Math 440 - Advanced Topics in Algebra: Cryptology

The Digital Signature Algorithm, known as DSA, is a United States government standard for digital signatures. The public key is consists of a prime, p, a prime q such that $q|(p-1)$, a number g such that $g^q \equiv 1 \pmod{p}$ and $y = g^x \pmod{p}$ where x is the secret key.

A signature on a message, M, is produced as follows:

Signature Algorithm

1. Generate a random number k in the range $0 < k < q$.
2. Compute $r = g^k \pmod{p} \pmod{q}$ (i.e. first mod by p, then mod that result by q)
3. Calculate $s = (k^{-1}(M + xr)) \pmod{q}$ (Note: k^{-1} is mod q). If $s = 0$, then choose a new value for k and start over.
4. The signature for M is (r, s).

Given a message M and a signature (r, s), the signature is verified using the following:

Verification Algorithm

1. Calculate $w = s^{-1} \pmod{q}$.
2. Calculate $u_1 = M \cdot w \pmod{q}$.
3. Calculate $u_2 = rw \pmod{q}$.
4. Calculate $v = (g^{u_1} \cdot y^{u_2} \pmod{p}) \pmod{q}$
5. Accept the signature as valid if $v = r$.

Suppose that my public key was

$$p = 233,\ q = 29,\ g = 23,\ y = 175$$

1. Determine whether or not the signature $(r, s) = (10, 17)$ is a valid signature on the message $M = 15$. Show steps.

2. Using the same p, q, g as above, a secret key of $x = 19$, and a $1-$time secret value k of $k = 11$, find the signature on the message $M = 8$. Show all steps.

3. Show that the signature you found in the previous problem correctly verifies. Show all steps.