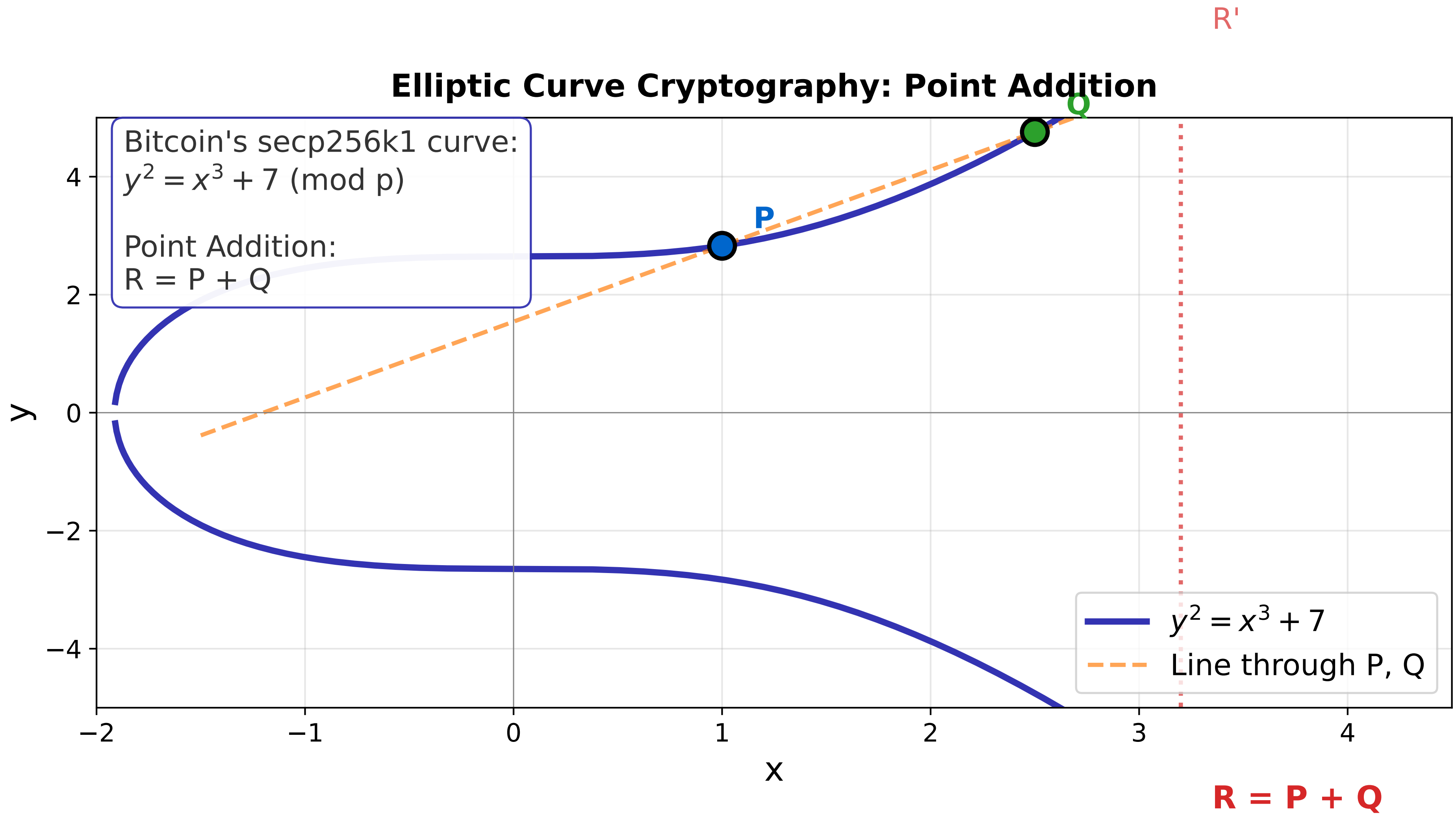
R'
Elliptic Curve Cryptography: Point Addition
Bitcoin's secp256k1 curve:
$y^2 = x^3 + 7$ (mod p)
Point Addition:
R = P + Q
P
Q
4
2
0
−2
−4
y
−2
−1
0
1
2
3
4
x
$y^2 = x^3 + 7$
Line through P, Q
R = P + Q