2. *Verification.* To verify A's signature (r, s) on m, B should do the following:
   (a) Obtain A's authentic public key (p, q, α, y).
   (b) Verify that $0 < r < q$ and $0 < s < q$; if not, then reject the signature.
   (c) Compute $w = s^{-1} \bmod q$ and $h(m)$.
   (d) Compute $u_1 = w \cdot h(m) \bmod q$ and $u_2 = rw \bmod q$.
   (e) Compute $v = (\alpha^{u_1} y^{u_2} \bmod p) \bmod q$.
   (f) Accept the signature if and only if $v = r$.