1. Suppose that p is a prime number and g is a primitive root modulo p. Prove that, for any two positive integers x and y, the following two congruences are equivalent (that is, either both are true or both are false).

$$\begin{aligned} g^x &\equiv g^y \pmod{p} \\ x &\equiv y \pmod{p-1} \end{aligned}$$

   (This makes precise the notion that primitive roots allow you to simulate arithmetic modulo $p-1$ with arithmetic modulo p.)

2. As we have seen, the security of a number of cryptosystems depends on the difficulty of *discrete logarithm problems.* Suppose that Eve is listening in on an encrypted conversation, and that she will be able to decrypt it if she manages to solve the following two discrete logarithm problems. You may assume that 18 is a primitive root modulo 101.

$$\begin{aligned} 18^x &\equiv 38 \pmod{101} \\ 18^y &\equiv 69 \pmod{101} \end{aligned}$$

   If a cryptosystem is not implemented properly, it may accidentally give Eve some auxiliary information that allows here to crack the discrete logarithm problems in question. For example, suppose that Eve is able to deduce the following two congruences from the communication that she intercepts.

$$\begin{aligned} 38^2 \cdot 69 &\equiv 18^{91} \pmod{101} \\ 38 \cdot 69^2 &\equiv 18^{13} \pmod{101} \end{aligned}$$

   Using this information, find integers x and y solving the first two congruences. (Try to find a short solution that does not require a calculator)

   Note. The ElGamal signature scheme I described in class is vulnerable to an attack like this if it is not implemented well. In particular, if the signer accidentally uses the same "ephemeral key" to sign two different documents, an eavesdropper can efficiently crack her private signing key.

3. For each number, either write the number as a sum of two squares or explain why it is not possible to do so. *Hint: begin by factoring the number into primes.*

   (a) 4370
   (b) 1885
   (c) 1189
   (d) 3185

4. Beginning with the equation $557^2 + 55^2 = 26 \cdot 12049$, apply the "descent procedure" on page 187 of the textbook to write the number 12049 as a sum of two squares.