Elliptic Curves

Reel-Valued

general : \( y^2 + axy + by = x^3 + cx^2 + dx + e \)

Simplify : \( y^2 = x^3 + ax + b \quad 4a^3 + 27b^2 \neq 0 \).

Define addition over pts on curve

1. Point O, call additive identity.
   For all point \( P \), \( P + O = P \), \( O = -O \).

2. \( -P \) is going to have the same \( x \)-coordinate as \( P \).

3. \( P + Q = \text{draw line between } P \text{ and } Q \text{ and call the point of intersection } R \) (w/ curve), then \( P + Q = -R \).

4. \( P + P \) use tangent line.

5. Multiplication is repeated addition.
   \( kP = \overbrace{P + P + P + \cdots + P}^{k \text{ times}} \)

Change Discrete \( \Rightarrow y^2 = x^3 + ax + b \mod p \)

Valid pts have \( x, y \in [0, p - 1] \) \( x, y \in \mathbb{Z} \)
These curves addition op form an Abelian Group. (Abel)

(A1) Closure if \( a, b \in G \) \( a \cdot b \in G \)

(A2) Associate \( a \cdot (b \cdot c) = (a \cdot b) \cdot c \)

Identity \( I \in G \) s.t. \( a \cdot I = a \) for all a.

(A4) Inverse For each \( a \in G \) there exists \( a' \) such that \( a \cdot a' = I \)

(AS) Commutative \( a \cdot b = b \cdot a \)

\[ P = (x_P, y_P) \]
\[ Q = (x_Q, y_Q) \]

How to do \( P + Q \)

Calculate \( \lambda \) :

\[ \lambda = \left\{ \begin{array}{ll} \frac{y_Q - y_P}{x_Q - x_P} \mod p & \text{if } P \neq Q \\\n\left( \frac{3x_P^2 + a}{2y_P} \right) \mod p & \text{if } P = Q. \end{array} \right. \]

\[ p = x^3 + ax + b \]
\[ 2y = 3x^2 + a \]
\[ y' = \frac{3x^2 + a}{2y} \]

Let's use the curve \( E_{23}(1,1) \)

\[ y^2 = x^3 + x + 1 \mod 23 \]

\[ E_{29}(2,4) \]

\[ y^2 = x^3 + 2x + 4 \mod 29 \]
\( p = (3, 10) \quad q = (9, 7) \)

\[ x_R = (\lambda^2 - x_p - x_Q) \mod p \]
\[ y_R = (\lambda(x_p - x_R) - y_p) \mod p \]

\[ \lambda = \frac{y_Q - y_p}{x_Q - x_p} = \frac{7 - 10}{9 - 3} = \frac{7}{6} \]

\[ 6^{-1} \mod 23 = 4 \]

\[ \frac{-3}{6} = -3 (4) = -12 = 11 \mod 23 \]

\[ x_R = (\lambda^2 - x_p - x_Q) = 11(2 - 3 - 9) \]
\[ = 121 - 12 \]
\[ = 109 \mod 23 \]
\[ = 17 \]

\[ y_R = (\lambda(x_p - x_R) - y_p) \]
\[ = 11(3 - 17) - 10 \]
\[ = -154 - 10 \]
\[ = -164 \]
\[ = 20 \mod 23 \]

11/13/19