add (P, Q)

both are in projective coordinates

zero at infinity

- if P == O
  return Q
- if Q == O
  return P

$S_1 = \dots$
$S_2 = \dots$
$U_1 = \dots$
$U_2 = \dots$

- if $((S_1 == S_2) \&\& (U_1 == U_2))$
  return double (P)

$W = \dots$
$P = \dots$
$R = \dots$
$Z_3 = \dots$
$X_3 = \dots$
$Y_3 = [\dots]$ ← at first calculate the content of the brackets only

- if (Y_3 is odd) ← the prime number determining the field.
  $Y_3 := Y_3 + p$;
- shift Y_3 to the right by one bit
  $Y_3 := Y_3 / 2$
- return (X_3, Y_3, Z_3)

double (P)

- if (P == O)
  return P. (mod p)
- if (P.Y == 0) return O.

zero at infinity (0, 1, 0)

P.Y ← the Y coordinate of point P

$S = 2 \cdot P.Y \cdot P.Z \pmod p$

$B = \dots$
$W = \dots$
$h = \dots$
$X_3 = \dots$
$Y_3 = \dots$
$Z_3 = \dots$
- return (X_3, Y_3, Z_3)

tests:
$2P + 3P$
$= 2(2P) + P$