# 11 - Krzywe Eliptyczne

Wednesday, 19 June 2024 15:17

Krzywa eliptyczna (postać Weierstrassa)

$y^2 = x^3 + ax + b$ nad pewnym ciałem $\mathbb{F}$

- Symetryczne względem OX.

Dodawanie:

P+Q: trzecie przecięcie krzywej przez prostą PQ - i odbicie przez OX.

P+-P=0 - punkt w nieskończoności

P+P: styczna do krzywej.

Zastosowania

Diffie-Hellman / El-Gamal działają na krzywych eliptycznych.

Nie ma na nich aż tak wielu heurystyk.