Q8

Recall that the decryption is computed with the following routine:

$$\begin{aligned} D(\mathrm{sk}, (\mathbf{c}_1, c_2)) &= c_2 - \mathbf{c}_1 \cdot \mathbf{s} \\ &= (\mathbf{s}'^{\intercal}\mathbf{e} - \mathbf{e}'^{\intercal}\mathbf{s}) + e'' + m\lfloor\frac{q}{2}\rceil \end{aligned}$$

Where $\mathbf{s}, \mathbf{s}'$ are coordinate-wise drawn from the secret distribution and $\mathbf{e}, \mathbf{e}', e''$ are coordinate-wise drawn from the error distribution.

According to the decryption routine, a decryption error occurs if and only if the "noise" $(\mathbf{s}'^{\intercal}\mathbf{e} - \mathbf{e}'^{\intercal}\mathbf{s}) + e''$ exceeds $\lfloor\frac{q}{4}\rceil$. So to find a modulus that guarantees correct decryption all the time, we need to find the upper bound of noise.

With (baby) Kyber-512, $\chi_s = \mathcal{B}(n = 6, p = 0.5), \chi_e = \mathcal{B}(n = 4, p = 0.5)$. Noise is maximized when all entries of $\mathbf{s}, \mathbf{e}$ reach the extremes of the support of their respective distributions. For example, with $\mathbf{s} = \mathbf{s}' = (3, 3, \ldots, 3)$, $\mathbf{e} = (2, 2, \ldots, 2)$, $\mathbf{e}' = (-2, -2, \ldots, -2)$, $e'' = 2$, the noise term evaluates to $(6 \cdot 512 + 6 \cdot 512) + 2 = 6146$. The smallest prime q such that $\lfloor\frac{q}{4}\rceil \geq 6146$ is 24593.

P.S. the smallest odd q such that $\lfloor\frac{q}{4}\rceil \geq 6146$ is 24583

P.S. the smallest integer q such that $\lfloor\frac{q}{4}\rceil \geq 6146$ is 24582