

問 2.5

(1) 加算

乗算: 2回, 2乗算: 1回, 逆元: 1回, 法演算: 3回

2倍算

乗算: 2回, 2乗算: 2回, 逆元: 1回, 法演算: 4回

(2) 加算: 7個

2倍算: 6個

(3)  $A = (x_1, y_1)$ ,  $B = (x_2, y_2)$  ( $A \neq B$ ) に対し,  $A+B$  を計算する.

加算

$$\begin{cases} \lambda = (y_2 - y_1) / (x_2 - x_1) \\ x_3 = \lambda^2 - x_1 - x_2 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$

$A = (x_1, y_1)$  に対し,  $2A$  を計算する.

2倍算

$$\begin{cases} \lambda = (3x_1^2 + a) / (2y_1) \\ x_3 = \lambda^2 - 2x_1 \\ y_3 = \lambda(x_1 - x_3) - y_1 \end{cases}$$