

Q1)

The verification procedure works by the following argument. Assume that the signature is valid.

As  $s \equiv k^{-1}(m - zr) \pmod{p - 1}$ , we have  $sk \equiv (m - zr) \pmod{p - 1}$  and hence  $m \equiv sk + zr \pmod{p - 1}$ . Therefore by Fermat's little theorem, that a congruence mod  $p - 1$  in the exponent yields a congruence mod  $p$  overall, we have:

$$v_2 \equiv a^m \equiv a^{sk+zr} \equiv a^{sk} \times a^{zr} \equiv \beta^{rs} \equiv v_1 \pmod{p}$$

Q2)