W202 - Homework 5

Problem # 1a: On an elliptic curve, what is the negative of a point A?

Note: Consider the case where x and y vary over the real numbers.

Answer: The negative of a point A on an elliptic curve is the point's reflection over the x-axis and is defined as the point's inverse or point of infinity.

Problem 1b: What is zero on an elliptic curve, and why is it important from a group theory perspective?

Note: Consider the case where x and y vary over the real numbers.

Answer: zero is defined as the point of infinity on an elliptic curve, and it exists in order to satisfy the identity property of a group. More specifically, when projecting an elliptic curve across a plane, a group structure can be defined, which means the curve must adhere to properties of a group (ie associative, identity, inverse properties). The identity property states the existence of some identity element (E) in group such that some binary operation (such as addition) with some point (P) on curve, does not change (P). In mathematical notation: $P \oplus E = P$ or in elliptic curve notation: $P \oplus \mathcal{O} = P$.

Problem 2: When computing $A \oplus B = C$, we take the straight line through A and B and find the point it intersects the elliptic curve. We then reflect that point through the x-axis. If we don't do reflection, this breaks something about elliptic curve addition. What have we broken?

Answer: If we do not perform a reflection ove x-axis we break the ability to perform scalar multiplication, which is a form of elliptic curve addition (ie: $3P = P \oplus P \oplus P$). As elliptic curves are symmetric over the x-axis, the reflection allows elliptic curve arithmetic (ie addition, scalar multiplication) to be mathematically consistent. Without the reflection, elliptic curve addition would continuously add a tangent line to itself.

Problem 3: Prove that the only points on elliptic curve $y^2 \equiv x^3 + 4x + 3 \pmod 7$ are the following: $\{ \mathcal{O}, (1,1), (1,6), (3,0), (5,1), (5,6) \}$

① Find square roots (mod 7):

$\hookrightarrow 0^2 = 0 \pmod 7$
$\hookrightarrow 1^2 = 1 \pmod 7$
$\hookrightarrow 2^2 = 4 \pmod 7$
$\hookrightarrow 3^2 = 9 \equiv 2 \pmod 7$
$\hookrightarrow 4^2 = 16 \equiv 2 \pmod 7$
$\hookrightarrow 5^2 = 25 \equiv 4 \pmod 7$
$\hookrightarrow 6^2 = 36 \equiv 1 \pmod 7$

– square roots : $\{0, 1, 2, 4\} \pmod 7$

$\hookrightarrow \sqrt{0} = (0,0)$ point of infinity
$\hookrightarrow \sqrt{1} = (1,-1) = (1,6) \pmod 7$
$\hookrightarrow \sqrt{2} = (2,-2) = (2,5) \pmod 7$
$\hookrightarrow \sqrt{4} = (4,-4) = (4,3) \pmod 7$

② Confirm points on curve (mod 7):

$\underline{x=1}$

$$\begin{aligned} y^2 &\equiv (1)^3 + 4(1) + 3 \pmod 7 \\ &\equiv 1 + 4 + 3 \pmod 7 \\ &\equiv 8 \pmod 7 \\ &\equiv \underline{\underline{1}} \pmod 7 \end{aligned}$$

As $1 \pmod 7$ gives a valid square root of 1, and $\sqrt{1} \approx (1,-1) \approx (1,6) \pmod 7$, then points $\underline{\underline{(1,1)}}$ and $\underline{\underline{(1,6)}}$ exists on the curve

(next page)

$\underline{x = 2}$

$$
\begin{aligned}
y^2 &\equiv (2)^3 + 4(2) + 3 \pmod 7 \\
&\equiv 8 + 8 + 3 \pmod 7 \\
&\equiv 19 \pmod 7 \\
&\equiv \underline{\underline{5}} \pmod 7
\end{aligned}
$$

As there are no valid square roots for 5 mod 7, there are no valid points when $x = 2$

$\underline{x = 3}$

$$
\begin{aligned}
y^2 &\equiv (3)^3 + 4(3) + 3 \pmod 7 \\
&\equiv 27 + 12 + 3 \pmod 7 \\
&\equiv 42 \pmod 7 \\
&\equiv \underline{\underline{0}} \pmod 7
\end{aligned}
$$

As 0 (or $\mathcal{O}$) is always a point on every elliptic curve, the point $(\underline{\underline{3,0}})$ is valid point.

$\underline{\underline{x = 4}}$

$$
\begin{aligned}
y^2 &\equiv (4)^3 + 4(4) + 3 \pmod 7 \\
&\equiv 64 + 16 + 3 \pmod 7 \\
&\equiv 83 \pmod 7 \\
&\equiv \underline{\underline{3}} \pmod 7
\end{aligned}
$$

As there is no valid square root for 3 mod 7, there are no valid points when $x = 4$.

(next page)

$\underline{x = 5}$

$$
\begin{aligned}
y^2 &= (5)^3 + 4(5) + 3 \pmod 7 \\
&\equiv 125 + 20 + 3 \pmod 7 \\
&\equiv 148 \pmod 7 \\
&\equiv 1 \pmod 7
\end{aligned}
$$

As $1 \pmod 7$ gives a valid square root of 1, and $\sqrt{1} \approx (1, -1) \approx (1, 6) \pmod 7$, then points $(5, 1)$ and $(5, 6)$ exist on curve.

$\underline{x = 6}$

$$
\begin{aligned}
y^2 &= (6)^3 + 4(6) + 3 \pmod 7 \\
&\equiv 216 + 24 + 3 \pmod 7 \\
&\equiv 243 \pmod 7 \\
&\equiv \underline{5} \pmod 7
\end{aligned}
$$

As there is no valid square root for 5 mod 7, there are no valid points when $x = 6$.

Answer: By calculating the square roots of $\pmod 7$, and testing x values in range of the modulus, we confirmed the following points are only points that exist on elliptic curve of equation: $y^2 = x^3 + 4x + 3 \pmod 7$

$$\left(\mathcal{O} ; (1,1) ; (1,6) ; (3,0) ; (5,1) ; (5,6) \right)$$

Problem 4a: Which rule justifies the calculation?

$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}$; $\mathcal{O} \oplus (1,1) = (1,1)$; $\mathcal{O} \oplus (1,6) = (1,6)$

$\mathcal{O} \oplus (3,0) = (3,0)$; $\mathcal{O} \oplus (5,1) = (5,1)$; $\mathcal{O} \oplus (5,6) = (5,6)$

Answer:

$\mathcal{O} \oplus \mathcal{O} = \mathcal{O} \longrightarrow$ Rule 1 $(P \oplus \mathcal{O} = P)$

$\mathcal{O} \oplus (1,1) = (1,1) \longrightarrow$ Rule 1 $(P \oplus \mathcal{O} = P)$

$\mathcal{O} \oplus (1,6) = (1,6) \longrightarrow$ Rule 1 $(P \oplus \mathcal{O} = P)$

$\mathcal{O} \oplus (3,0) = (3,0) \longrightarrow$ Rule 1 $(P \oplus \mathcal{O} = P)$

$\mathcal{O} \oplus (5,1) = (5,1) \longrightarrow$ Rule 1 $(P \oplus \mathcal{O} = P)$

$\mathcal{O} \oplus (5,6) = (5,6) \longrightarrow$ Rule 1 $(P \oplus \mathcal{O} = P)$

Problem 4b: Which rule justifies the calculation?

$(1,1) \oplus (1,6) = \mathcal{O}$; $(3,0) \oplus (3,0) = \mathcal{O}$

$(5,1) \oplus (5,6) = \mathcal{O}$

Answer:

$(1,1) \oplus (1,6) = \mathcal{O} \approx (1,1) \oplus (1,-1) \pmod 7 \longrightarrow$ Rule 2

$(3,0) \oplus (3,0) = \mathcal{O} \approx$ Rule 2

$(5,1) \oplus (5,6) = \mathcal{O} \approx (5,1) \oplus (5,-1) \pmod 7 \longrightarrow$ Rule 2

Problem 5a: Show $(1,1) \oplus (1,1) = (5,6)$

Solution:

① Equation: $y^2 \equiv x^3 + 4x + 3 \pmod 7$

where $A = 4$; $B = 3$

$X_1 = 1$; $Y_1 = 1$; $X_2 = 1$; $Y_2 = 1$

② Calculate λ using equation: $\lambda = \dfrac{3x_1^2 + A}{2y_1}$:
(where $P = Q$)

$\hookrightarrow \lambda = \dfrac{3(1)^2 + 4}{2(1)}$

$\lambda = \dfrac{3(1) + 4}{2}$

$\lambda = \dfrac{7}{2} \approx 7 \cdot 2^{-1} \pmod 7$

$\lambda = 7 \cdot 4 = 28 \pmod 7$

$\lambda = \underline{\underline{0}}$

Extended Euclidean Algorithm

$2X + 7y = 1$

$7 = 2(3) + 1$

$2 = 1(2) + 0$

$1 = 7(1) + 2\underline{\underline{(-3)}}$

$-3 \bmod 7 \approx \underline{\underline{4}}$

③ Calculate X_3 using equation $X_3 = \lambda^2 - X_1 - X_2$:

$\hookrightarrow X_3 = (0)^2 - 1 - 1$

$X_3 = 0 - 1 - 1$ → (used calculator)

$\underline{\underline{X_3}} = -2 \pmod 7 \approx \underline{\underline{5}}$

④ Calculate Y_3 using equation $Y_3 = \lambda(X_1 - X_3) - Y_1$:

$\hookrightarrow Y_3 = 0(1-5) - 1$

$Y_3 = 0(-4) - 1$ → (used calculator)

$Y_3 = 0 - 1$

$\underline{Y_3} = -1 \bmod 7 \approx \underline{6}$

$\boxed{\text{Answer: we showed } (1,1) \oplus (1,1) = (X_3, Y_3) = (5,6)}$

Problem 5b: show $(5,1) \oplus (5,1) = (5,6)$

Solution:

① Equation : $y^2 \equiv x^3 + 4x + 3 \pmod 7$

where $A = 4$; $B = 3$

$X_1 = 5$; $Y_1 = 1$; $X_2 = 5$; $Y_2 = 1$

② Calculate λ using equation : $\lambda = \dfrac{3x_1^2 + A}{2y_1}$:

(where $P = Q$)

↳ $\lambda = \dfrac{3(5)^2 + 4}{2(1)}$

$\lambda = \dfrac{3(25) + 4}{2}$

$\lambda = \dfrac{75 + 4}{2}$

$\lambda = \dfrac{79}{2} \approx 79 \cdot 2^{-1} \pmod 7$

$\lambda = 79 \cdot 4 = 316 \pmod 7$

$\lambda = \underline{1}$

Extended Euclidean Algorithm

$2x + 7y = 1$

$7 = 2(3) + 1$

$2 = 1(2) + 0$

$1 = 7(1) + 2(\underline{\underline{-3}})$

$-3 \bmod 7 \approx \underline{\underline{4}}$

③ Calculate X_3 using equation $X_3 = \lambda^2 - X_1 - X_2$:

↳ $X_3 = (1)^2 - 5 - 5$

$X_3 = 1 - 5 - 5$ → (used calculator)

$\underline{\underline{X_3}} = -9 \pmod 7 = \underline{\underline{5}}$

④ Calculate Y_3 using equation $Y_3 = \lambda(X_1 - X_3) - Y_1$:

↳ $Y_3 = 1(5-5) - 1$

$Y_3 = 1(0) - 1$ → (used calculator)

$\underline{\underline{Y_3}} = -1 \pmod 7 = \underline{\underline{6}}$

$\boxed{\text{Answer: We showed } (5,1) \oplus (5,1) = (X_3, Y_3) = (5,6)}$

Problem 5c: Show $(1,1) \oplus (3,0) = (5,1)$

Solution:

① Equation: $y^2 \equiv x^3 + 4x + 3 \pmod 7$

where $A = 4$; $B = 3$

$X_1 = 1$; $Y_1 = 1$; $X_2 = 3$; $Y_2 = 0$

② Calculate λ using equation: $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$

(as $P \neq Q$)

↳ $\lambda = \dfrac{0-1}{3-1}$

$\lambda = \dfrac{-1}{2} \approx -1 \cdot 2^{-1} \pmod 7$

$\lambda = -1 \cdot 4 \approx -4 \pmod 7$

$\lambda = \underline{\underline{3}}$

Extended Euclidean Algorithm

$2x + 7y = 1$

$7 = 2(3) + 1$

$2 = 1(2) + 0$

$1 = 7(1) + 2(\underline{\underline{-3}})$

$-3 \bmod 7 \approx \underline{4}$

③ Calculate X_3 using equation $X_3 = \lambda^2 - X_1 - X_2$:

↳ $X_3 = (3)^2 - 1 - 3$

$X_3 = 9 - 1 - 3$ → (used calculator)

$\underline{\underline{X_3}} = 5 \pmod 7 \approx \underline{\underline{5}}$

④ Calculate Y_3 using equation $Y_3 = \lambda(X_1 - X_3) - Y_3$:

↳ $Y_3 = 3(1-5) - 1$

$Y_3 = 3(-4) - 1$ → (used calculator)

$Y_3 = -12 - 1$

$\underline{\underline{Y_3}} = -13 \pmod 7 \approx \underline{\underline{1}}$

$\boxed{\text{Answer: We showed } (1,1) \oplus (3,0) = (X_3, Y_3) = (5,1)}$

Problem 5d : Show $(1,1) \oplus (5,6) = (3,0)$

Solution :

① Equation : $y^2 \equiv x^3 + 4x + 3 \pmod 7$

where $A = 4$; $B = 3$

$X_1 = 1$; $Y_1 = 1$; $X_2 = 5$; $Y_2 = 6$

② Calculate λ using equation : $\lambda = \frac{y_2 - y_1}{X_2 - X_1}$:

(as $P \neq Q$)

$\hookrightarrow \lambda = \frac{6-1}{5-1}$

$\lambda = \frac{5}{4} \cong 5 \cdot 4^{-1} \pmod 7$

$\lambda = 5 \cdot 2 \pmod 7$

$\lambda = 10 \pmod 7$

$\lambda = \underline{\underline{3}}$

Extended Euclidean Algorithm

$4x + 7y = 1$

$7 = 4(1) + 3$

$4 = 3(1) + 1$

$1 = 4 + 3(-1)$

$1 = 4 + (7 + 4(-1))(-1)$

$1 = 4 + 7(-1) + 4(1)$

$1 = 4(\underline{\underline{2}}) + 7(-1)$

③ Calculate X_3 using equation $X_3 = \lambda^2 - X_1 - X_2$:

$\hookrightarrow X_3 = (3)^2 - 1 - 5$

$X_3 = 9 - 1 - 5$ → (used calculator)

$\underline{\underline{X_3}} = 3 \pmod 7 \cong \underline{\underline{3}}$

④ Calculate Y_3 using equation $Y_3 = \lambda(X_1 - X_3) - Y_1$:

$\hookrightarrow Y_3 = 3(1-3) - 1$

$Y_3 = 3(-2) - 1$ → (used calculator)

$Y_3 = -6 - 1$

$\underline{\underline{Y_3}} = -7 \pmod 7 \cong \underline{\underline{0}}$

$\boxed{\text{Answer : We showed } (1,1) \oplus (5,6) = (X_3, Y_3) = (3,0)}$

Problem 5e : show $(1,6) \oplus (5,1) = (3,0)$

Solution :

① Equation : $y^2 = x^3 + 4x + 3 \pmod 7$

where $A = 4$; $B = 3$

$X_1 = 1$; $Y_1 = 6$; $X_2 = 5$; $Y_2 = 1$

② Calculate λ using equation $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$:
(where $P \neq Q$)

↳ $\lambda = \dfrac{1-6}{5-1}$

$\lambda = \dfrac{-5}{4} \approx -5 \cdot 4^{-1} \pmod 7$

$\lambda = -5 \cdot 2 \pmod 7$

$\lambda = -10 \pmod 7$

$\lambda = \underline{\underline{4}}$

Extended Euclidean Algorithm

$4x + 7y = 1$

$7 = 4(1) + 3$

$4 = 3(1) + 1$

$1 = 4 + 3(-1)$

$1 = 4 + (7 + 4(-1))(-1)$

$1 = 4 + 7(-1) + 4(1)$

$1 = 4(\underline{2}) + 7(-1)$

$= 2 \bmod 7$

③ Calculate X_3 using $X_3 = \lambda^2 - X_1 - X_2$:

↳ $X_3 = (4)^2 - 1 - 5$

$X_3 = 16 - 1 - 5$ → (used calculator)

$\underline{\underline{X_3}} = 10 \pmod 7 \approx \underline{\underline{3}}$

④ Calculate Y_3 using equation $Y_3 = \lambda(x_1 - x_3) - Y_1$:

↳ $Y_3 = 4(1-3) - 6$

$Y_3 = 4(-2) - 6$ → (used calculator)

$Y_3 = -8 - 6$

$\underline{\underline{Y_3}} = -14 \pmod 7 \approx \underline{\underline{0}}$

$\boxed{\text{Answer : We showed } (1,6) \oplus (5,1) = (X_3, Y_3) = (3,0)}$

References

Student Discussions

- Nick Keith
- Jyotsna Sharma
- Aaron Crouch
- Matthew Holmes

Office hours / Slack

Tools and Resources

- Hoffstein textbook
- Stallings textbook
- Async video (module 5)
- Google searches
- Youtube
- Wikipedia
- Stack Exchange
- Standford crytography
- Calculator