Directions: Solve the following problems. All written work must be your own. See the course syllabus for detailed rules.

1. Samantha uses the ElGamal signature scheme with prime $p = 29669$ and primitive root $g = 7$.
   (a) Samantha selects private signing exponent $a = 8216$. Her private signing key is $(p, g, a) = (29669, 7, 8216)$. What is her public verification key?
   (b) Samantha wishes to sign a document D. At first, she picks random element $k = 12480$, but she realizes this will not work. Why not?
   (c) Instead, Samantha picks $k = 20233$. What is the value of k^{-1}? (Hint: the answer is not 7499.)
   (d) Given that $D = 24910$, find the signature D_{sig}.

2. WVU decides to use the ElGamal signature scheme to sign its official messages. It publishes the public verification key $(p, g, A) = (64937, 24, 32107)$. Which of the following document/signature pairs, if any, are authentic? Show your work.
   (a) $D = 57917$, $D_{\text{sig}} = (38546, 36585)$
   (b) $D = 35829$, $D_{\text{sig}} = (59960, 34982)$
   (c) $D = 4737$, $D_{\text{sig}} = (4196, 48679)$

3. Let E be the elliptic curve given by $y^2 = x^3 - 27x + 55$. In class, we showed that
$$[(2,3)(3,1)](-1,-9) = [(-1,-9)](-1,-9) = (-1,-9)^2 = (34/9, 71/27).$$
   (a) Compute $(3,1)(-1,-9)$.
   (b) Use part (a) to verify that $(2,3)[(3,1)(-1,-9)] = (34/9, 71/27)$.