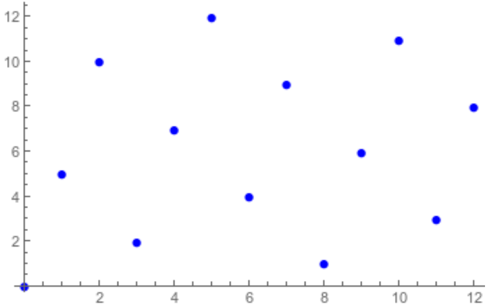
$$1^2 \equiv 1 \qquad 2^2 \equiv 4 \qquad 3^3 \equiv 9 \qquad 4^3 \equiv 3 \qquad 5^2 \equiv 12 \qquad 6^2 \equiv 10$$
$$7^2 \equiv 10 \qquad 8^2 \equiv 12 \qquad 9^2 \equiv 3 \qquad 10^2 \equiv 9 \qquad 11^2 \equiv 4 \qquad 12^2 \equiv 1$$

$$E : y^2 = x^3 + 3x + 8 \text{ over } \mathbb{F}_{13}$$

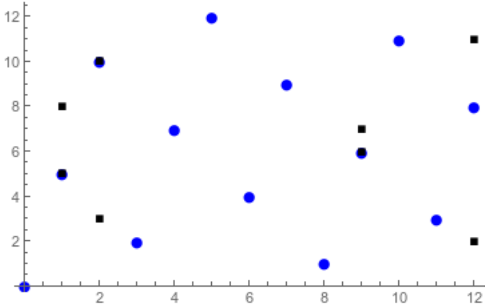
$$E(\mathbb{F}_{13}) = \{\mathcal{O}, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (12,11)\}.$$



$$E : y^2 = x^3 + 3x + 8 \text{ over } \mathbb{F}_{13}$$



The line $y = 5x$ over $\mathbb{F}_{13}$



$$y^2 = x^3 + 3x + 8 \text{ and } y = 5x$$

Proposition

Let $E : y^2 = x^3 + Ax + B$ *be an elliptic curve over* $\mathbb{Q}$*, and let* $P = (x_1, y_1)$ *and* $Q = (x_2, y_2)$ *be points on* $E(\mathbb{Q})$*. Then:*

Proposition

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$, and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on $E(\mathbb{Q})$. Then:

1. *If $y_1 \equiv -y_2 \mod p$ then $P \oplus Q = \mathcal{O}$.*

Proposition

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$, and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on $E(\mathbb{Q})$. Then:

1. *If $y_1 \equiv -y_2 \mod p$ then $P \oplus Q = \mathcal{O}$.*
2. *If $P_1 = P_2$, then define $\lambda = \frac{3x_1^2 + A}{2y_1}$. Set*

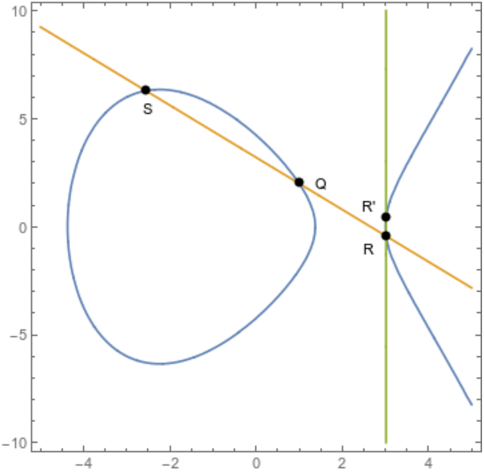
$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$

Then $P \oplus Q = (x_3, y_3)$.

Proposition

Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over $\mathbb{Q}$, and let $P = (x_1, y_1)$ and $Q = (x_2, y_2)$ be points on $E(\mathbb{Q})$. Then:

1. *If $y_1 \equiv -y_2 \mod p$ then $P \oplus Q = \mathcal{O}$.*
2. *If $P_1 = P_2$, then define $\lambda = \frac{3x_1^2+A}{2y_1}$. Set*
$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$
Then $P \oplus Q = (x_3, y_3)$.
3. *If $P_1 \neq P_2$, then define $\lambda = \frac{y_2-y_1}{x_2-x_1}$. Then as before, set*
$$x_3 = \lambda^2 - x_1 - x_2 \qquad y_3 = \lambda(x_1 - x_3) - y_1.$$
Then $P \oplus Q = (x_3, y_3)$.


10
5
0
−5
−10
−4
−2
0
2
4
S
Q
R'
R