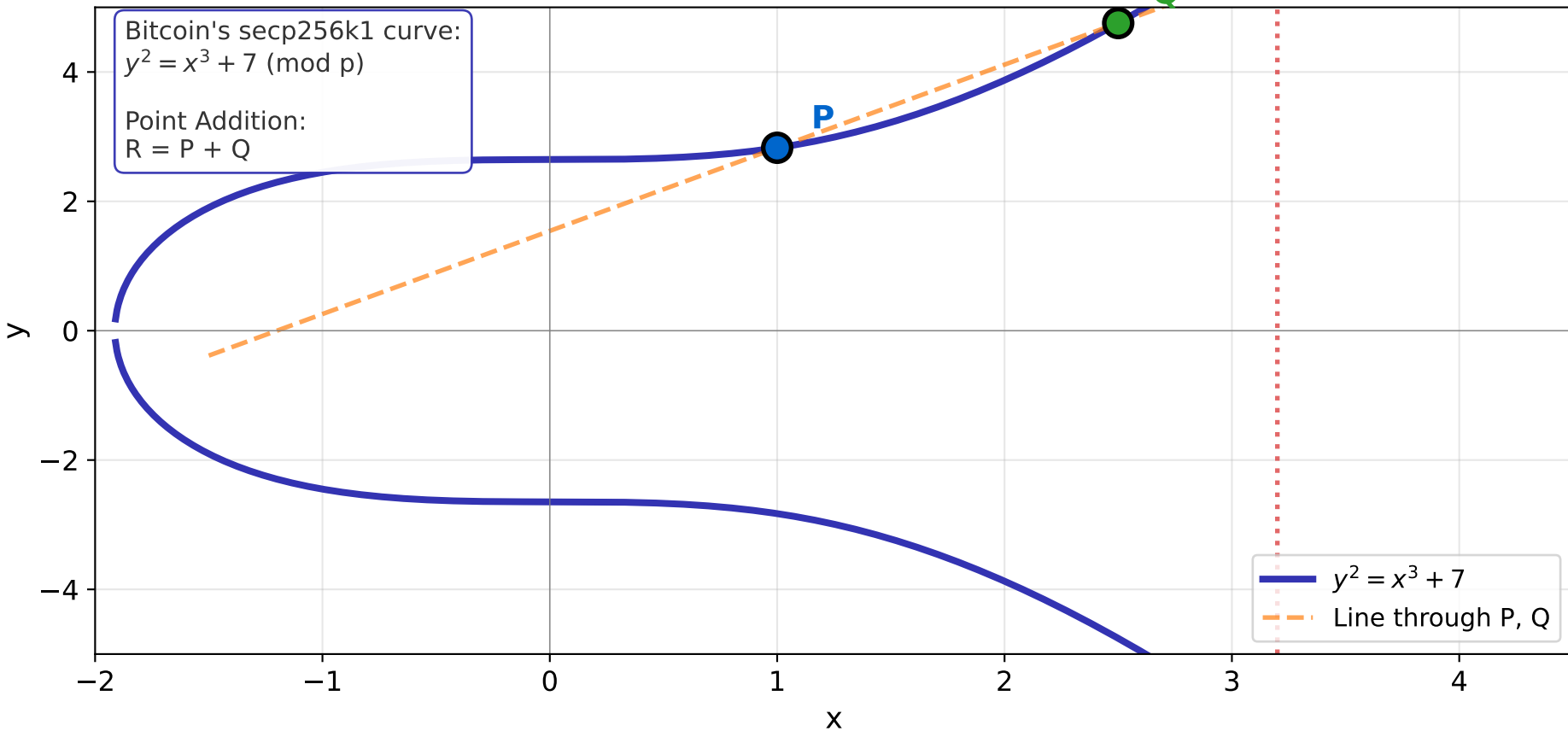


# Elliptic Curve Cryptography: Point Addition

Bitcoin's secp256k1 curve:  
 $y^2 = x^3 + 7 \pmod{p}$

Point Addition:  
 $R = P + Q$



$R = P + Q$