1. (a) Prove that if n is an even number that is not divisible by 3, then all of the prime factors of $n^2 + 3$ are congruent 1 $\pmod 3$. *Hint.* Use a similar idea as in problem 3 on the last problem set.

   (b) Read the proof of theorem 21.3 in the textbook (it is on page 152). Using a similar argument, prove that there are infinitely many primes congruent to 1 modulo 3 (you will need to use part (a) to finish the argument).

   Note. Both theorem 21.3 and the result of part (b) are special cases of Dirichlet's theorem on primes in arithmetic progressions.

2. Find all of the primitive roots of 31.

   Hint. Once you find one, you can generate the others by computing suitably chosen powers of it.

3. *ElGamal encryption.* This problem describes an encryption scheme whose security is based on the difficulty of the discrete logarithm problem. Suppose that Bob wishes to receive an encrypted message from Alice. He selects a prime number p, and computes a primitive root g of p. Then he chooses a number b at random, and computes the remainder $y \equiv g^b \pmod p$. The number b will be kept secret. The numbers g, y, p are published for all to see. To summarize:

Public key:	(g, y, p)
Bob's secret random number:	b
	such that $y \equiv g^b \pmod p$

   To send Bob a message m, Alice encrypts it as follows: she chooses a random number a, and then she computes two remainders c_1, c_2 such that $c_1 \equiv g^a \pmod p$ and $c_2 \equiv m \cdot y^a$. To summarize:

Plain text message:	m
Alice's secret random number:	a
Encrypted message:	two numbers (c_1, c_2)
	such that $c_1 \equiv g^a \pmod p$ and $c_2 \equiv my^a \pmod p$

   (a) Suppose that Bob receives an encrypted message (c_1, c_2) from Alice. Show that, although he does not know the secret random number a, he can nevertheless compute a "shared secret" $s \equiv g^{ab} \pmod p$, using only his private key and the first part c_1 of Alice's encrypted message.

   (b) Show that using the "shared secret" s and the second part c_2 of Alice's encrypted message, Bob can recover Alice's plain text message m.

(c) Suppose that Bob's public key is $(2, 43, 101)$, and that his secret number is 42 (if you wish, you can verify that $2^{42} \equiv 43 \pmod{101}$). Bob receives a message $(75, 38)$ from Alice. Decrypt this message (determine the original value m). *Note:* you will almost certainly want to use a calculator to do some of the arithmetic here.