Question 4

(a)

By the definition of the (quotient) ring $R_q = \mathbb{Z}_q[x]/\langle p(x) \rangle$ we know that:

$$a(x)s(x) + e(x) = p(x)g(x) + b(x) \tag{1}$$

Where $g(x)$ is some polynomial in $\mathbb{Z}_q[x]$.

Where ω is a root of $p(x)$, evaluating equation (1) at $x = \omega$ is as follows:

$$a(\omega)s(\omega) + e(\omega) = 0 \cdot g(\omega) + b(\omega) = b(\omega)$$

■

(b)

From equation (1) we know that $a(\omega)s(\omega) + e(\omega) = b(\omega)$ if and only if $p(\omega)g(\omega) = 0$. Where ω is not a root of $p(x)$, the equality holds if and only if $g(\omega) = 0$.

Because $a(x), s(x), e(x) \in R_q$ are all polynomials of degree (up to) $d - 1$, and $p(x)$ is a polynomial of degree d, the degree of $g(x)$ cannot be more than $2 \cdot (d - 1) - d = d - 2$. By the fundamental theorem of algebra we know that $g(x)$ cannot have more than $d - 2$ roots in $\mathbb{Z}_q$. Therefore, if $q > d - 2$, then there exists $\omega \in \mathbb{Z}_q$ such that ω is not a root of $g(x)$, which means that $b(\omega) \neq a(\omega)s(\omega) + e(\omega)$.

On the other hand, if the sum of degrees of $a(x)$ and $s(x)$ is less than the degree of $p(x)$, then $g(x) = 0$ (aka $b(x)$ does not need to be reduced modulus $p(x)$).