Formelsammlung MP4-IT4

Differenzenquotient: $\Delta y/\Delta x = \frac{y_Q - y_P}{x_Q - x_P}$

Ableitung (Steigungsfunktion) einer quadratischen Funktion:

$y = ax^2 + bx + c \rightarrow y' = 2ax + b$

Beispiel: $y = 3x^2 - 4x + 13 \rightarrow y' = 6x - 4$

Punkte auf der Secp256k1 (Bitcoin):

$y^2 = x^3 + 7$

Geg. $x \rightarrow y = \pm\sqrt{x^3 + 7}$ zwei Lösungen!

Geg. $y \rightarrow x = \sqrt[3]{y^2 - 7} = (y^2 - 7)^{1/3}$

Punkte addieren:

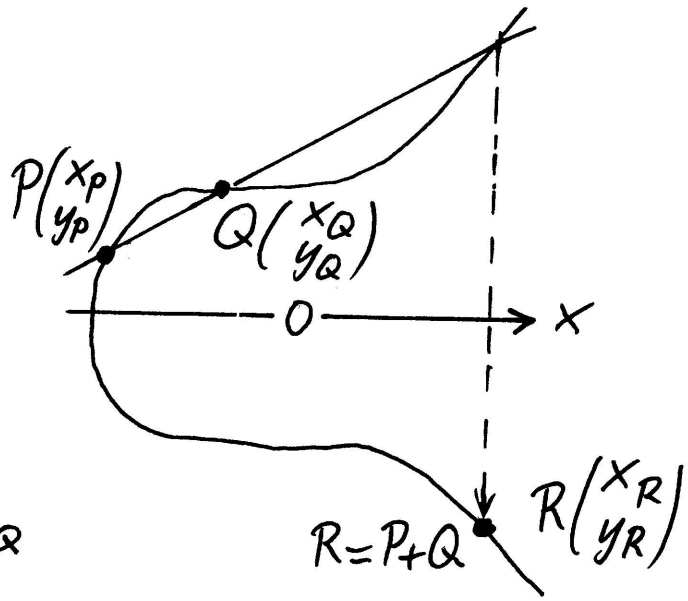
$m = \frac{y_Q - y_P}{x_Q - x_P}$

$x_R = m^2 - x_P - x_Q$

$y_R = m(x_P - x_R) - y_P$

oder

$y_R = m(x_Q - x_R) - y_Q$



Skalare Multiplikation von Punkten: (Nur Verdoppelung, d.h. P+P)

$m = \frac{3x_P^2}{2y_P}$

$x_R = m^2 - 2x_P$

$y_R = m(x_P - x_R) - y_P$