Question 3

First, the result of the multiplication in the quotient ring is as follows:

$$(a_1 + a_2x)(b_1 + b_2x) \equiv (a_1b_1 + a_2b_2\zeta) + (a_1b_2 + a_2b_1)x \mod x^2 - \zeta \tag{1}$$

Using schoolbook multiplication, the R.H.S. from above requires 5 multiplication. Using Karatsuba we can compute $a_1b_2 + a_2b_1$ using only one multiplication (but at the expense at more addition/subtraction):

$$a_1b_2 + a_2b_1 = (a_1 + a_2)(b_1 + b_2) - a_1b_1 - a_2b_2 \tag{2}$$

The R.H.S. of equation (2) only takes one multiplication because a_1b_1 and a_2b_2 have already been computed from previous steps of schoolbook multiplication.

Putting everything together:

Algorithm 1 Karatsuba-ish monomial multiplication

Start with $a_1 + a_2x$ and $b_1 + b_2x$
$c_1 \leftarrow a_1b_1$ ▷ first multiplication
$c_3 \leftarrow a_2b_2$ ▷ second multiplication
$c_2 \leftarrow (a_1 + a_2)(b_1 + b_2) - c_1 - c_3$ ▷ third multiplication
$c_3 \leftarrow c_3\zeta$ ▷ fourth multiplication
return $(c_1 + c_3) + c_2x$