Prob 43

$$x \stackrel{?}{=} \frac{sk - H(m)}{r} \bmod q$$

$$= r^{-1}(sk - H(m)) \bmod q = (r^{-1} \bmod q)\left[(sk - H(m)) \bmod q\right] \bmod q$$

$$= (r^{-1} \bmod q)\left[\{sk \bmod q - H(m) \bmod q\} \bmod q\right] \bmod q$$

$$s = k^{-1}(H(m) + xr) \bmod q$$

$$sk \bmod q = \left[k^{-1}(H(m) + xr) \bmod q\right] \underset{k \bmod q}{k} \bmod q$$

$$= k^{-1}(H(m) + xr)k \bmod q = (k^{-1}k \bmod q)\left[(H(m) + xr) \bmod q\right] \bmod q$$

$$x \stackrel{?}{=} (r^{-1} \bmod q)\left[\{(H(m) + xr) \bmod q - H(m) \bmod q\} \bmod q\right] \bmod q$$

$$= (r^{-1} \bmod q)\left[\{H(m) + xr - H(m)\} \bmod q\right] \bmod q$$

$$= r^{-1}xr \bmod q = \left[(r^{-1}r \bmod q)\underbrace{(x \bmod q)}_{x}\right] \bmod q \stackrel{\checkmark}{=} x$$