Question 5

(i) If $n = p$, then $n + \sigma(n) = p + (p+1) = 2p + 1$ is divisible by 3. Now $2p + 1 \equiv 0 \pmod 3$ has solution $p \equiv 1 \pmod 3$. In terms of modulo 6, that is $p \equiv 1$ or $4 \pmod 6$, but as numbers congruent modulo 6 to 4 are not prime, $p \equiv 1 \pmod 6$.

(ii) If $n = p^2$, then $n + \sigma(n) = p^2 + p^2 + p + 1 = 2p^2 + p + 1$. This is not divisible by 3 when $p = 2$ or 3. When $p > 3$, $p^2 \equiv 1 \pmod 3$ and so $2p^2 + p + 1 \equiv p \pmod 3$ and once again this is not divisible by 3. Hence $n \neq p^2$.

(iii) If $n = 2^k$, for $k > 0$, then $n + \sigma(n) = 2^k + (2^{k+1} - 1) = 3 \times 2^k - 1$. This is not divisible by 3, and so $n \neq 2^k$.

(iv) If $n = 2p^k$ then $n + \sigma(n) = 2p^k + \sigma(2p^k) = 2p^k + \sigma(2)\sigma(p^k) = 2p^k + 3\sigma(p^k)$. As the second term is a multiple of 3, this is divisible by 3 when $2p^k$ is divisible by 3. But the only primes dividing $2p^k$ are 2 and p, so we must have $p = 3$.

Question 6

(i) The discriminant is $4^2 - 4 \times 6 = -8$, and so the congruence has solutions if the Legendre symbol $(-8/23) = 1$. Now

$$\begin{aligned}(-8/23) &= (-1/23)(2/23)(4/23), && \text{by the multiplication property,}\\ &= (-1)(1)(1) = -1, && \text{since } 23 \equiv 3 \pmod 4,\ 23 \equiv 7 \pmod 8\\ & && \text{and 4 is a square.}\end{aligned}$$

So the congruence does not have a solution.

(ii)
$$\begin{aligned}(102/67) &= (35/67)\\ &= (5/67)(7/67) && \text{by the multiplication property}\\ &= (67/5)(-1)(67/7) && \text{by LQR, as } 5 \equiv 1 \pmod 4 \text{ and } 7 \equiv 67 \equiv 3 \pmod 4\\ &= (2/5)(-1)(4/67)\\ &= (-1)(-1)(1) && \text{as 4 is a square}\\ &= 1\end{aligned}$$

(iii) According to Gauss' Lemma, $(2/p) = (-1)^n$, where n is the number of integers in $S = \{2, 4, 6, \ldots, p-1\}$ which exceed $\frac{p}{2}$.

Now when $p = 8k + 7$,

$$S = \{2, 4, 6, \ldots, 4k+2, 4k+4, \ldots, 8k+6\},$$

and n is the number of these in $\{4k+4, 4k+6, \ldots, 8k+6\}$. Halving each term in the set, we see that n is the number of integers in $\{2k+2, 2k+3, 2k+4, \ldots, 4k+3\}$, namely

$$(4k+3) - (2k+2) + 1 = 2k + 2.$$

So n is even and $(2/p) = 1$, confirming that 2 is a quadratic residue of p.