Solutions for CS174 Homework 10

1. $M_2/M_1 \mod p$

2. The hash function needs to be one-way and strongly collision-free. In RSA for example, the attacker can simply pick an element x and compute $y = x^e$. If the attacher can find a preimage of y such that $h(m) = y$, then the attacker can claim x is the signature on m. So we need the one-way property. Assume that the attacker can find x_1 and x_2 such that $h(x_1) = h(x_2)$. Then the attacker might be able to persuade the signer to sign the message x_1 and then the attacker could go around to claim that the signature is on x_2 instead. So we need strong collision-free property also.

3. We can do a three-step protocol for the zero-knowledge proof. Assume the original graph is G.

   (a) The prover randomly generate a graph G' which is isomorphic to G and send the verifier G'.

   (b) The verifier randomly selects either 0 or 1 and send it to the prover.

   (c) If the verifier selects 0, the prover sends the verifier the mapping between G and G' to show that G' is isomorphic to G. If the verifier selects 1, the prover shows the k-clique in G'.

   To make the proof non-interactive, we could make the choice in the second step equals to the hash of the random graph G'.